NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696 Website: ijiert.org
VOLUME 8, ISSUE 6, June. -2021

# CLOUD DEPLOYMENT MODELS FOR RESILIENCE INTERNET DISASTER RECOVERY: A REVIEW

Anigbogu, Gloria N.
Department of Computer Science, Ebonyi State University, Abakaliki, Nigeria
gn.anigbogu@unizik.edu.ng

Ituma Chinagolum
Department of Computer Science, Ebonyi State University, Abakaliki, Nigeria
ichinagolum@gmail.com

Anigbogu, S. O.
Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria
so.anigbogu@unizik.edu.ng

Anigbogu, K. S.
Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria

## ABSTRACT
Organizations of all sizes require safeguarding of their data on regular basis, which makes disaster recovery and backup procedures, a much desired responsibility. This paper reviewed the various cloud deployment models for resilience internet disaster recovery in cloud computing environment. The work was able to show the relevance of deployment of appropriate disaster recovery models in cloud computing environment that can help to improve quality of service and customer confidence in their service provider.

**KEYWORDS**: Cloud deployment, Internet disaster, Business continuity, Disaster recovery

## INTRODUCTION
Disaster recovery involves procedures to preserve continuation of business in case of a disaster (Brook et al., 2015). Shaw (2018) observed that disaster recovery is a part of business continuity, which focuses more on keeping all aspects of a business running despite the disaster. And since information Technology IT systems these days are so critical to the success of the business, disaster recovery remains a major pillar in the business continuity process.

Disasters often take place in vicinity of human livelihood. Disaster can either be natural or man - made. Most natural disasters come without warning and take lives of tens, hundreds and thousands of people. Natural disaster can destroy entire cities if precaution is not taken. The types are erosion, earthquakes, floods, tornadoes, hurricanes, lightning, landslide, tsunamis, wildfires and thunderstorms. The effects of natural disasters are very serious and the destruction caused may take a very long time to recover. The damages can equally take billions of dollars (Dimiter and plamena 2011). Some of the dangerous disasters in the history of mankind are Bhopal (India) gas accident of 1984, Chansala (India) mining disaster of 1975, September 11 terroist attack (USA) 2001, Chernobyl (Russia) nuclear accident of 1986, Indian ocean tsunami of 2004, Nepal earthquake (2005) and Fort McMurray (Canada) forest – fire (2016). Hurricane is one of the major natural disasters that affect countries like Canada, Bahamas, and USA etc. That of USA can be traced back since 1850's to 2019 and beyond, with different name tag; 2019 hurricane was named Dorian (Hauck, 2019).

Mohammad *et al.,* (2014) had noted that disaster recovery is a persistent problem in IT industries. It equally goes beyond IT industries and cut across every other industry. The society today depends mainly on computer system that even a short period of down time can result in significant financial loss or in some cases can even put human lives at risk (Wood *et al*., 2010).

However, Mohammad *et al.,* (2014) observed that most man-made disaster can be hardware or software failure, human error or sabotage. It is not every disruptive event is a disaster. For instance, a power outage may just be an inconvenience if there is a back-up generator and reasonable quantity of fuel. Again, it is not every disaster that involve catastrophic destruction or loss of life, like a cyber-attack can wreak havoc on a business, even though the fabric of the IT infrastructure remains physically untouched.

According to a white paper published by IBM (2012), only 50% of disasters in IBM were because of weather and the rest were caused by other causes like cut of lines, server hardware failures and security breaches. The white paper also indicated that the disaster recovery was not only a mechanism for natural events, but also for severe disruption in cloud systems.

In any business or organization, it is essential to have a backup plan in the event of a disaster which may occur at any time. A disaster recovery plan is a set process or a documented set of procedures which are created in order to retrieve the IT infrastructure of a business in the event of a disaster. This process can also be referred to as an IT disaster recovery. A disaster recovery plan can be a written document with specific steps and procedures set by the company or organization which should be followed when any kind of disaster happens. A good sample disaster recovery plan should state everything that should be done before, during and after a disaster occured. Using these services, data protection and service continuity are guaranteed for customers at different levels. The enterprises main goal is business continuity which means resuming back services online after a disruption

Disaster occurrence can affect the cloud, especially server locations. This problem is more crucial in cloud computing because cloud service providers (CSPs) have to provide the services to their customers even if the data center is down due to disaster. (Mohammad *et* a*l.,* 2014).

