2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)

A Proposed Virtual Private Cloud-Based Disaster Recovery Strategy

Siham Hamadah
Computer Information System Department
Al-Zaytoonah University of Jordan
Amman, Jordan
Email: siham@zuj.edu.jo

Darah Aqel
Computer Science- Artificial Intelligent Department
Al-Zaytoonah University of Jordan
Amman, Jordan
Email: D.aqel@zuj.edu.jo

***Abstract*—Disaster is an unexpected event in a system lifetime, which can be made by nature or even human errors. Disaster recovery of information technology is an area of information security for protecting data against unsatisfactory events. It involves a set of procedures and tools for returning an organization to a state of normality after an occurrence of a disastrous event. So the organizations need to have a good plan in place for disaster recovery. There are many strategies for traditional disaster recovery and also for cloud-based disaster recovery. This paper focuses on using cloud-based disaster recovery strategies instead of the traditional techniques, since the cloud-based disaster recovery has proved its efficiency in providing the continuity of services faster and in less cost than the traditional ones. The paper introduces a proposed model for virtual private disaster recovery on cloud by using two metrics, which comprise a recovery time objective and a recovery point objective. The proposed model has been evaluated by experts in the field of information technology and the results show that the model has ensured the security and business continuity issues, as well as the faster recovery of a disaster that could face an organization. The paper also highlights the cloud computing services and illustrates the most benefits of cloud-based disaster recovery.**

Keywords—Cloud Computing, Disaster Recovery (DR), Disaster Cycle, Cloud-Based Disaster Recovery, Recovery Time Objective (RTO), Recovery Point Objective (RPO).

I. INTRODUCTION

Cloud computing is a type of computing that uses different services over the internet and depends on shared resources. As cloud computing is becoming more and more important from day-to-day, where most organizations adopted the use of this technology in disaster recovery (DR). Cloud disaster recovery is a backup strategy and a protection method that includes storing and maintaining copies of data in a cloud computing environment.

The main requirements for an effective DR services are two key metrics including the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). The RTO refers to how long it can take for an application to comeback online after a major incident (MI) has occurred. In contrast, the RPO refers to the maximum acceptable length of time in which the data might be lost from an application according to MI, the most recent backup preceding any failure [1]. The main objective of the DR plan is to minimize RPO and RTO. There are many cloud computing services such as Disaster Recovery as a Service (DRaaS) [1, 2], which is considered as one of the most significant cloud computing services for DR. Mainly, it is a low cost service comparing with the services of traditional disaster recovery. Organizations should take this service into account in order to protect their data against any disaster. DRaaS is flexible in replicating data physically or virtually and has the ability to quickly recover from any disaster with a minimal user interaction. In general, cloud computing services face security threats and risks that can be found in computing platform, networks, and internets. Therefore, security issues should be clarified clearly before adopting any cloud computing service. Many researchers proposed different solutions for security issues e.g. [3, 4].

Hence, this paper firstly contributes to illustrate the importance of cloud computing in DR instead of the traditional DR. Moreover, it proposes an innovative model for ensuring the use of cloud-based in DR, where this will guarantee the existence of security in clouds. This paper also focuses on the cloud computing services which are provided to customers, especially DRaaS.

The rest of the paper is organized as follows. In Section II, the related work is briefly introduced. In Sections III, the paper represents the disaster cycle phases. Cloud computing services are illustrated in Section IV. Section V introduces the cloud-based DR strategies and proposes a virtual secured private cloud-based DR. Section VI presents the analysis and evaluation of the proposed model. Finally, Section VII concludes the paper.

II. RELATED WORK

In [2], the authors discussed the causes of data loss due to disaster occurrence. They also illustrated some mechanisms that are implemented for data backup when disaster recovery techniques are used. In general, the types of data backup are either hot, cool, or warm backups. Besides, the authors illustrated the implementing of DRaaS in business continuity and demonstrated that it can overcome the issue of data loss when a disaster occurs. In [5], the design and test of the disaster recovery plan are elaborated along with the Google cloud platform based on two key metrics: the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). The article in [5] presents the advantages of the Google cloud platform that is relevant to a well-designed disaster recovery plan. Additionally, the article outlines the best practices for designing and testing a disaster recovery plan.

