Survey on Disaster Recovery as a Service (DRaaS)

[1]Chhaya Chaudhari, [2]Vaishali R. Patel

[1]M.E. Student, [2]Professor
Department of Information Technology,
Shri S'ad Vidya Mandal Institute of Technology, Bharuch, India

Abstract— **Disaster Recovery (DR) is a big term that helps to recover data from any disaster that happened by any situation. Many Private and public sector enterprises use DR Service to protect their data and service applications. Now a days cloud-based DR solution changed the legacy approaches. Many cloud providers like Amazon, Microsoft's and Google drive provides backup service for Disaster Recovery over cloud. This paper presents survey on Disaster Recovery as a Service (DRaaS) and it also includes information about DRaaS providers that provides DR Failover in cloud. This paper presents the detailed information about the DRaaS that can help to provide basic knowledge of DraaS.**

Index Terms — **Cloud, Cloud Computing, Disaster Recovery (DR), DRaaS, IaaS, SaaS, PaaS, Backup/Recovery.**

_____

I. INTRODUCTION

DISASTER RECOVERY is about preparing and recovering data from any kind of disaster. Any event that can harm and have negative effect on business continuity can be termed as disaster for enterprise. This includes software or hardware failure, physical damage to building, network issue, power cut or any human error. To overcome this problem companies planning for DR system. Instead of enterprises buying resources for offsite DR location, cloud computing and its pay-per-use pricing model allows them to pay for long-term data storage and applications while only paying for required storage. In practice, most traditional DR techniques rely on manual detection of disaster situation. Cloud based DR systems can simplify this problem by monitoring the primary data center from cloud nodes. It's another benefits are elastic nature, flexibility and scalability.

DRaaS is category of cloud computing and the term "recovery as a service" (RaaS) is considered to be part of the nomenclature of cloud computing, along with infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). DRaaS is the replication and hosting of physical or virtual servers by a third-party to provide failover in the event of a human-made or natural disaster. Typically, DRaaS requirements and expectations are documented in a service-level agreement (SLA) and the third-party vendor provides failover to a cloud computing environment, either through a contract or pay-per-use basis. A good IT disaster recovery plan will help our company recover lost data and accelerate their organizations return to normal business operations. It will also ensure a disaster will not trigger a major business disturbance and adverse financial consequences. DR should be implemented by all organizations, and not only for Cloud Computing. Even so, the rapidity of putting data and bring up-to-date data in the Cloud is much quicker than desktop systems, and the routine of Cloud also means that users can be anywhere and at any time. In other words, organizations should emphasis on improving the effectiveness and excellence of data recovery. One indicator is the percentage of data lost and damage in the DR process should be minor than using desktops [12].

Contribution

This paper includes survey on DRaaS (Disaster Recovery as a Service). This also includes overview of DRaaS that helps to understand DraaS and solutions given by DRaaS. It also provides basic knowledge about cloud computing storage and its way of storing data. This paper also includes abstract information of DRaaS vendors and their provided solution. This will help to choose relevant solution for recovery. Furthermore, it includes literature survey of some papers that used to complete this survey. Finally it includes the advantage and disadvantage of DRaaS.

Organization

This paper proceeds as follows. Section 2, provides overview and techniques used in DRaaS. Section 3, includes literature survey of research papers. Section 4, includes information of DRaaS providers. Section 5 and 6, includes advantages and disadvantages of DRaaS. Finally we have conclusion of paper.

II. OVERVIEW OF DRaaS AND TECHNIQUES USED

Most of the cloud providers like Amazon and Microsoft azure offers backup services which is Do-it-Yourself (DIY) model. Many cloud service providers tie up with the DR solution vendors to offer Disaster Recovery as a Service (DRaaS) over cloud. DRaaS solutions are pre-packaged cloud facilities that provide a standard DR Failover to a cloud environment where responsibility of keeping and handling periodic/continuous backups lies with the DRaaS solution provider. Using DRaaS,

professionals can use cloud infrastructure on a pay-per-use basis with flexible rates based upon requirement of recovery point objective (RPO) and recovery time objective (RTO). The DRaaS suppliers such as CA ARCserve have vendor lock- in for the cloud service provider or DR solution providers. In short it will ease the DR activity but compromise the flexibility of professionals for DR solution or cloud selection [1].

