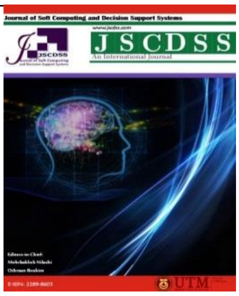
An International Journal
JSCDSS
http://www.jscdss.com
Vol.4 No.4 August 2017: 1-10
Article history:
Accepted 26 June 2017
Published online 26 June 2017

Journal of Soft Computing and Decision Support Systems



E-ISSN: 2289-8603

Hybrid Service for Business Contingency Plan and Recovery Service as a Disaster Recovery Framework for Cloud Computing

Fatemeh Sabbaghi [a,*], Arash Mahboubi [b], Siti Hajar Othman [a]
[a] Faculty of Computer Science and Information System, Universiti Teknologi Malaysia (UTM), Malaysia
[b] Queensland University Technology (QUT), Australia

*** Corresponding author email address**: mfzsab@gmail.com

Abstract

Cloud computing is the latest effort in delivering computing resources as a service to small and medium sized enterprises. These enterprise organizations require installing and maintaining expensive equipment to keep business up and running at all the times. Naturally this requires building an infrastructure flexible enough to respond to any threat under all circumstances. Any disaster may be considered to be a threat associated with the IT infrastructure in a data center. Disaster can occur either naturally or by humans. This paper is focused on how disaster may be controlled in a cloud computing data center which provides services to an organization and how to keep the organization business running while a disaster strikes. The availability and performance of any service is measured by its overall uptime. Recent recovery techniques that have been developed in cloud computing domain have several advantages and disadvantages. Therefore, researchers should conduct some investigations in this field. A hybrid service which utilize redundancy and fault tolerance techniques for providing more accurate recovery in cloud computing when disaster strikes is proposed in order to overcome these challenges in this paper. This hybrid service integrates the Infrastructure as a Service (IaaS) and Disaster Recovery as another Service (DRaaS). The proposed framework is formed by the integration of five essential types of proven redundancy techniques that have a major impact on the uptime of the services during disaster in cloud data centers. For evaluation of the proposed framework, a survey was conducted through a questionnaire presented to and filled by networking professionals and experts. The outcome of data analysis indicates that redundancy-based disaster recovery framework improves the performance of data center recovery and results in a high level of availability of the restored enterprise when disaster strikes. A total of 59.4 % of survey respondents accepted the fact that this framework reduces more than 70 % of threats associated with disaster.

Keywords: Cloud computing, Disaster recovery, Infrastructure as a Service (IaaS), Disaster Recovery as a Service (DRaaS)

1. Introduction

Cloud Computing is a technology that provides services to the users and access to the resources regardless of geophysical location. It consists of several service models for different types of organizations. These services may consist of private or global services. Cloud computing consists of three major services namely Infrastructure as a Service, Platform as a Service and finally Software as a Service. These services are scalable on consumer demand that can be priced on a pay-per-use basis (Bohm et al., 2010). However, cloud services are demanded in enterprise organization for the last several years (Sriram and Khajeh-Hosseini, 2010). Nevertheless, cloud may consist of several data centers or individual data centers that are dependent on the size of organization. Cloud often leverages massive scale, homogeneity, virtualization, resilient computing, low cost software, geographic distribution, service orientation, and advanced security technologies. The last aspect is composed of four deployment models in cloud computing including Private, Community, Public, and Hybrid Clouds. These resources are provided by service providers and require minimal effort for management. Third party management is also applicable (Mell and Grance, 2011; Susanto et al., 2012; Suganya, 2015).

Most enterprises are equipped with expensive IT infrastructure complex network architectures that keep their business running. These infrastructures required management, maintenance, protection to keep business running and avoiding any business contingency. Due to the fact that data in any circumstances should be available to the customers and partners of the organizations, any single point failure might cause unlimited damage to the business impacts. In other words, there are internal and external threats to hard and soft assets and organizations must provide effective prevention and recovery for their assets. In fact, critical incidents may occur any time either naturally or accidentally. However, one form of these incidents is a disaster. Almost all enterprise organizations take precautions and protect the assets of the organization and thus protection of data requires proper strategy and plan against disaster. Every organization requires a Business Continuity Plan

(BCP) or Disaster Recovery Plan (DRP) within the cost constraints that can achieve the target recovery requirements of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) (Alhazmi and Malaiya 2013; S. Suganya, 2015). The likely events that can cause disasters must be identified and their impact must be evaluated. The objectives must be clearly established and feasible DRPs must be evaluated in order to choose the optimal one (Lufaj, 2012).

Since incident affects any critical business application where the company must provide the continuous availability of service, even having an outage for a few moments may cause a serious damage to the organization's productivity (Lufaj, 2012). Therefore, lack of a proper Disaster Recovery Plan (DRP) (Luetkehoelter, 2008) in cloud computing might cause extended damages to the business. A cloud disaster recovery framework plus network redundancy is proposed in this paper in order to avoid single point failures as a business contingency plan. The rest of this paper is organized as follows: Section 2 is related to work in cloud computing and disaster recovery; in Section 3 we propose a new disaster recovery framework and network redundancy; in Section 4 the results are presented and finally in section 5 we conclude the results and discussion.

2. Literature review

Cloud based disaster recovery is very cost effective and it does not need much support while it offers a good opportunity for Small and Medium Enterprises (SME). SME is looking forward to setup disaster recovery. The cloud is an appealing option for disaster recovery since it only requires the business to pay for what is used. Adoption rates in the SME market remain modest (Prakash et al., 2012).

Parity Cloud Service (PCS) is the most reliable method that uses a new technique of generating virtual disks in the user system for backup3. This technique makes parity groups across virtual disks and it stores parity data of parity group in cloud computing (Song et al., 2011).

Each resource maintains its privacy and tries to reduce the cost of the infrastructure. Complexity in implementation is one of the weaknesses in PCS (Sharma and Singh 2012). High Security Distribution and Rake Technology (HSDRT) is an innovative file backup concept. This method is considered as an efficient technique for mobile devices such as laptops and cell phones (Ueno et al., 2010).

It is utilized as an effective mechanism for transfer of distributed data and encryption mechanisms. One of the weaknesses of this method is its inability to handle low cost recovery implementation. It also fails to deal with data duplication (Sharma and Singh, 2012).