The relief and recovery procedures are studied and discussed in [6] during the Hudhud cyclone in October 2014. The work in [6] on information collection is conducted for a large amount of information about the activities during the disaster phases in order to reduce and avoid the disaster risks

978-1-5386-7942-5/19/$31.00 ©2019 IEEE

in the future. The main objective is to reduce the response time by understanding the multi-stakeholder participation in the disaster recovery. Every stakeholder should be better prepared to face the disaster recovery. The researcher discusses the preparedness phase including the immediate relief and response to reduce the loss of lives. In [7], the authors illustrated the importance of data centers for continuous operation. They explained the types of database backup which are cold, warm, or hot standby. They analyzed the classification technology of DR and replication technology. This article explained the distributed disaster tolerance, since the distributed disaster can prevent single point of failure, improve business continuity, reduce RTO of an application, and reduce the network traffic load. In [8], a preventive approach for data backup and recovery was proposed to minimize the number of replicas. This approach was called Preventive Disaster Recovery Plan with Minimum Replica (PRPMR). The authors suggested a single replica to ensure the high data availability for short-term backups (7 days), and a two replica for long-term backups (more than 7 days). They illustrated the disaster recovery plan for multi-cloud environments. Their proposed approach was simulated and experimented using three scheduling strategies namely: COST preferred strategy, RTO preferred strategy, and COST/RTO preferred strategy. It provided an effective and less expensive mechanism which reduces the number of replicas to less than three.

III. DISASTER CYCLE

Disaster is an unexpected ruinous event that seriously disrupts the community or organizations and causes losses in possessions. Organizations, therefore, should take care of disaster recovery and pay attention to DR planning. Organizations should also realize the disaster cycle which is a fundamental step in robust DR planning. The disaster involves the following four phases [9, 10]:

- Mitigation: involves steps for eliminating or reducing vulnerability to disaster impacts such as injuries, loss of life, and property. This phase includes fortifying buildings and strengthening public infrastructure to reduce damage and destruction by certain natural hazard events. Hazard mitigation planning involves organizing resources; assessing risks; developing mitigation strategies, writing plans and implementing and reviewing plans. Mitigation planning enables managers to make good decisions based on sound hazard identification and risk assessment data to reduce risks from future hazards.

- Preparedness: Refers to activities and programs that provide more information on how to better prepare an organization and a business community for a disaster. These programs focus on understanding how a disaster might impact the community and how education, outreach and training could support the response and how to recover from a disaster. Preparing for a disaster is a function of thinking about the worst thing that could possibly cause to your organization.

- Response: This phase refers to the immediate reaction as soon as a disaster event occurs. It includes saving lives and meeting humanitarian needs. The organization must attempt to control and maintain the damage, and call for suitable emergency assistance. The resumption step starts after the response phase. During the resumption phase, an organization starts the process by resuming and returning to operations while it is moving from the initial emergency reaction of the disaster to the beginning of the restoring services.

- Recovery: refers to the restoration of all aspects of the disaster's impact on a community and focuses on returning some sense of normalcy. The main objective of the recovery is to restore the less time-sensitive functions of an organization to the operation. The recovery phase of the disaster can be divided into two phase-periods, which are the short-term phase and the long-term phase. The short-term phase typically involves delivering immediate services to businesses. The long-term phase refers to how an organization finally puts itself and its operations back together again. Fig. 1 represents the interrelated phases.