Virtualization solutions like VMware derived with their own DR solutions. These types of solutions may be appropriate for professionals with own private cloud such as State-Data-Centers (SDC). The main limit for such solution is constraint of parallel architecture at production and DR environment. Such solutions are not appropriate for the combined production sites with heterogeneous virtualization environment [1].

Recovery Point Objective (RPO)
Recovery Point Objective (RPO) RPO states a point in time that data must be backed up and recovered in direction for business processes to resume. The RPO defines the least possible frequency at which interval backups need to occur, from 24 hours to sub-minute time frames [2].
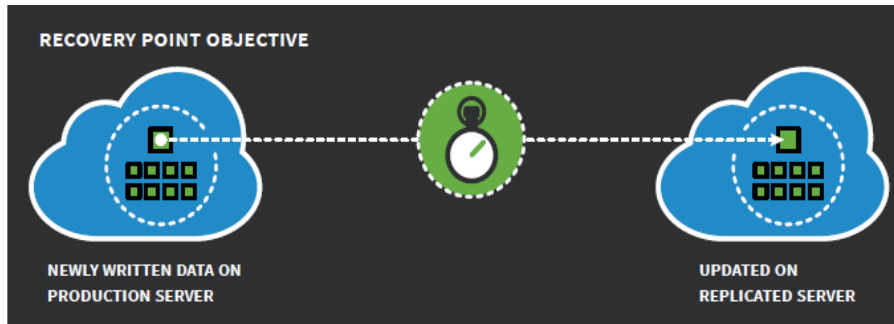

Fig. 1: Recovery Point Objective (RPO) [2]

Recovery Time Objective (RTO)
Recovery Time Objective (RTO) RTO states to the maximum length of time a system (or computer, network or application) can be down after a disaster before the company is adversely impacted by the downtime. Defining the expanse of lost profits per amount of lost time can help define which applications and systems are serious to business sustainability [2].
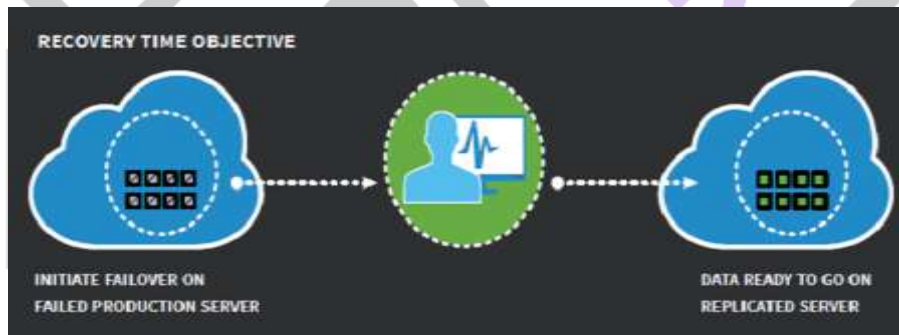

Fig. 2: Recovery Time Objective (RTO) [2]

The RPO and RTO factors delivered by DRaaS solution rest on the data duplication approach used at the back-end. Data duplication may work at any of the following layers: i) Application layer that uses file based duplication ii) OS layer that uses host based duplication, iii) Virtualization layer that uses hypervisor based duplication, iv) Device driver layer that uses appliance based, duplication (usually block duplication), v) Storage layer that uses storage based duplication mechanism. Each of these mechanisms has some challenges and limitation [1].