Caraman et al., (2009) named their model Romulus, which is a disaster tolerant system based on kernel virtual machines. Romulus can tolerate failure in two situations; on the fly and failover. It uses new egress traffic buffer to replicate disk write after any checkpoint. It is operational within service provider premises even though their algorithms are accurate for disaster tolerant.

Tamura et al., (2008) designed a model known as Kemari. It is a virtual machine synchronization for fault tolerance which provide a cluster system that synchronizes virtual machine for fault tolerance. Kamari uses the primary backup approach so that any storage or network event that changes the state of the primary virtual machine must be synchronized in backup virtual machine. Unfortunately it is only operational within service provider premises.

Nitesh and Bindu (2016) had opined that it is possible to realize a real time disaster management cloud where applications in cloud will respond within a specified time frame. The researchers equally suggested that if a Real Time Cloud (RTC) was available for intelligent machines like robots, the complex processing may be done on RTC through request and response model. Therefore it may be possible to manage disaster sites more efficiently with more intelligent cloud robots without great loss of human lives waiting for various assistance at disaster sites.

Rodrigo De *et al* (2014) also noted that many corporations rely on disaster recovery schemes to keep their computing and network services running after unexpected situation, such as natural disaster and attacks. As corporations migrate their infrastructure to the cloud using the Infrastructure as a Service (IaaS) model. cloud providers need to offer disaster – resilient services. The work also provided guidelines for design of a data center network infrastructure that can support a disaster – resilient IaaS Cloud. This guideline described design

requirement, such as the time to recover from disaster, and allow the identification of important domains that deserve further research efforts, such as the choice of data center site locations and disaster – resilient virtual machine placement.

## CLOUD DEPLOYMENT MODELS

We have the following as the typical cloud deployment models.

(i) Private cloud: The cloud infrastructure is operated entirely for a single organization. It may be managed by the organization or a third party and may exist on- premises or off- premises.

(ii) Public cloud: The cloud infrastructure is made available to the general public or large industry group and is owned by an organization selling cloud services.

(iii) Community cloud: The cloud infrastructure is shared by organization and it supports a specific community. It may be managed by the organization or a third party and may exist on – premises or off-premises.

(iv) Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, Public or community) that are bound together by standardized or proprietary technology which enables portability of data and application (Dimiter and plamena 2012)

## INTERNET DISASTER RECOVERY APPROACHES

Recovery Time Objectives (RTO) and Recovery Point Objective (RPO) are two key metrics that organizations must consider in order to develop an appropriate disaster recovery plan that can maintain business continuity after an unexpected event.

Although, only one letter separates RTO from RPO, it is important not to confuse these two metrics. Both help to determine maximum tolerable hours for data recovery; how often data backups should occur and what recovery process should take place. Again, both need to be considered when creating a disaster recovery plan.

### Recovery Time Objective (RTO)

It is a metric that helps to calculate how quickly you need to recover your IT infrastructure and services following a disaster in order to maintain business continuity.

RTO is measured in terms of how long your business can survive following a disaster before operations are restored to normal. If RTO is twenty-four hours, it means that the business can maintain operations for that amount of time without having its normal data and infrastructure available. If data and infrastructure are not recovered within twenty-four hours, the business could suffer irreparable damage or loss.

### Recovery Point Objective (RPO)

It is a measurement of the maximum tolerable amount of data to lose. It also helps to measure how much time can occur between your last data backup and a disaster without causing serious damage to your business. RPO is useful for determining how often to perform data backups.

RPO is significant because in most cases, one will likely lose some data when a disaster occurs. Even data that is backed up in real-time has a risk of being lost. Most businesses back up data at fixed intervals of time: say once every hour; every day or perhaps as infrequently as once every week. The RPO measures how much data you can afford to lose as a result of a disaster. (Dennis, 2019)