The Efficient Routing Grounded on Taxonomy (ERGOT) is completely based on semantic analysis (Ueno et al., 2009). It fails in handling time, and the complexity of implementation in distributed infrastructures in cloud computing (Sharma and Singh, 2012). Linux Box has a simple data backup and recovery architecture (Pirro et al., 2010).

Although this recovery model is very cost effective, it does not meet required data protection level in cloud computing (Sharma and Singh, 2012).

Shared Backup Router Resources (SBBR) technique is another model (Sun et al., 2011) which is cost effective. However, it cannot concentrate on optimizing concepts as well as redundancy. With the entirely new concept of virtualization, Research Education Network (REN) cloud also focuses on low cost infrastructures with complex implementation and low security level. Therefore, recent recovery techniques for cloud computing suffer from various complexity issues. This necessitates the development of more adequate solutions for disaster recovery in cloud computing.

2.1 Cloud Computing Variants and Services

Generally cloud computing services fall into three categories namely Infrastructure as a Service (IaaS), Platform as a Services (PaaS), and Software as a Service (SaaS). These services are demanded based on IT infrastructure and components that the enterprise needs. However, each service is distinct from the others. Fig. 1 illustrates cloud computing variants.

2.1.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is the least service provided by cloud computing vendors in order to run IT infrastructures in an enterprise. IaaS are lower levels of the services that are managed by cloud vendors. The main purpose of these services is to drive towards from traditional IT infrastructure provided by the enterprise data center into virtualization technologies. The virtualization technologies may consist of the following services (Girola et al., 2011):

- Provisioning Physical or Virtual Machines (Hypervisor)
- Web Services (Amazon Web Services Elastic Cloud Compute (EC2))
- Test solutions and, run the results in production in Sandbox Environments

2.1.2 Platform as a Service (PaaS) and Software as a Service (SaaS)

The provision of platform as a Service is to provide network infrastructures through the runtime and it is provided and managed by cloud computing vendors. In facts within PaaS service, enterprises are able almost immediately, to start creating the business logic, and run IT infrastructures. The intensity of hardware up-gradation and cost efficiency makes PaaS worthy of consideration among other cloud services. Finally, SaaS is a complete set of cloud computing services that provide all IT infrastructure components for demands of an enterprise.

2.2 Redundant Recovery Backups

An International Journal JSCDSS E-ISSN: 2289-8603

Disaster Recovery (DR) should be planned based on business sensitivity, the size of the enterprise, and customers of the enterprise. The level of data protection and speed of recovery depends on the type of backup mechanism used and the nature of resources available at the backup site. The various forms of sites may be classified as follows.

In a cold backup site, data is often only replicated on a periodic basis. This leads to an RPO of hours or days. In addition, after a given failure, the servers are not readily available to run the application. Thus, there may be a delay in the order of hours or days as hardware is brought out and installed. Thus, there is a high RTO, and it is difficult to support business continuity with cold backup sites. The only advantage of cold sites is their low cost.

The next type of backup are standby servers that are available to run the application after a failure occurs. These are kept in a "warm" state where it may take minutes to bring them online. This slows the recovery, but also reduces cost. The server resources to run the application should be available at all times, but active costs such as electricity and network bandwidth are lower than that of normal operation. The third category of backup sites are hot backup sites that provide a set of mirrored stand-by servers that are always available to run the application once a disaster occurs. These provide minimal RTO and RPO. Hot standbys usually employ synchronous replication in order to prevent any data loss due when a disaster occurs. This form of backup is the most expensive since fully powered servers must be available all the time to run the application. It can also have the largest impact on normal application performance since network latency between the two sites increases the response times (Cegiela, 2006). A hot site is a must for mission critical cases. Using a hot site is one form of redundancy recovery backup that redirects services from the data center to another data center somewhere in the city or another country with real time data duplication (Cegiela, 2006) (Fig. 2).

A Hot site requires the following conditions:

- Setup an alternative data center in a different geographical location.
- Equipment and location of the alternative data center must be the properties of the enterprise.
- Data must be synchronized during normal business operation with the alternative data center.