The file based and host based duplication reduce performance of user request. Hypervisor based duplication is fit for the private cloud based solution as it needs same virtualization architecture at production and DR site. Additionally these solution uses file based data duplication that reduces performance. Application based solution may generate kernel license problems as it interferes with disk drivers. Furthermost Storage based solutions existing in the market deliver quicker data duplication but with the consequence of vendor lock-in and non-flexibility to the professionals for selecting DR storage[1].

III. LITERATURE SURVEY

Summary: They present an adaptive algorithm for addressing a common management problem in enterprise service networks: safely and fast improving from the failure of one or more services. Due to poorly documented and shifting dependencies, Dependency-Directed Recovery (DDR) algorithm, which senses dependencies by observing network interactions and recovers

near-optimally from failures following a distributed graph algorithm. The work presented in this paper builds upon on an architecture designed to support retrofitting of new service management mechanisms onto existing services without modification of those services. The goal of a distributed recovery algorithm is thus as follows: given a service network with some set of failed daemons and services, coordinate daemon actions in order to return as rapidly as possible to a state in which all services are running correctly [3].

They present the design and implementation of ZORFU, hierarchical system architecture for replication across data centers. The prime impact of ZORFU is a local recovery system that considerably increases accessibility of duplicated strongly reliable services. Local recovery reaches this by reducing the recovery time by an order of magnitude, while striking only a negligible latency overhead. Experimental results show that ZORFU can recover a 100MB object in 4ms [4].

In pervasive end situation, numerous mobile devices can work willingly to deliver effective and consistent service. But device movement or failure frequently causes service disruption. How to improve the service path fast and improve the user experience significantly is an main problem. The approach conducts the local service recovery process. If it fails, the method will use the global service recovery process. They use MANET's network service to determine the results [5].

This paper presents one of the first studies on progressive recovery for cloud-based infrastructure services. The difficulty is presented and numerous heuristic algorithms are anticipated using random placement, physical node/link degree, and virtual node/link degree to place repair resources. Overall, the results indicate that the final two strategies give faster recovery of failed demands [6].

Network virtualization permits users to build personalized interrelated storage/computing configurations for their business requirements. Today this ability is being generally used to expand the scalability and reliability of cloud based services, comprising virtual infrastructures services. This paper studies progressive recovery for network virtualization (infrastructure) services. Several heuristic systems are defined using uniform, random, physical node degree, and virtual node degree (load-based) resource delivery. Results indicate that uniform resource placement gives faster initial recovery of interrupted virtual networks. Though, the virtual node degree scheme ultimately reaches equivalent or higher recovery. Conversely uniform and physical node degree placements produce considerably more proficient usage of network bandwidth resources [7].

An effective recovery plan is discovered to decide which datacenters should be recovered at each recovery stage to maximize collective content reachability from any source considering limited existing network resources. They create an Integer Linear Program (ILP) formulation to model the related optimization problem. The numerical instances in paper showed that an effective progressive recovery plan can considerably increase the access to important contents at the early stages of recovery. They provided a large number of examples to discover the sensitivity of inputs such as network-recovery plan, the number and locations of datacenters, and the connectivity of the topology [8].

In this paper they considered and implemented a service recovery framework, including a landmark based/ centralized algorithm and a distributed algorithm, for publish/subscribe messaging services for disaster management. The developed mechanisms recover a failed service without physical efforts. The centralized algorithm uses a landmark node to observe the services and to recover the failed one; the distributed algorithm is a Paxos-based algorithm to compile a reliable recovery plan among nodes, monitoring the failed service [9].

In this paper, they designed an Optimal-DRaaS solution using DR-appliance based data duplication method. The DR-appliance uses iSCSI protocol for block level data access and handover from production to DR site over cloud. The solution is particularly designed for the database applications. Technique of fetching database data using an appliance based (device-driver layer) duplication solution do not need any kernel alterations which will not violate the databases kernel license. The main part of the Optimal DRaaS solution is its flexibility of working with any cloud architecture/platform. The solution can be installed on any cloud architecture as Software as a Service (SaaS). Optimal DRaaS Solution will internally use Infrastructure as a Service (IaaS) of cloud for running the infrastructure required by its user [1].