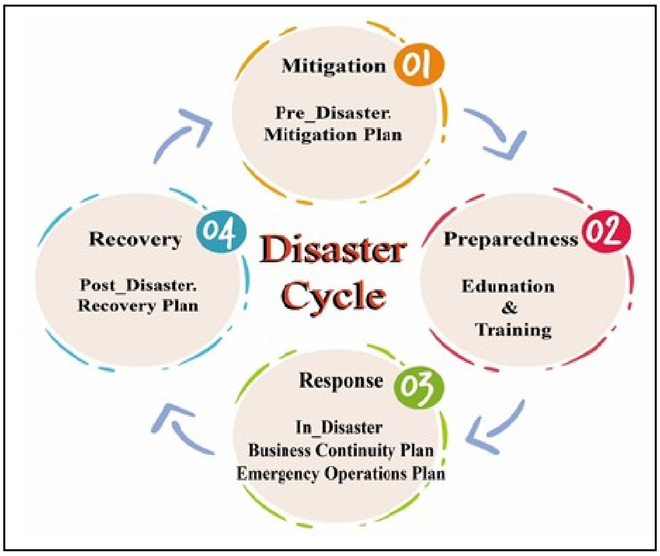

Fig. 1. Disaster phases and cycle.

IV. CLOUD COMPUTING SERVICES

Cloud computing services depend on the end user requirements. Cloud computing providers deliver a variety of services to the customers. The main services are [11, 12]:

- Infrastructure as a Service (IaaS). This service provides computing infrastructure such as servers, storage systems, switches, routers, virtual machines, IP addresses, networks and operating system. It makes computer infrastructure available for customers and this helps in reducing cost of purchasing these devices. There are a number of IaaS providers in the cloud computing, such as Amazon Web Service, Microsoft Azure, and Google Cloud.
- Platform as a Service (PaaS). This service provides a platform and environment in the cloud that allows customers to develop and build applications. It also provides the additional tools such as database management system, analytics and business intelligence services. This service is hosted in cloud and available to customers over the Internet. There are many examples of

PaaS throughout the cloud, such as Microsoft Azure PaaS, Google App Engine, and Red Hat OpenShoft.

- Software as a Service (SaaS). This service is the most popular and simplest one, where it provides an access to software and its functions remotely and makes them available to customers over the Internet. SaaS examples are Facebook, Dropbox, Salesforce, Microsoft office 365, and Tableau.
- Disaster Recovery as Services (DRaaS). It is a service of cloud computing and backup services that is used to help organizations in protecting applications and data against the destructive consequences of disasters whether it was as a cyber-attract or a natural disaster. This service can get rapid recovery and allow organizations to backup and recover their assets on cloud. DRaaS can replicate critical servers and data center infrastructure in cloud. DRaaS examples are Zerto, Axcient, and iland DRaaS. [1].

Iaas, PaaS, SaaS, and DRaaS are expected to grow more and more on the coming years, so that organizations can choose the best service for its business and also for DR. The organizations need to take into account the workload and outcomes that would like to achieve. IaaS improves the business continuity and DR, where PaaS is also useful for business continuity and DR, since it helps to design DR plan in different ways. DRaaS is a full recovery solution that can provide information technology (IT) availability for business.

V. CLOUD- BASED DISASTER RECOVERY STRATEGIES

The cloud based disaster recovery is a service that enables the backup and recovery of remote machines. It reduces the costs that are associated with both the RTO and RPO. The cloud-based systems are more efficient and offer several advantages. So organizations should pay attention to when defining its cloud-based DR strategy and procedures. There are four common types of clouds: private, public, community, and hybrid [13, 14]. These types are discussed in Section A.