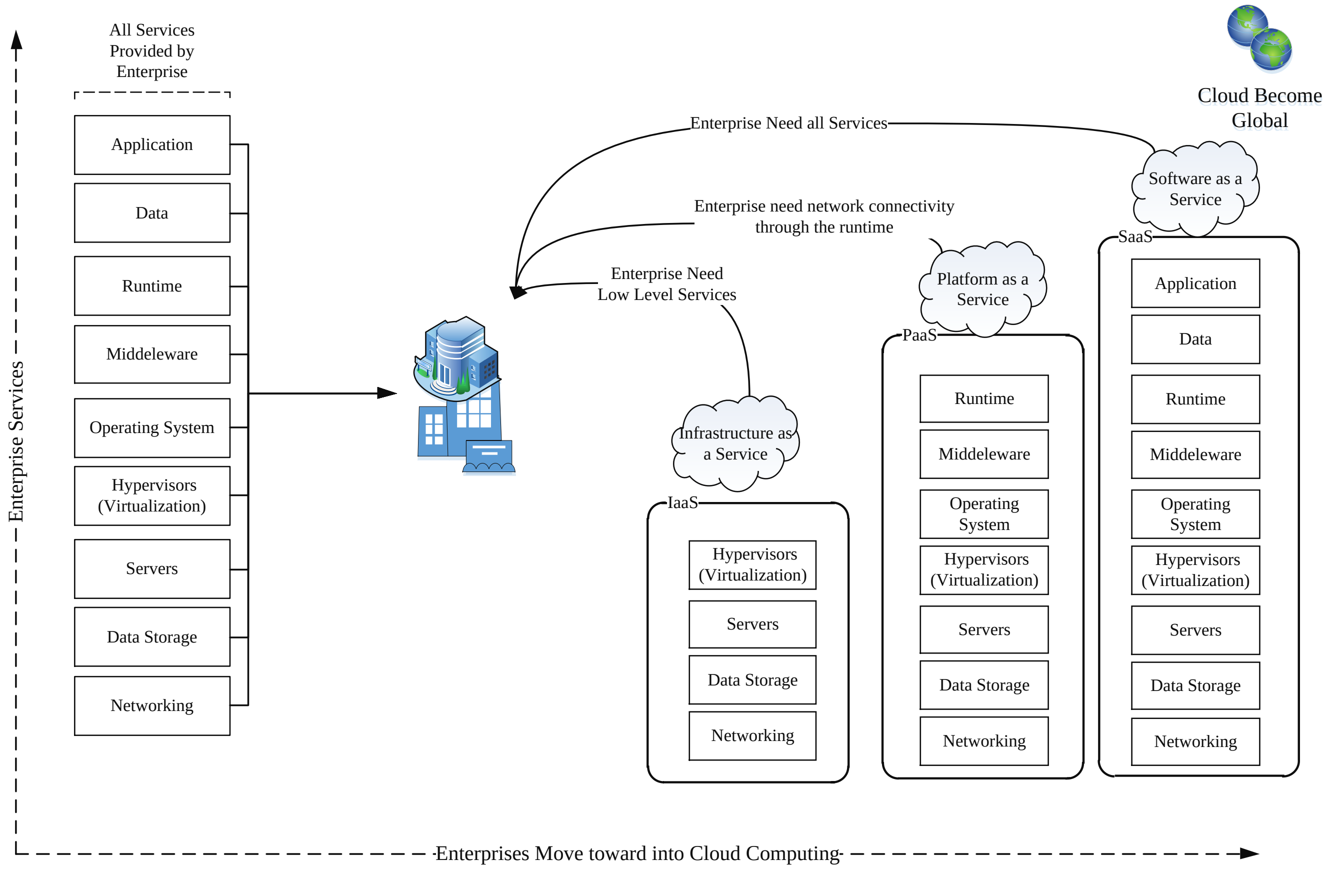

All Services Provided by Enterprise
Application
Data
Runtime
Middeleware
Operating System
Hypervisors (Virtualization)
Servers
Data Storage
Networking
Enterprise Services
Enterprise Need all Services
Enterprise need network connectivity through the runtime
Enterprise Need Low Level Services
Cloud Become Global
Software as a Service
SaaS
Platform as a Service
PaaS
Infrastructure as a Service
IaaS
Application
Data
Runtime
Middeleware
Operating System
Hypervisors (Virtualization)
Servers
Data Storage
Networking
Enterprises Move toward into Cloud Computing

Fig. 1. Cloud Computing Variants

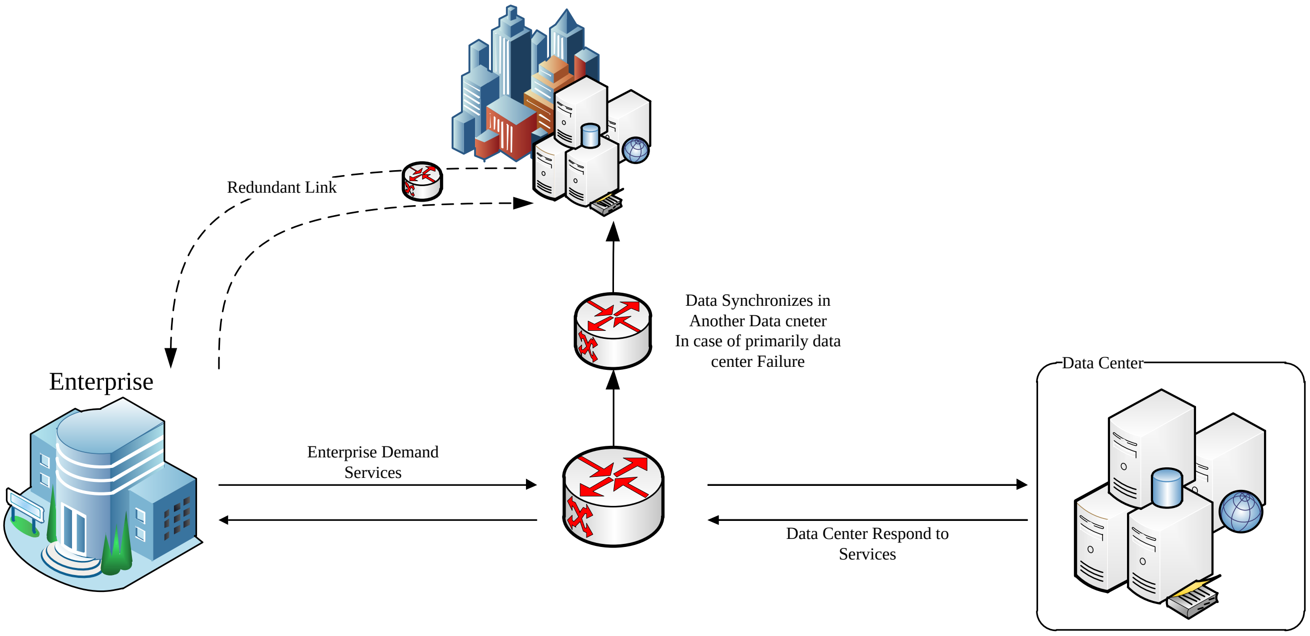


Fig. 2. Hot Site Redundant Plan

As an alternative to Hot Site redundancy, use of a warm site is another type of redundancy plan. It is less expensive compared to the hot site strategies, and it may involve just data storage in alternative data centers (Jian-hua and Nan, 2011). Recovery of off-site data may take more than one day while a warm site can typically be configured within a few hours. However, hot site data recovery only takes (Table 1).