IV. INFORMATION ABOUT DRaaS PROVIDERS

1. Bluelock

Bluelock delivers Disaster Recovery-as-a-Service for complex environments and sensitive data to help companies' moderate risk with confidence. Bluelock supports unique requirements such as multi-tiered recovery, varied configuration environments with physical and virtual machines and complex security requirements. Bluelock is well known for its Recovery Agreement program, which includes deliberate processes and services designed to certify that clients are completely confident that their disaster recovery plan will work when required [10].

Strengths:
1. Bluelock has strong professional services and robust Onboarding, training and run book improvement processes, which are verified through its Recovery Assurance program [10].
2. Bluelock offers DRaaS solutions designed precisely for sensitive data and compliance (HIPAA/HITECH) [10].

3. Its client portal, Bluelock Portfolio, permits clients to track and manage service charges, resources and RPO realization [10].
4. Bluelock has involvement with hybrid recovery configuration (virtual and physical machines) support and experience handling large enterprise recovery configurations [10].

Bluelock dominates in client satisfaction within the DRaaS industry with a Net Promoter Score of 81 (a score of 50 is considered world-class) and is also recognized by Gartner as a "Visionary" in the Magic Quadrant for Disaster Recovery as a Service [10].

2. IBM Cloud Services

IBM Cloud Services for Virtualized Server Recovery (CVSR) keeps continuous business processes and enhanced flexibility against data interruption. The entirely managed cloud disaster recovery service supports virtual and physical locations on a virtualized cloud infrastructure at a selected secure data recovery center [10].

Strengths:
1. IBM has variable levels of test frequency, declaration costs, recovery goals and service pricing, making it at ease for clients to build the ideal service for their desires [10].
2. Client-initiated premises-to-cloud failovers offer clients more control over activities [10].
3. Recovery management easiness is best for enterprise customers [10].
4. A comprehensive provider portal interface leads to accessible administration [10].

IBM offers an array of data security alternatives and a multi-tiered portal for shortened recovery times. The ready-to-go configuration helps customer decrease time and investment in building, operating and dealing the resiliency solution. IBMs data recovery service confirms non-stop duplication of data to avoid risky gaps. Clients can also employ continuous data observation for a monthly subscription price [10].

3. Seagate Cloud Resiliency Services

Seagate Cloud Resiliency Services offers both self-managed and provider-managed data security and recovery services. Their DRaaS model provides real-time duplication of your system data, as well as access during scheduled downtime. They promise accessibility of your critical data within one hour of an outage, confirming you'll be able to access your systems even in the event of a disaster [10].

Strengths:
1. Seagate offers tiered storage to guarantee your most critical data can be recovered as soon as possible during an outage [10].
2. Additional storage can reach up to 15 percent more at no extra charge [10].
3. Regular data integrity checking confirms system stability [10].
4. Seagate offers extensive language support [10].

Seagate uses a one-hour SLA option that is compatible with any backup solution, modifying the need for a secondary site. The services also support a number of Windows and virtual platforms, to protect your data and applications, including NetApp; Microsoft Windows Server 2003, 2008 and 2012; Microsoft Exchange; SQL Server, File Server and SharePoint; Blackberry Server; IBM i and IBM AIX; Red Hat and SUSE Linux; and VMware [10].

4. Sungard Availability Services

Sungard has a multi-solution DRaaS service that contains Recover2Cloud, Managed Recovery Program and Enterprise Storage Replication. Their model is a managed service that contains customer-managed features for a more customizable practice. They offer both cloud and hosting services to fit their disaster recovery service to your desires [10].

Strengths:
1. Sungard offers integrated applications and data recovery management [10].
2. Crash-consistent and application-consistent recovery for both virtual and physical locations guarantees your data will be secure no matter what [10].
3. A plenty of data backup and application recovery professional services are offered [10].
4. Sungard put up with SSAE 16 service organization control (SOC) 2, PCI DSS, HIPAA and International Organization for Standardization (ISO) 9001 agreement [10].