A. Private, Public, Community and Hybrid cloud

Private cloud is a term of cloud computing that is only accessible by a single organization. It provides more privacy and high levels of security. Private cloud services offer the provider and the user more control of the cloud infrastructure. In a private cloud, data and processes are managed within the organization. The private cloud computing for disaster recovery is the restoration of data to the IT infrastructure, as data need to be reloaded to obtain the system and return it back to its previous state. Public cloud is another type of cloud computing in which resources could be efficiently shared, where this gives the best utilization of IT resources. In this type of clouds, applications, storage, and data run on the same public pool of resources, and are also available to the general user over the Internet. The public cloud is a suitable place to set up organization's backups and DR that provides financial savings and highly available environments [11, 13]. Community cloud is a cloud service that is controlled and used by a limited set of organizations which have shared interests and information. The members of the community share access to the data and applications in the cloud. This type of clouds helps to improve the user experience and provides communications among users and customers. Community cloud has DR capabilities and backups, and also achieves business continuity with fewer cost [13]. Finally, hybrid cloud is another solution for DR. It is mainly consisted of two or more clouds (private, community, or public). In this type of clouds, public cloud resources are integrated with private, virtual private, or community clouds to perform distinct functions within the same organization. Hybrid cloud is flexible and contains a several different services and applications including backups and DR [4, 13-14].

B. The Proposed Virtual Private Cloud-Based DR Model

The authors propose a virtual private cloud model to achieve scalability and availability after visiting three organizations in Jordan as a research study. In the private cloud, a multi-tenant can reduce cost by buying hardware slices, and by achieving isolation. Moreover, disasters are usually scary and the cloud server providers should maximize the resource utilization. DR levels are data levels, which comprise the system level and application level [10] as shown in Table I. These levels are defined in terms of the system requirements.

TABLE I. DATA LEVELS

DR level	System Requirements
Data level	Security of application data
System level	Reducing recovery time as short as possible. Minimize RTO and RPO.
Application level	Application continuity

DR depends on replication to make backups. This model can use multiple parallel backup locations with separate cloud provider, and the data should be stored in different geographical locations. The replications are synchronous and asynchronous. Synchronous replication can minimize the RTO and RPO, which are important metrics for the disaster recovery (virtual mirroring). Asynchronous replication is another backup of different locations as shown in Fig. 2. When a disaster occurs, primary sites become unavailable. The synchronous site has to be activated first to achieve business continuity. When the first backup site also fails, another one has to be activated. According to the data level and security, data could be encrypted once it's being received to the data center by using different security algorithms, such as the RSA or AES, and then data can be decrypted during recovery. This model is suitable for small or medium enterprises. For large enterprise, the hybrid model that includes the proposed virtual private could be used.

Advantages of the Proposed Virtual Private Cloud for the Disaster Recovery:

- Minimizes the cost.
- Minimizes the RTO and RPO.
- Ensures more security.
  Ensures business continuity.