Table 1
Comparison of Disaster Recovery Options in Cloud Computing

		Offsite Backup	Warm Site D/R	Hot Site D/R
Recovery Time		More than 24 Hours	1-4 Hours	1-5 Minute (Reh et al., 2011)
Services	Backup All Virtual Servers	Backup Server, Network configuration & Server in Warm site		Data Storage, Hardware & Network
Critical Path Recovery Services	Hardware, Network	Network Configuration		Network Failover
Time to Recover Service	24 Hour	1-24 Hour		No service Disruption
Average Monthly Cost	From $60	From $120		Depend on the size of the organization

3. The Proposed Framework for Contingency and Recovery Plan

In cloud computing Infrastructure as a Service (IaaS) is a basic service model that provides hardware components to cloud consumers. These components may include virtual machines, storage, networks, firewalls, load balancers, and so on (Bhardwaj et al., 2010). However, sometimes IaaS exceed services with operating systems, virtualization technology and file system as a service. Moreover, IaaS consists of network topologies, data storage, and routing services and provides for the administrative needs of the services needed to store applications and a platform for running applications. Disaster Recovery as a Service (DRaaS) is a new approach which provides full backup of cloud consumers data and maintains IT infrastructure in other data centers that are fully prepared for any sort of disaster (Prakash et al., 2012). DRaaS provides cloud advance maintenance during a disaster or any single point failures in the data center with minimal time efforts. Having DRaaS in business contingency plan should be considered since everything from the Operating System (OS) and lost files can be restored almost immediately depending on the recovery techniques used in the data center. Therefore, proposed framework utilizes DRaaS for full backup and a recovery service for cloud vendors. The combination of IaaS and DRaaS might be necessary for data synchronization in real time. The combination of cloud service is known as a cloud hybrid service. The proposed hybrid framework integrates fault tolerance and redundancy techniques to improved performance, yields a high level of availability and facilitates disaster recovery (Fig. 3).

An International Journal JSCDSS
E-ISSN: 2289-8603

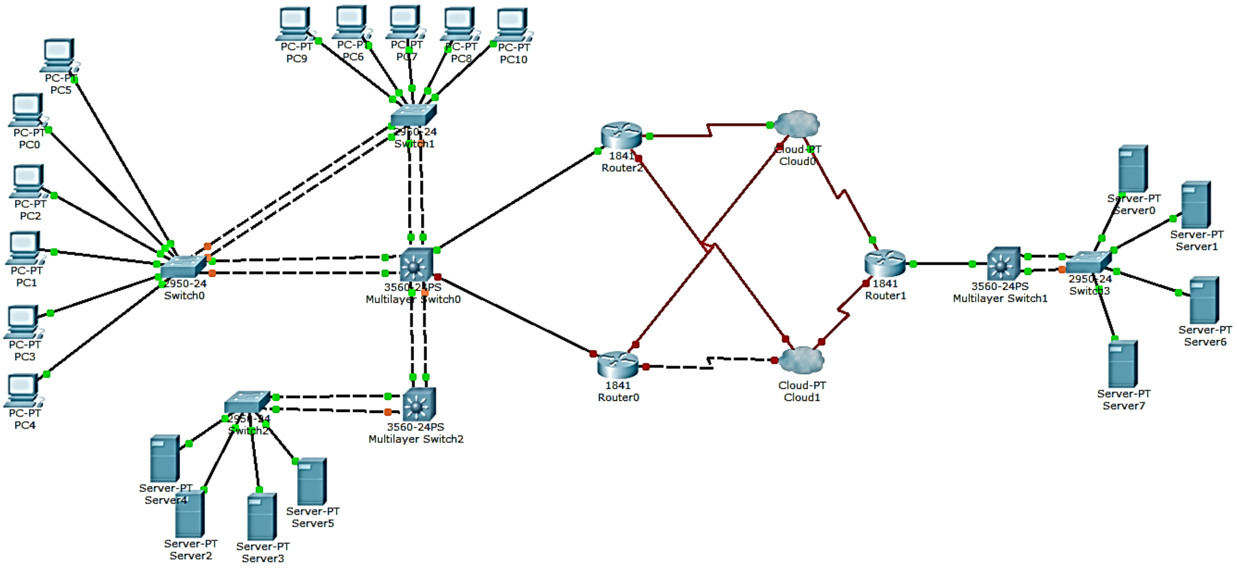


Fig. 3. Redundancy-Based Disaster Recovery Infrastructure for Cloud Computing

3.1 Active/Active, Active/Passive Disaster Recovery Architectures and RAID

It is a fundamental fact that data center design with high-level aspects, active/active, or active/passive architectures are necessary to accomplish fast recovery by spreading several independent servers and geographically distributed processing nodes (Engelmann et al., 2006). Using clustering techniques is necessary to ensure maximum network uptime. It means that every pair of servers configure in active/active or active-passive (Lin et al., 2010) cluster to synchronize session information for high availability (see Fig. 4).

The active one receives a request from the client and accesses the data that is using shared storage and does all work processes. In the passive technique network traffic passes through network equipment, but there is a heartbeat sequence between these servers and servers send messages to each other that are live and ready to provide service. If one of servers is not responding to the heartbeat sequence, automatically all of the traffic passes through redundant servers. Server clustering allows a server to act on its own while using one common, redundant mass storage device. In a basic server cluster, two servers would share one RAID array. This framework uses RAID Level 10 that has High input/output rates that is achieved by striping RAID 1 segment In addition, it is highly fault tolerant and has high data availability. It combines benefits of RAID 1 and RAID 0. It provides data protection by mirroring and it improves performance by striping.

3.2 Spanning Tree Protocol

Spanning Tree Protocol (STP) has proved to be an effective network path redundancy method while eliminating network traffic loops. This ensures that all data paths in a network of bridges are free of loop by disabling forwarding of packets through certain interfaces. The proposed framework also utilizes hot sites as work area recovery sites in business continuity planning of a cloud data center. Usually hot site backup site the data center is located off-site, it can be located in another city or another country. In this design. Spanning Tree Protocol (STP) is used between the switches since it has proven to be a reliable method for providing path redundancy while eliminating loops. It ensures that all data paths in a network of bridges are free of loops by disabling forwarding of packets through certain interfaces. Therefore, it configure a simply connected active topology from the arbitrarily-connected components of the network (Bocci et al., 2008). To avoid the formation of loops, most bridges and switches execute a spanning tree algorithm which allows them to calculate an active network topology that connects every pair of LAN within the network. In this framework, redundant network design enables network's availability by duplicating components in a network. This technique eliminates any single point failures in the network.

3.3 Virtual Router Redundancy Protocol

Routing redundancy is necessary to ensure maximum network uptime. Virtual Router Redundancy Protocol (VRRP) (Hsu et al., 2009) defined in IETF RFC 5798 is for the designs of automatic assignment of available Internet Protocol (IP) for both IPv4 and IPv6 routers to participating hosts. The Router Advertisements are multicast periodically at a rate that the hosts will learn about the default routers in a few minutes in IPv6. They are not sent frequently enough to rely on the absence of the Router Advertisement to detect router failures. However, if the main router has compromised for any reasons such as Denial of Service (DoS) attacks, alternative VRRP is able to divert network traffic into different routing paths.