Sungard works to support your IT environment to protect against unwanted hybrid situations. Its provider-managed recovery testing helps in effective assessments, leading to customizable improvements. Sungards general method of disaster recovery is adjustable for each client's RTOs and RPOs, giving extensive flexibility and completeness [10].

5. Acronis Disaster Recovery Service

Acronis Disaster Recovery Service is a complete DRaaS service that offers security and renewal of data, servers and complete data centers. Their model is an flexible, pay-as-you-go service that transfers, protects and recovers data in physical, virtual and cloud backgrounds. This recovery service providers aim is to make things easier and reduce the costs of protecting your data [10].

Strengths:
1. Acronis shows extensive knowledge of hybrid recovery configurations [10].
2. A recovery console gives clients authority over administration, reporting and analytics [10].
3. Full automation offers runbook austerity [10].
4. Acronis uses automated and isolated recovery testing for client ease [10].

Acronis is planned for mid-size organizations and enterprises and offers self-service web-based disaster management for a active practice with your data recovery. Their push-button recovery uses automated runbook events to recover complete data centers at once and automated testing allows for consistent assessment [10].

6. iland Disaster Recovery as a Service

iland Disaster Recovery as a Service is a completely managed service that supports the duplication and recovery of VMware, Microsoft Hyper-V and Citrix Xen VMs inside the enterprise cloud. A number of premiseto-cloud options are supported, including SAN-to-SAN replication [10].

Strengths:
1. Strong attention on long-term customer relationships [10].
2. Target response time 15 minutes or less for all customer questions [10].
3. No charge or constraints on fail-over testing [10].
4. 100 percent service uptime availability SLA [10].

iland has integrated disaster recovery management within its Enterprise Cloud Services Console, supporting selfservice failover and failback of workloads at the click of a button. Users can also set RTOs and RPOs from seconds to minutes to hours, according to the tier of application [10].

7. NTT Communications

NTT Communications Disaster Recovery as a Service (DRaaS) group offers cloud-based services including Cloud Recovery and Cloud Backup that can assist as a key part of a company's disaster recovery plan or offer a complete solution, allowing a business to function as normal during planned or unplanned outages [10].

Strengths:
1. Highly functional and easy-to-use DRaaS portal [10].
2. Users can describe, configure and monitor virtually any level of service [10].
3. Offers global support for hybrid configurations [10].
4. No charge for unlimited failover and recovery testing [10].

NTT Coms DRaaS offering also comprises its Enterprise Cloud resources, and Disaster Recovery consulting services, provides in addition to unlimited failover and recovery testing, all with the aim to deliver each customer the top disaster recovery and business continuity program for their business. Through NTT Coms dynamic and scalable Enterprise Cloud platform and one of the prime global data center tracks, customers are able to leverage NTT Coms infrastructure in over 196 countries to deploy a robust and secure DRaaS program [10].

8. Axcient Business Recovery Cloud

Axcients Business Recovery Cloud removes data loss, keeps applications up and running, and makes sure that IT infrastructures never go down. Axcient swaps legacy backup, business continuity, disaster recovery and archiving products, with a single integrated platform that copies an complete business in the cloud, making it simple to restore data, failover applications, and virtualize servers or an complete office with a click [13].

9. Amazon Web Services (AWS)

Amazon Web Services (AWS), a company can expand its infrastructure as-needed, pay-as-you-go basis. They acquire access to the same highly secure, reliable, and fast infrastructure that Amazon uses to run its own global network of websites. AWS also gives the flexibility to quickly change and optimize resources during a DR event, which can result in major cost savings [14].

With the many DRaaS providers out there, it is important to choose the one with services that best suit your company's goals and objectives. DRaaS platforms vary, so do your homework and make sure all your questions are answered satisfactorily before you sign an SLA [11].