Table 1 Comparison of different Disaster recovery models and features. (Source: Mohammad *et al.*, 2014)

| S/N | DR Model | Year developed | Authors | Features |
|---|---|---|---|---|
| 1 | SecondSite | 2012 | Rajagopalan | 1)Uses quorum node to detect and distinguish a real failure.<br>2)Make use of checkpointing.<br>3)Geographically separated backup site<br>4) SecondSite not good for stateless services |
| 2 | Remus | 2005 | Cully et al | 1) Make use of storage replication combined with live LM migration<br>2) Providing low level service to gain generality<br>3) Transparent<br>4) seamless failure recovery<br>5) uses checkpointing<br>6) Needs significant bandwidth and it also increases performance overhead |
| 3 | Kemari | 2008 | Tamura et al | 1) Uses the benefits of Lock stepping and Checkpointing<br>2) No need for external buffering mechanism |
| 4 | RUBis | 2010 | Wood et al | 1)Uses replication mode resources<br>2) Uses failover mode resourses |
| 5 | Taji | 2011 | Zhu et al | 1) Uses a Hypervisor- Based Fault Tolerant (HBFT) prototype<br>2) Uses Network attach storage (NAS)<br>3) Decreases synchronization |
| 6 | Romulus | 2009 | Caraman et al | Disk replication and Network protection<br>2) VM Checkpointing<br>3) VM replication<br>4) failover detection |
| 7 | HS-DRT | 2010 | Ueno | Uses encryption, spatial scrambling, fragmentation of data<br>The weakness: the performance of web application decreases if the number of duplicated copies increases |
| 8 | Pipe Cloud | 2011 | Wood et al | Uses pipeline replication technique.<br>Tracking the order and dependencies of the disk writes.<br>Uses higher throughput and lower response time by decreasing the impact of WAN latency on the performance.<br>pipeCloud cannot protect the memory states because it leads to large overhead on WAN |
| 9 | Distributed Cloud system Architecture | 2013 | Silva et al | Uses redundancy with multiple data centers which are geographically separated.<br>Active VM in both warm and hot nodes |

**Issus of Cloud Deployment Models and Internet Disaster Recovery: An Overview**

Kemari is a fault tolerance system by Tamura et al (2008) which used Virtual machine synchronization to deal with fault tolerance

Again, Wood et al (2010) observed that many businesses rely on disaster recovery (DR) services to prevent either man made or natural disaster from causing expensive service disruptions. Unfortunately, current DR services come either at high cost or with only weak guarantees about the amount of data lost or time required to restart operation after a failure. The authors argued that cloud computing platform are well suited for offering DR as a service due to the pay as you go pricing model which can lower costs and also use of automated virtual platforms that can minimize the recovery time after a failure. The authors also performed a

pricing analysis to estimate the cost of running a public cloud based DR Service which showed significant cost reduction compared to using privately owned resources

Furthermore, Rajagopalan et al., (2012) developed a disaster tolerance as a service named SecondSite. SecondSite is designed to tackle three challenges: Reducing RPO, Failure detection and Service restoration with the following three techniques;

a. Using a storage to keep writes between 2 checkpoints. Checkpoints move between sites in a specific period. However if a failure happens at the time of movement of data then, some data will be lost
b. Using a quorum node to detect and distinguish a real failure. A quorum node has been designed to monitor primary and backup server. If replications have not been received by the backup site in the waiting time, backup time sends a message to quorum node. In this case, if the quorum node receives a heartbeat from primary node, it means primary server is active and the replication link has a problem, otherwise the backup site will be active.
c. Using a backup site: There is a geographically separated backup site which allows one to replicate groups of virtual machines through wide – area internet links. Secondsite increases ability to fast failure detection and also differentiate between network failures and host failure.

The process of SecondSite being used for disaster recovery and its tolerance is illustrated in figure 1