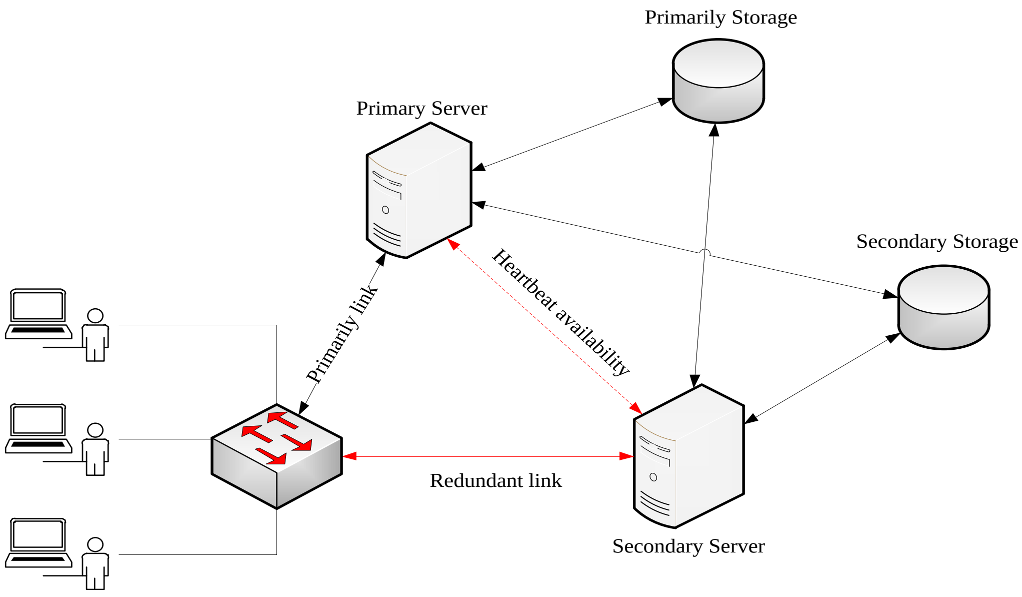


Fig. 4. Active/Active Heartbeat Sequence Redundancy

4. Results

4.1 Description of the Experiment

A quantitative research method was used for data collection by conducting a survey and interview. Due to the limitations of the number of experts available in any given center, the survey samples were chosen from a wide range of institutions including universities and data centers. After meeting with or corresponding with nearly one hundred professionals and experts and asking them for permission to send them the questionnaire, 60 questionnaires were distributed among those who expressed their consent to receive the questionnaire. However, only 32 of them responded to the survey questionnaire. The experts and professionals chosen were either university professors in the field of computer science and/or engineering, and professionals actively working in data centers. The demographic characteristics of the respondents to the survey are listed in Table 2. Experts to whom the survey questionnaire was sent included:

- Three professionals working in the computer data center and Professors at the University Technology Malaysia.
- Network Administrators (CCNP routing and switching, CCNP security, CCNP service provider)
- People working in the data centers of the Islamic Azad University in Mashhad, Shiraz, Behbahan, Mashhad University of Medical Sciences, and a few other centers in Iran.

Table 2
Demographic characteristics of the respondents to the survey

Variable	Classification of variables	Frequency	Percentage
Gender	Male	28	87.5
	Female	4	12.5
Age	Less than 30 years old	6	18.8
	31-40	13	40.6
	41-50	13	40.6
	More than 51 years old	0	0
Education	Degree	0	0
	Master	26	81.2
	PhD	6	18.8
	Post-PhD	0	0
Position	Administer	15	46.9
	Manager	6	18.8
	Lecturer	4	12.5
	Others	7	21.9
Work experience	1-3 years	11	34.4
	4-6 years	18	56.2
	7-10 years	2	6.2
	More than 10 years	1	3.1

The proposed framework was evaluated and validated through the use of a questionnaire that was filled up by networking experts and professionals. The design of the questionnaires was based on disaster recovery and redundancy techniques that are currently used in data centers and the proposed framework. SPSS Statistics software was used to analyze the obtained data. The reliability of the designed questionnaire is 0.7 and it was calculated using Cronbach's Alpha and the reliability coefficient of 0.7 or higher is considered "acceptable" in statistics (George and Mallery, 2010; Reh et al., 2011; García-Peñalvo et al., 2014).