Key Consideration when Choosing a DRaaS Provider

1. Does the provider use flat-rate pricing for VMs or for host servers?[13]
2. Is the provider able to protect your physical servers?[13]
3. Does the provider charge you for DR testing?[13]
4. Does the provider charge for failovers in which you must temporarily operate workloads in the cloud?[13]
5. Is there a fee for data recovery operations?[13]
6. If a failover does occur, how easy will it be to fail back?[13]
7. **Does the provider have multiple data centers, and where are they? Will my organization be protected against regional disasters?[13]**

V. ADVANTAGES OF DRaaS

Rapid and Immediate Recovery: Your company can never be sure when a disaster might occur. If one does happen, how much downtime is acceptable? Each second the power is out or your servers fail means huge losses for your organization. With a DRaaS solution in place, you do not have to worry about this: if a disaster strikes, you will be able to restore normal operations within minutes [11].

Resources Used: Virtualized DRaaS uses vast and scalable infrastructure, and allows virtual access of assets, with little or no hardware and software expenditures. In other words, DRaaS requires far fewer operational resources. This results in significant savings in software licenses and hardware, allowing the organization to increase its budget in other areas of operation, such as marketing and R and D. Businesses using DRaaS do not have to worry about backup servers, as their service provider will be supported by a state-of-the-art data center, along with enterprise-grade bandwidth and computing power [11].

Flexibility: Compared to more traditional methods of backup, DRaaS is much more flexible. The various DRaaS services offer clients more options in how to handle different business systems. Any enterprise using DRaaS solutions can select from a variety of recovery scopes, depending on the type of the disaster. These can include server failure, human-caused disasters, loss of power or building access, data hampering, and much more [11].

Reliable Security: Security in DRaaS is commonly misunderstood, so choose your provider wisely. For example, its important to ensure that the provider is compliant with all the relevant regulatory bodies. In addition to making sure the data center itself is physically secure, you should also verify that data is encrypted in-flight and at rest. DRaaS providers should implement automatic systems to monitor the health of your data. For peace of mind, they should also be able to provide you with reports for any specified period [11].

Professionalism: A team of DRaaS professionals will handle your account in case a disaster strikes. They will make sure your data is up and running in a short period of time, as specified in the service level agreement (SLA). Depending on the provider you choose, 24 x 7 x 365 services might be available [11].
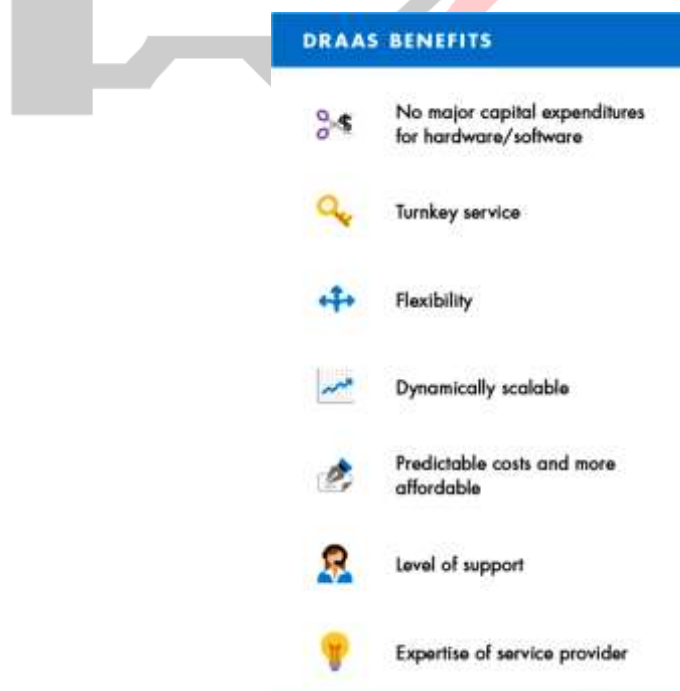

Fig. 3: DRaaS Benefits [13]

VI. DISADVANTAGES OF DRaaS

There are some issues that are connected with DRaaS in comparison with Colocation recovery.