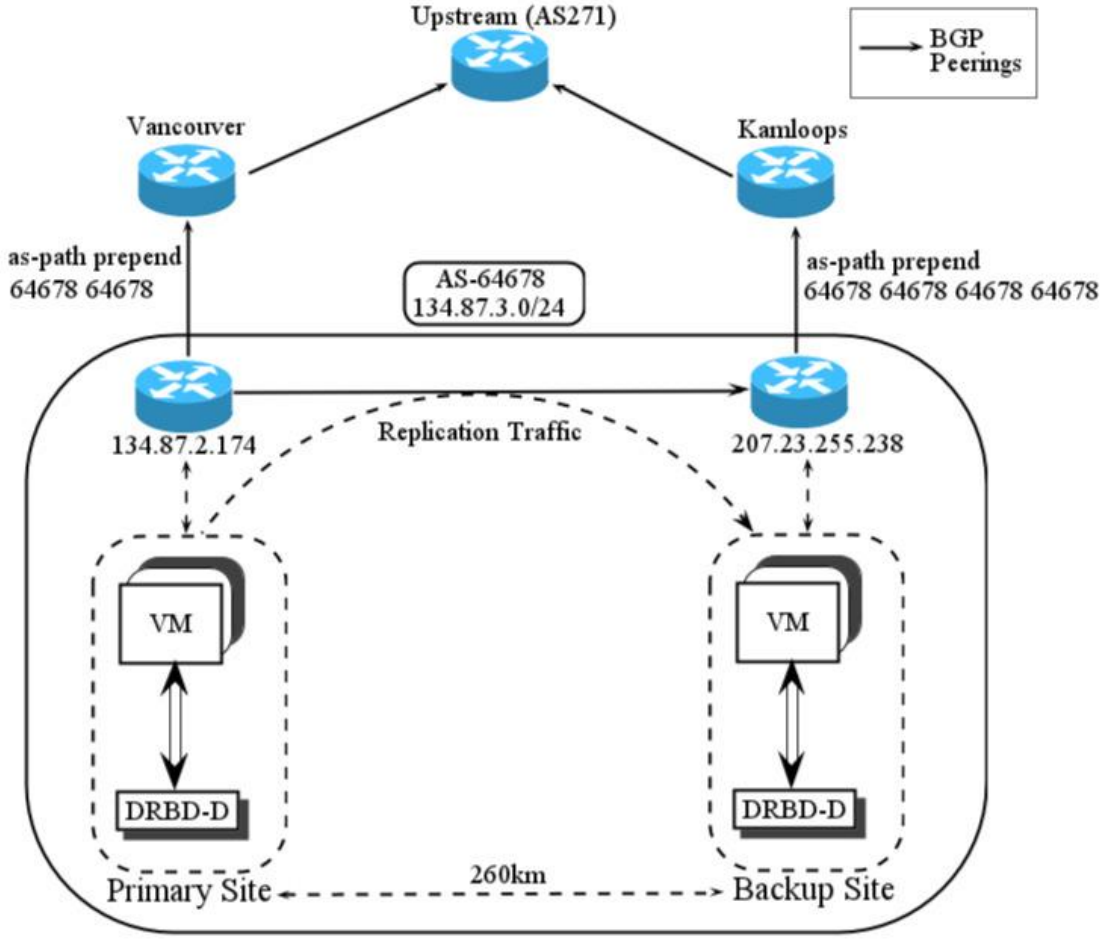


Fig 1. SecondSite setup over WAN (Rajagopalan et al., 2012)

Again a related work by Caraman et al., (2012) was called DT Enabled Cloud Architecture. This work uses Romulus seven stage algorithms. It was important to observed here that Romulus is another disaster recovery model designed by Caraman et al., 2009. DT Enabled Cloud Architecture provides a disaster tolerant service with respect to resource allocation, which is a challenge in DT services. However,host and backup clusters are monitored by high availability controllers. Each cluster has three different controllers;

1 Storage controller: To control and manage the cluster storage

2 Cluster controller: To manage IPs, centralized memory and CPU availability

3 Node controller: To load, start and stop the virtual machines (VMs)

Zhu et al., (2011) also developed disaster recovery system called Taiji. Taiji is a Hypervisor – Based Fault Tolerant (HBFT) prototype which uses a mechanism similar to Remus. We also note here that Remus is another hypervisor designed by Cully et al (2008). Taiji uses a network attach storage (NAS) instead of Remus separated local disk. Shared storage may become a single point that cause a weakness of this method.

Cully *et al.*, (2008) equally developed disaster recovery system called REMUS. Remus provides an extremely high degree of fault tolerance, to the point that a running system can transparently continue execution on an alternate physical host in the face of failure with only seconds of downtime, while completely preserving host state such as active network connections. Remus encapsulates protected software in a virtual machine, and asynchronously propagates changed state to a backup host at frequencies as high as forty times a second. It uses speculative execution to concurrently run the active virtual machine slightly ahead of the replicated system state. And unfortunately, since high availability is hard to achieve; it requires that the system should be constructed with redundant components which are capable of maintaining and switching to backups in the face of failure. Indeed, commercial high availability systems that aim to protect modern servers generally use specialized hardware or customized software or both. In each case, the ability to transparently survive failure is complex and expensive enough to prohibit deployment on common servers.