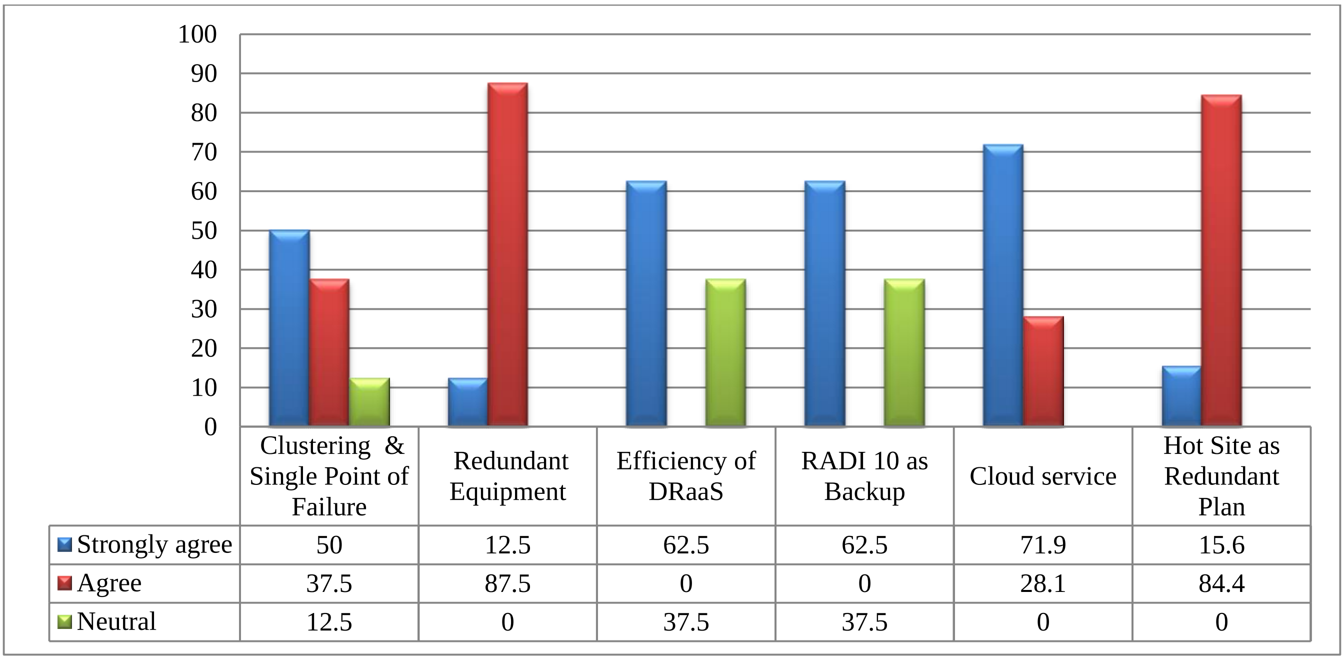
4.2 Experiment Results

The results of the conducted survey reveal that four effective factors have an impact on business continuity during single point failure or disaster. Fig. 5 illustrates effective factors that have an impact on business continuity during single point failures. The first factor is utilizing hot site backup recovery during a disaster. Analysis of multivariate data obtained shows that 84.4% of respondents agreed and the 15.6% strongly agreed that hot site backup recovery reduces probability of service disruption and minimal losses of normal operations in the shortest recovery time by implementing real time data synchronization between the two sites. The second factor is that redundant array of inexpensive disks will increase the level of storage performance and additional storage redundancy in data center. Among four types of RIAD redundancy disks, 62.5% of the respondents to the survey strongly agreed and 37.5% agreed that RAID 10 is able to satisfy and eliminate storage single point failures. The third factor that has an impact and affects business continuity is server clustering. 50% of the respondents to the survey strongly believed that clustering provides failover cluster and increased availability of server workloads and cloud services, or parallel calculating power in case of high performance computing in grid computing. These may include but are not limited to Hypervisors, Database servers and File server services. Finally 71.9% of the respondents to the survey strongly agreed that cloud computing can approach enterprise cost reductions. However, 62.5% of the respondents to the survey strongly agreed that DRaaS is necessary to ensure disaster risk reduction in case of disaster occurrence.

The results also showed that 50% of the respondents to the survey believe that the best choice for storing the backup media is off -site, whereas 37.5% of the respondents to the survey prefer to store data on-site but in a secure location. However, it was found that only 12.5% respondents use encryption mechanisms while they attempt to get backup.

Many interesting results indicating the potential of disaster occurrence is quite possible outside of normal working hours when key personnel are not present. According to the data obtained, 68.8% of the respondents to the survey believed that cloud service is the best option. On the other hand, 31.2% of the respondents believed that the hot site backup recovery service is the best option in terms of privacy and security.

The majority of the respondents (75%) used RAID 10 since it is appropriate for the reduction of storage redundancy and it provides optimization for fault tolerance in data centers whereas, 18.8% of the respondents used RAID 5 and 6.2% RAID 1 because of the high cost in terms of read and write operations (Fig. 6).



	Clustering & Single Point of Failure	Redundant Equipment	Efficiency of DRaaS	RADI 10 as Backup	Cloud service	Hot Site as Redundant Plan
🟦 Strongly agree	50	12.5	62.5	62.5	71.9	15.6
🟥 Agree	37.5	87.5	0	0	28.1	84.4
🟩 Neutral	12.5	0	37.5	37.5	0	0

Fig. 5. Effective Factors on Business Continuity during Single Point Failure in the Proposed Framework

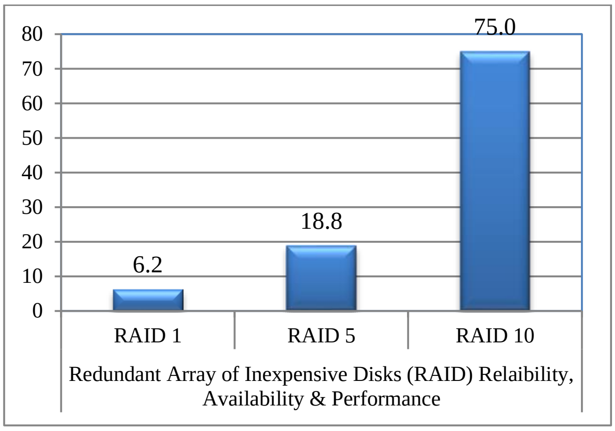


Fig. 6. The Effective Level Percentages for Selections of Good RAID for Backup

Finally, several data center administrators were interviewed in order to analyze and evaluate the proposed framework. Most of the administrators believed that disaster recovery operation and procedures depend upon data center size and financial support. The first priority for most data centers was found to be data center security rather than keeping the data off-site the organizations. However, they agreed (37.5% strongly agree and 62.5% agree) that the proposed framework could help improve redundancy performance if the following techniques that are essential components are taken into consideration for disaster recovery:

- Active/Active or Passive/Active Architectures
- Hot Site/ Warm Site Backup Recovery (in terms of financial support)
- Virtual Router Redundancy Protocol (VRRP)
- Virtualization / Hypervisors
- Utilizing of Network Cloud Services in term of connectivity and not storage services
- Spanning Tree Protocol
- Utilizing RAID