1. Control over solution setup of DraaS is lower.
2. Recovery Time Objectives Minutes to hours (depending on the SLA with the provider).
3. Length of contract Monthly, quarterly, annual terms.

In future we can create more reliable, faster and secure service that can help enterprises and big firms to recover and protect their data.

VII. CONCLUSION

This paper provides all information about DRaaS that can help get basic knowledge about DR system over cloud. This also shows that recovery over cloud will help users to be free from disasters that are man-made or done by machines and network. There is number of providers that provide Disaster Recovery as a Service (DRaaS). From this paper we can get the clear idea about DRaaS. This paper includes information about different providers that will help to recover your data from large scale disaster by providing DR solutions and you can choose any provider depending on your enterprise use.

References

[1] Zia Saquib, Veena Tyagi, Shreya Bokare, Shivraj Dongawe, Monika Dwivedi and Jayati Dwivedi,"A New Approach to Disaster Recovery as a Service over Cloud for Database system", Published on - Advanced Computing Technologies (ICACT), 2013 15th International Conference.

[2] A white paper by Online Tech service provider,"Disaster Recovery", Published by- OnlineTech, 2016.

[3] Shane S. Clark, Jacob Beal and Partha Pal,"Distributed Recovery for Enterprise Services", Published on - 2015 IEEE 9th International Conference on Self-Adaptive and Self-Organizing Systems.

[4] James W. Anderson, Hein Meling, Alexander Rasmussen, Amin Vahdat, and Keith Marzullol,"Local Recovery for High Availability in Strongly Consistent Cloud Services", Published on - IEEE Transation on Dependable and Secure Computing VOL. X, NO. Y, JANUARY 2013.

[5] Danmei Niu, Lanlan Rui , Shaoyong Guo and Xuesong Qiu,"A Novel Recovery Strategy for Service Interruption in Ubiquitous
Stub Environment", Published on - IEEE 2014.

[6] Mahsa Pourvali, Kaile Liang, Feng Gu, Khaled Shaban, Samee Khan and Nasir Ghani,"Progressive Recovery for Cloud-Based
Infrastructure Services", Published on - 2015 IEEE 4th International Conference on Cloud Networking (CloudNet).

[7] Mahsa Pourvali, Kaile Liang, Feng Gu, Hao Bai, Khaled Shaban, Samee Khan and Nasir Ghani,"Progressive Recovery for Network Virtualization After Large-Scale Disasters", Published on - IEEE 2016 International Conference on Computing, Networking and Communcations, Optical and Grid Networking.

[8] Sifat Ferdousi, Ferhat Dikbiyikt, Massimo Tornatore and Biswanath Mukherjee,"Progressive Datacenter Recovery over Optical Core Networks after a Large-Scale Disaster", Published on - IEEE 2016 12th Int. Conference on the Design of Reliable Communication Ne works (DRCN 2016).

[9] Chi-Sheng SHIH, Hsin-Yi CHEN, and Zi-You YEH,"Service Recovery for Large Scale Distributed Publish and Subscription Services for Cyber-Physical Systems and Disaster Management", Published on -The 2nd IEEE International Conference on Cyber-Physical Systems, Networks, and Applications.

[10] ITBusinessEdge website Available: http://www.itbusinessedge.com/slideshows/disaster-recovery-as-a-service-7-top-providers2-7.html

[11] Enterprise Features website Available: http://www.enterprisefeatures.com/benefits-disaster-recovery-servicedraas/

[12] Victor Chang,"Towards a Big Data System Disaster Recovery in a Private Cloud", Published on -Ad Hoc Networks, Elsevier on 19
November 2014.

[13] A white paper by Brien M. Posey from axcient ,"Best Practices in Business Recovery:Colocation or DRaaS?", Published on -2015 Axcient, Inc.

[14] A white paper by Glen Robinson, Attila Narin, and Chris Elleman from AWS ,"Using Amazon Web Services for Disaster Recovery", Published on - October 2014.