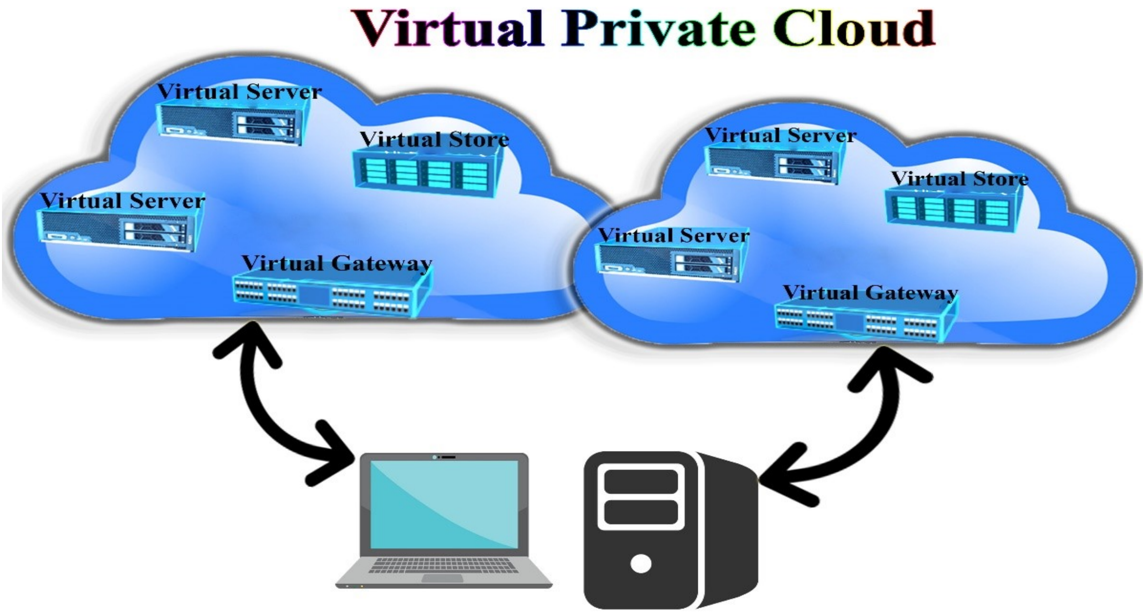

Fig. 2. A proposed virtual private cloud-based DR..

Organizations should consider and pay attention to the business continuity issue whether its primary systems are in their own premises or on the cloud. The cloud-based DR has achieved many important aspects including high reliability, scalability, and availability in comparing with the conventional model. There are some main advantages of cloud-based DR whether the cloud was private, public, community, hybrid, or virtual cloud. The following points summarize these advantages [14, 12]:

- Faster response. The cloud-based DR can respond more quickly to a disaster and can reduce the RTO and RPO from days or weeks to hours or minutes.
- Lower costs. The cost might be reduced in cloud-based DR because some or all resources are shared and by considering the "pay-as-you-go" system, the company will not have to store many backup tapes.
- Conserves resources. Organizations do not have any expenses of setting up a duplicate data center. So the organization is not responsible for maintaining the data center.
- Security. Cloud computing security speeds up growing services to protect critical information. So cloud server provider can provide organizations with more security features in comparison with the conventional model. The cloud services have different security algorithms for encryptions and decryptions.
- Scalability. Cloud services can handle the growing of a business. Increasing or decreasing the storage capacity as organization business demands are easier than the conventional model.
- More Flexible. The organization do not have to select a location for a disaster recovery facility. DR facilities can quickly and easily be moved to different parts of the world within a cloud.

VI. Analysis and Evaluation

This model has been validated by experts in the field assigned from IT bank employees and university computer center staff of three organizations in Jordan. Interviews were conducted between the staff and questionnaires were provided to them. Additionally, they discussed the conventional model for disaster recovery and listed the entire problems regarding the cost and availability. The whole three organizations have conventional methods for disaster recovery. They own servers in many different remote geographical sites, which are being tested from time to time. Consequently, this leads to add more costs, especially when an organization upgrades the entire systems and servers where in return it needs to upgrade disaster servers and systems.

The limitations of this research are the less time available for employees during their work where there was insufficient time to make interviews with the entire IT department. Additionally, the organization cannot sometimes give the whole information regarding the current situation of the disaster recovery systems for security purposes.

The main objective of this model is to provide an organization with a robust planning for disaster recovery, which can protect their data based on the use of cloud-based disaster recovery with a minimum cost. The proposed model could also ensure security, business continuity and faster recovery. Further, this model solves the problems pertaining to the conventional disaster recovery systems.

VII. Conclusion

The paper concentrates on adopting the cloud solutions for DR. Accordingly, a new virtual secured private cloud model was proposed by using the RTO and RPO in order to obtain the whole benefits of the cloud-based computing. This model depends on replication to make backups. It can use multiple parallel backup locations with a separate cloud provider. Prior to the proposal of this model, the author of this paper visited three organizations as a research study in order to investigate about the phenomena of any natural disasters that are currently running in different countries. Some cloud-based DR strategies were illustrated in this paper. These strategies achieved the data availability, scalability, financial saving, and faster response in a way that is more efficient than the conventional model. Further, an instructive study about the cloud computing services was carried out, especially DRaaS which is appropriate for DR.