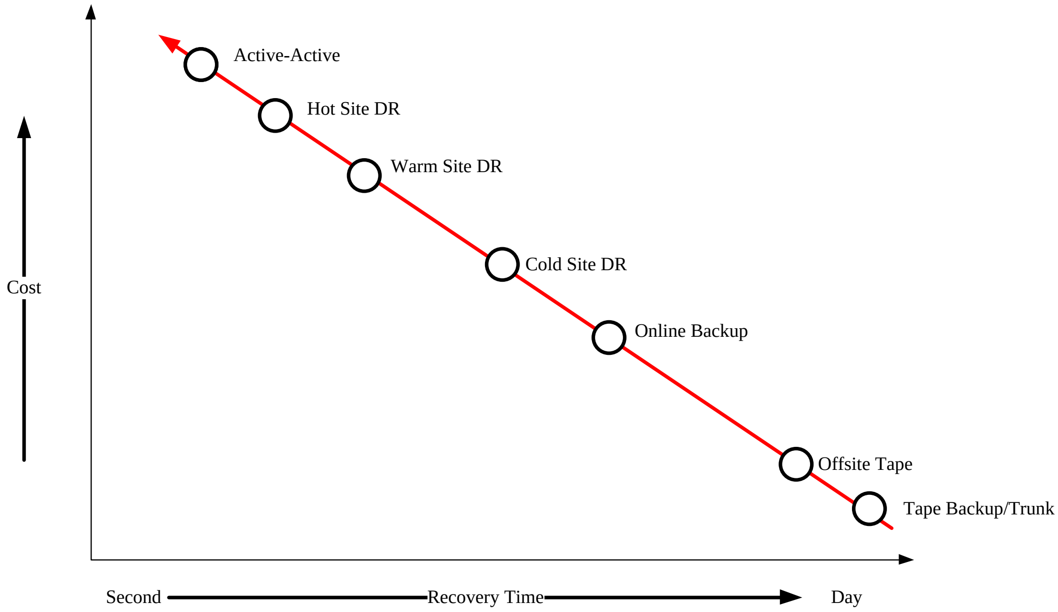


Fig. 7. Different Types of Backup of Disaster Recovery in Terms of Cost Benefit Analysis and Time

Surprisingly Active/Active disaster recovery architecture found a high performance reliably utilized with a minimum of down-time. The results show that 62.5% of the respondents to the survey accepted that Active/Active DR technique is able to stretch between two sites. In addition, if any hardware/software fault is detected, immediately Active/Active servers restart the application on another system without requiring administrative intervention. However, Fig. 7 shows the spectrum of different types of backup for disaster recovery in terms of cost benefit analysis and time to restore normal operation.

Regardless of the Disaster Recovery techniques and cost of technologies used in the proposed framework, 59.4% of the respondents to the survey believed that the implementation of such a framework would increase service high availability and high performance during data center operation. Fig. 8 illustrates the answers given by the respondents to the proposed framework reliability, performance and availability in case a disaster strikes.

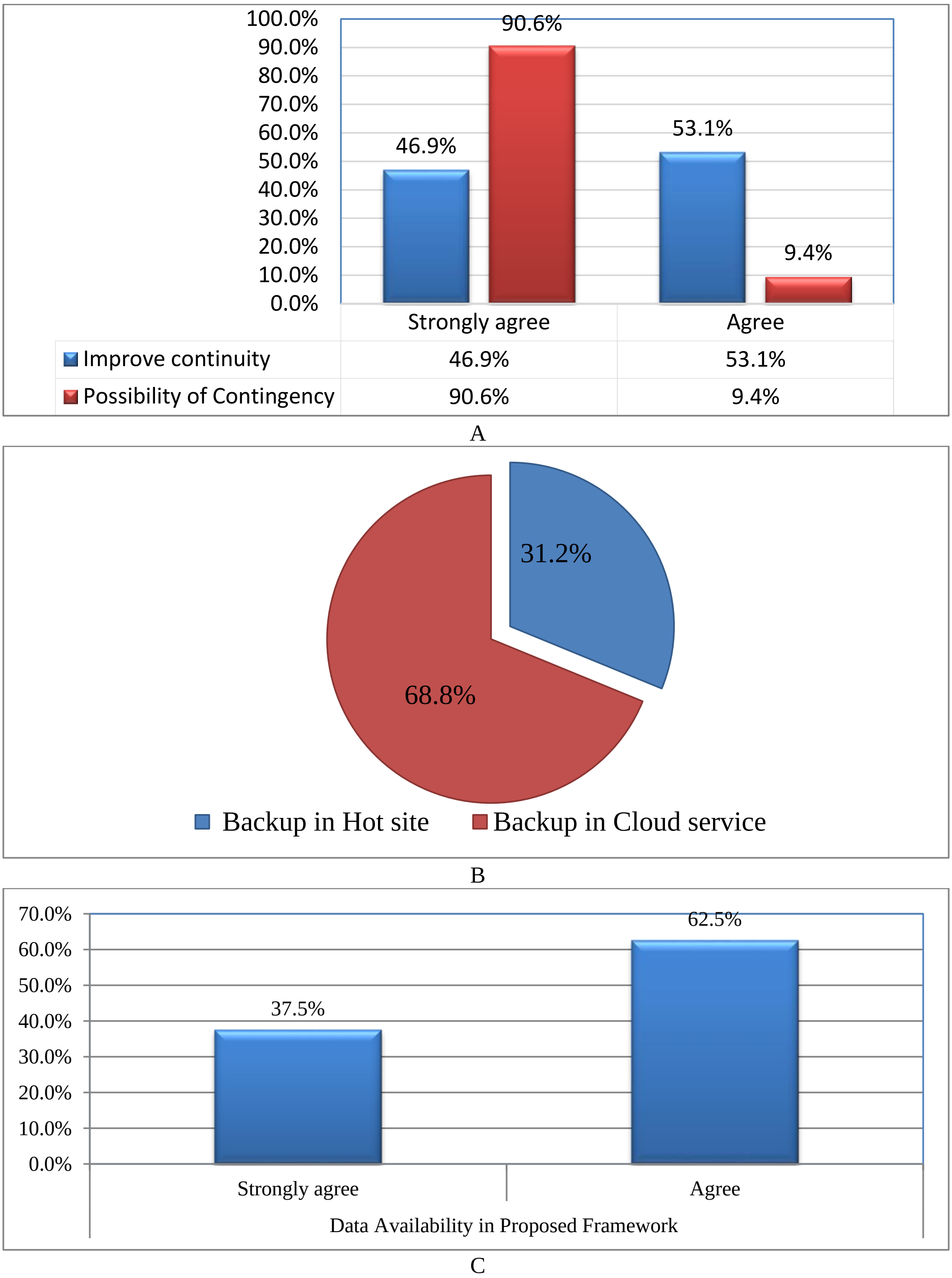


Fig. 8. A) Contingency Level by the Proposed Framework after Disaster, B) Performance Level of Proposed Framework in Disaster Recovery, C) Percentage of Best Choices for Storing the Backup Media