Again, Ueno et al., (2011) in their work evaluated some results for a high security disaster recovery system using distribution and rake technology. The authors proposed an innovative file backup concept which makes use of an effective ultra-widely distributed data transfer mechanism and a high –speed encryption technology. The concept is based on the assumption that we can use a small portion of the storage capacity of a large number of PC's and cellular phones which are in use in daily life; to efficiently realize safe data backup at an affordable maintenance and operation cost. The HS-DRT system capability is based on the following:

i. It does not require the use of expensive leased lines
ii. It only utilizes otherwise unused network resources, such as unused network bandwidth and unused storage capacity in PC's, smart phones and cellular phones, etc.
iii. It can utilize cloud computing facilities/environment which is one of the remote Grid nodes to obtain a requested amount of storage and a specific security level in accordance with the customer's requirement
iv. It can cipher a number of important data files at the same time using spatial scrambling and random dispatching technology
v. As the number of user company increases, the security against being deciphered illegally increases accordingly
vi. The maintenance cost can be drastically reduced.

In addition, data is increased since it uses a stream cipher encryption. Therefore, it can also be applied to secure streaming for video transmission services

Nayak, et al (2010) developed a system known as ENDEAVOUR. This consists of framework for integrated end- to – end disaster recovery planning. And unlike other research that provided disaster recovery planning within a single layer of the IT stack (eg storage controller based replication), ENDEAVOUR can choose technologies and composition of technologies across multiple layers including virtual machines, databases and storage controllers. ENDEAVOUR also uses a canonical model of available replication technologies at all layers; explores strategies to compose them, and perform a novel map- search- reduce heuristic, to identify the best disaster recovery plan for given administrator requirements.

Furthermore, Gharat & Mhamunkar (2015) proposed a disaster recovery as a service (DRaaS) which is a nomenclature of cloud computing. This DRaaS is a low cost service when compared to traditional disaster recovery. It is flexible in replicating physical or virtual data. It provides application consistent recovery for

some working applications like SQL server. It has pre- built options for virtual recovery environments including security, network connectivity and server failover when it is continuously replicating among servers. When disaster occurs, disaster recovery backup will run all the applications until the primary site is restored.
Again, Machuca et al., (2016) in their work gave an overview of different solutions in the context of technology-related disasters affecting communication networks and focused more on the importance of Software Defined Networking (SDN), its state of art on the resilience issues and approaches towards resilient SDN networks.

## CONCLUSION

Interstingly, from the overview we have done, it can be seen that it is essential to have a backup plan in the event of a disaster which may happen at any time in our business or organization. A disaster recovery plan as already noted is a set process or a documented set of procedures which are created in order to retrieve the IT infrastructure of a business in the event of a disaster, and this is why it can also be referred to as an IT disaster recovery.
In Nigeria, for instance many business concerns and relevant government agencies are yet to fully embrace this emerging technology (Cloud computing) and disaster recovery in order to be able to enhance their profitability by reducing overhead cost on services, in the cause of hosting their services individually on the Internet. This is because most organization in Nigeria outsource the service. And consequently, there is a palpable fear not only about the security of data of individual organizations when they are co- hosted in the cloud as the technology today demands but also, the issues associated with disaster occurrences that are rampant today in the IT industry.
Therefore, disaster whether it is natural or man-made may affect big data stored in cloud environment in one way or the other. It is apparent that the flow of information and commerce in our global business environment never sleeps. Hence organizations and individuals need to think in terms of application continuity in the face of interruptions. Business downtime can result in huge losses in productivity. Breaches of customers service agreements, whether explicit or implicit can cause irreparable damage to the organizations reputations and huge financial loss. Hence, addressing issues relating to such breaches needs a scalable environment provided with flexible information, access to easy communication and real time collaboration from all computing devices.
In this regard, the relevance of an overview of cloud deployment model of a disaster-resilient Internet system in cloud computing cannot be over emphasized since the knowledge about the phenomenon can help to improve the quality of service and customer confidence when handling their businesses.