As a result, it can be shown to be proven that the cloud-based DR is better and more scalable than the conventional model. The validation of the proposed model can be conducted with the assistant of experts in the aforementioned organizations who can efficiently assess the produced model. Finally, this work could support the future researchers who might be interested in cloud-based disaster recovery.

Acknowledgment

We would like to express our special thanks to Al Zaytoonah University of Jordan for the effort that it provides to us for supporting this research paper.

References

[1] S. Suganya and S. Dhanalakshmi, "Evaluation of disaster recovery in cloud computing," *in the International Journal of Multidisciplinary Research and Development*, vol. 2 , no. 6, pp 300-304, June 2015.

[2] A. Srinivas, Y. Seetha Ramayya and B. Venkatesh, "A Study on Cloud Computing Disaster Recovery," *in the International Journal of Innovative Research in Computer and Communication Engineering,* vol. 1, no. 6, August 2013.

[3] B. Hari Krishna, S. Kiran, G. Muralia, and R. Pradeep Kumar Reddy, "Security Issues In Service Model Of Cloud Computing Environment", *in the International Conference on Computational Science*, Procedia Computer Science 87 (2016), pp. 246 – 251 Elsevier. 2016.

[4] A. Dubey, G. Shrivastava and S. Sahu,"Security in Hybrid Cloud", In *the Global Journal of Computer Science and Technology Cloud and Distributed,* vol. 13, no. 2, pp. 1–7, 2013.

[5] Creative Commons Attribution 3.0 License, How to Design a Disaster Recovery Plan. 2017. [Online]. Available: https://cloud.google.com/solutions/designing-a-disaster-recovery-plan. [Accessed: Jan. 25, 2018].

[6] Y. Meduri, "Multi-stakeholder participation in disaster recovery: A case study," in *Humanitarian Technology: Science, Systems and Global Impact 2016,* HumTech2016, 7-9, Procedia Engineering 159, Elsevier, pp. 179–185, June 2016.

[7] T. Zhu, Y. Xie, Y. Song, W. Zhang, K. Zhang and F. Gao," IT Disaster Tolerance and Application Classification for Data Centers," in *International Congress of Information and Communication Technology (ICICT 2017),* Procedia Computer Science 107 (2017) 341 – 346, Elsevier ,2017.

[8] M. Alshammari, A. Alwan, A. Nordin and A. Abualkishik, "Disaster Recovery with Minimum Replica Plan for Reliability Checking in Multi-Cloud*," in The 9th International Conference on Ambient Systems, Networks and Technologies,* Procedia Computer Science 130 (ANT 2018) pp. 247–254. Elsevier, 2018.

[9] Post-Disaster Recovery Planning Forum: How-To Guide Prepared by: Partnership for Disaster Resilience, University of Oregon's Community Service Center, 2007

[10] E. Maiwald and W. Sieglein, *Security Planning & Disaster Recovery,* USA: McGraw-Hill/Osborne, pp. 197–250, 2002.

[11] V. Spoorthy, M. Mamatha and B. S. Kumar, "A Survey on Data Storage and Security in Cloud Computing", In *the International Journal of Computer Science and Mobile Computing,* vol. 3, no. 6, pp.306–313, 2014.

[12] S. Challagidad, S. Dalawai and N. Birje, "Efficient and Reliable Data Recovery Technique in Cloud Computing", in the *Internet of Things and Cloud Computing,* vol. 5, no.1 , pp. 13–18,2017.

[13] Kh. Ali, Sh. Mazen and E. Hassanein, "A proposed hybrid model for adopting cloud computing in e-government," in the Future Computing and Informatics Journal, vol. 3, pp. 286-295, 2018.

[14] R. Rajan and S. Shanmugapriyaa, "Evolution of Cloud Storage as Cloud Computing Infrastructure Service", In *the IOSR Journal of Computer Engineering,* vol. 1, no. 1, pp. 38–45,2012.

.