5. Conclusion

Depending upon organization size and sensitivity of service availability, most organizations design a business contingency plan for times of disaster time. However, this study shows that financial support is one of the major concerns for IT administrators and data center designers to select which disaster recovery techniques best fit the data center. Most IT administrators that responded to the survey believed that cloud is the best option for disaster recovery, but not the best option in terms of security and privacy. However, most IT administrators were concerned about recovery time in case of a disaster. We may conclude that time has a high priority among small and large data centers. Based on the review and survey that was conducted, active/active disaster recovery architecture is an essential component for disaster recovery. Based on the fact that cloud data centers are required to provide services all the time to the consumers, combination of (1) Active/active disaster recovery, (2) Hot site (3) Virtual Router Redundancy Protocol (VRRP), (4) Spanning Tree Protocol and (5) RAID are essential components in cloud data centers. However, having dual equipment (N+1) mandatory for high availability for cloud data centers, such as Firewall, Storage Area Network (SAN), network service provider, power infrastructure and so on are also important. Last but not least, 59.4% of the respondents to the questionnaire believed that the proposed framework improves availability, performance, and minimum down-time by 70%in case of a disaster.

References

Alhazmi, O. H. and Malaiya, Y. K. (2013). Evaluating disaster recovery plans using the cloud. Proceedings-Annual of Reliability and Maintainability Symposium (RAMS), IEEE.

Bhardwaj, S., Jain, L. and Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS). International Journal of engineering and information Technology, 2(1): 60-63.

Bocci, M., Cowburn, I. and Guillet, J. (2008). Network high availability for ethernet services using

IP/MPLS networks. Communications Magazine, IEEE, 46 (3), 90-96.

Bohm, M., Leimeister, S., Riedl C. and Krcmar, H. (2010). Cloud computing and computing evolution. Technische Universität München (TUM), Germany, CRC press.

Cegiela, R. (2006). Selecting technology for disaster recovery. International Conference on Dependability of Computer Systems. DepCos-RELCOMEX'06, IEEE, 160-167.

Cegiela, R. (2006). Selecting technology for disaster recovery. Dependability of Computer Systems, 2006. DepCos-RELCOMEX'06. International Conference on Dependability of Computer Systems, IEEE, 160-167.

Engelmann, C., Scott, S. L., Leangsuksun, C. and He, X. (2006). Active/active replication for highly available HPC system services. Journal of Computers, 1(8), 43-54.

García-Peñalvo, F. J., Johnson, M., Alves, G. R., Minović, M. and Conde-González, M. Á. (2014). Informal learning recognition through a cloud ecosystem. Future Generation Computer Systems. 32, 282-294.

George, D. and Mallery, P. (2010). SPSS for Windows Step by Step: A Simple Guide and Reference. 18.0 Update: Pearson Education, Inc.

Girola, M., Friedman, M., Lewis, M. and Tarenzio, A. M. (2011). IBM Data Center Networking: Planning for virtualization and cloud computing. IBM Redbooks.

Hsu, I. P.-S., Jalan R., Kamat G., Kuo A. T.-C. and Moncada-Elias, J. (2009). System and method for providing network route redundancy across layer 2 devices, Google Patents.

Jian-hua, Z. and Nan, Z. (2011). Cloud Computing-based Data Storage and Disaster Recovery. International Conference on Future Computer Science and Education (ICFCSE), IEEE, 629-632.

Lin, G., Zhi-hai, Y., Hai-bo, L., Le-jun, Z. and Jian-pei, Z. (2010). A remote data disaster recovery system model based on undo. Sixth International Conference on Networked Computing and Advanced Information Management (NCM), IEEE, 123-128.

Luetkehoelter, J. (2008). Disaster Recovery Planning, Pro SQL Server Disaster Recovery, publisher: Apress, ISBN 978-1-4302-0601-9, 269-291.

Lufaj, B. (2012). Virtual Desktop and Cloud Services: New Security Demand. Master's thesis of Gjøvik University College.

Mell, P. and Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology Special Publication. 800-145.

Pirro, G., Trunfio, P., Talia, D., Missier, P. and Goble, C. (2010). Ergot: A semantic-based system for service discovery in distributed infrastructures. 10th International Conference on Cluster, Cloud and Grid Computing (CCGrid), IEEE/ACM, 263-272.

Prakash, S., Mody, S., Wahab, A., Swaminathan, S. and Paramount, R. (2012). Disaster recovery services in the cloud for SMEs. International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM), IEEE. 139-144.

Reh, R., Mursidi, M. L. and Husin, N. A. A. (2011). Reliability analysis for pilot survey in integrated survey management system. 5th Malaysian Conference in Software Engineering (MySEC), IEEE. 220-222.

Sharma, K. and Singh, K. R. (2012). Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review. International Journal of Engineering and Innovative Technology (IJEIT) 2(5): 249-254.

Song, C.-w., Park S., Kim, D.-w. and Kang, S. (2011). Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service. 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, 812-817.

Sriram, I. and Khajeh-Hosseini, A. (2010). Research agenda in cloud technologies. arXiv preprint arXiv: 1001.3259.

Sun, L., An, J., Yang, Y. and Zeng M. (2011). Recovery strategies for service composition in dynamic network. International Conference on Cloud and Service Computing (CSC), IEEE. 60-64.

Suganya , S. D. (2015). Evaluation of disaster recovery in cloud computing. International Journal of Multidisciplinary Research and Development 2(6): 300-304.

Susanto, H., Almunawar, M. N. and Kang, C. C. (2012). Toward Cloud Computing Evolution. arXiv preprint arXiv: 1209.6125.

Manvi Mishra, I. A., Singh, P., and Prabhakar, S. (2014). An assessment of cloud computing: evolution. International Journal of Research in Engineering and Technology (IJRET). 668-674.

Ueno, Y., Miyaho, N. and Suzuki, S. (2009). Disaster recovery mechanism using widely distributed networking and secure metadata handling technology. Proceedings of the 4th edition of the UPGRADE-CN workshop on Use of P2P, GRID and agents for the development of content networks, ACM. 45-48.

Ueno, Y., Miyaho, N., Suzuki, S. and Ichihara, K. (2010). Performance Evaluation of a Disaster Recovery System and Practical Network System Applications. Fifth International Conference on Systems and Networks Communications (ICSNC), IEEE, 195-200.