## REFERENCES

1) Brook, C., Bedernak, M., Juran, I., & Merryman, J., (2012): Disaster recovery strategies with Tivoli Storage Management. IBM Corp.
2) Caraman, M. C., Moraru, S. A., Dan, S. & Grama, C., (2012): Continous Disaster Tolerance in the IaaS clouds. 13th IEEE International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) pp. 1226-32. http://dx.doi.org/10.1109/OPTIM.2012.6231987
3) Caraman, M. C., Moraru, S. A., Dan, S. & Kristaly, D. M., (2009): Romulus, Disaster Tolerant System based on Kernel Virtual Machines. 20th International DAAAM Symposium: Intelligent Manufacturing & Automatum: Theory. Practice & Education (pp. 1671-78)
4) Cully, B., Lefebvre, G., Meyer, D., Feeley, M., Hutchinso, N., & Warfield, A. (2008): Remus: High Availability via Asynchronous Virtual Machine Replication. 5th USENIX symposium on Networked Systems Design and Implemantation pp161-174

5) Dennis, G., (2019): RTO vs RPO: Two means Towards the same End. https:www-cloudberrylab.com/resources/blog/rto-vs-rpo-difference/
6) Dimmter, V., & Plamena, Z., (2012): A Feasibility Study of Emergency Manageement with Cloud Computing Integration. International Journal of Innovation, Management and Technology Vol. 3 No 2 pages 188-193.
7) Gharat, A., & Mhamunkar, D., (2015): Disaster Recovery in Cloud Computing. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol. 4 Issue 5. ISSN: 2278-1323
8) Hauck, G., (2019): Lorenze Becomes The Most Powerful Hurricane To Make It So Far East In The Altantic. https:/www.usatoday.com/story/news/nation/2019/09/27/hurricane-lorenze-path–azores-strongest-eastern-a7858070021
9) IBM white paper (2013): Virtualizing Disaster Recovery using Cloud Computing . IBM Global Technology services.
10) Machuca, C.M., Secci, S., Vizarreta, P., Kuipers, F., Gouglidis, A., Hutchison, D., Jouet, S., Pezaros, D., Elmokashfi, A., Heegaard, P., & Ristov, S., (2016):Technology- related Disaster-resilient Software Defined Networks. 8th IEEE International Workshop on resilient Networks Design and Modelling. Sept 13-15,2016 Halmstad, Sweden Pages 35-42.
11) Mohammad, A.K., Azizol, A., Rohuya, L., Shamala, S., and Mohamed, O., (2014): Disaster Recovery in Cloud computing: A survey. Computer and Information Science journal vol.7, No.4 ISSN193-8989 pages 39-54
12) Nayak, T., Routray, R., Singh, A., Uttamchandani, S., & Verma, A.,(2010): End – to – end Disaster Recovery Planning: From Art to Science. IEEE/IFIP Network Operations and Management Symposium NOMS2010 Pages 357-364.
13) Rajagopalan, S., Cully, B., Connor, R. O., & Warfield, A. (2012): SecondSite: disaster tolerance as a service. ACM SIGNPLAN Notices, 47(7), 97-107. http://dx.doi.org/10.1145/2365864.2151039.
14) Silva, B., Maciel, P., Tavares, E., & Zimmrmann, A., (2013): Dependability Models for Designing Disaster Tolerant Cloud Computing Systems 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). June 24-27. 2013 Washington USA. Pages 1-6
15) Tamura, Y., Sato, K., Kihara, S., & Moriai,S., (2008): Kamari: Virtual Machine Synchronization for Fault Tolerance. Paper presented at the Proc. USENIX Annual Technology conference (Poster Session).
16) Ueno, Y., Miyaho, N., & Suzuki, S., (2011): Performance Evaluation of a Disaster Recovery System and Pratical Network Applications in Cloud Computing Envirnments. *International journal on Advances in Networks and Services* Vol.4 no 1&2, Pages 130-137.
17) Rodrigo, S. C., Stefano, S., Miguel, E. M., and Luis, H. K. C., (2014): Network Deisgn Requirement for Disaster Resilience in IaaS Clouds. IEEE Communication Magazine
18) Wood, T., Cecchet, E., and Ramakrishnam, K.K., (2010): Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Chanllenges. 2nd USENIC Workshop on Hot Topics in Cloud Computing (pp1-7)
19) Zhu, J., Jiang, Z., Xiao, V., &Lee, X., (2011): Optimizing the perfomance of vritual machine synchronization for fault tolerance. IEEE Transactions on Computers. 60(12). 1718-1729. http://dx.doi.org/10.1109/TC.2010.224.