CLOUD-BASED DISASTER RECOVERY AND PLANNING MODELS: AN OVERVIEW

Siham Hamadah

Computer Information System Department
Faculty of Science and Information Technology
Al-Zaytoonah University of Jordan
P.O.Box 130, Amman 11733, Jordan
siham@zuj.edu.jo

ABSTRACT. *Disaster recovery of information technology is a hot area of security for protecting data against unsatisfactory events, which involves a set of procedures for system continuation. Disaster recovery is a subset of business continuity, while the disaster recovery planning is a subset of business continuity planning. There are many policies for disaster recovery. This paper begins with an illustrative study of some models for disaster recovery. Then, it gives a discussion of some cloud-based disaster recovery strategies and compares them with the traditional disaster recovery. The results show that the cloud-based disaster recovery achieved better results than traditional disaster recovery. Also, the paper highlights importance of disaster recovery planning.*
Keywords: Disaster Recovery (DR), Disaster recovery planning, Cloud-based disaster recovery

1. **Introduction.** Due to rapid development of information technology, data security of information system is facing more and more challenges. In addition to the increase in the number of various types of disasters, either natural or man-made, it is necessary to pay attention to and focus on the Disaster Recovery (DR). DR is a part of security planning that aims to protect an organization from bad effects of inacceptable events [1]. Cloud-based disaster recovery is a facility that is applied in DR models to enable backup and recovery of remote machines on a cloud-based platform. It has many benefits such as faster recovery of disaster, more scalability of Information Technology (IT) infrastructure, less cost and high availability of data [2]. Recently, different models for cloud-based DR have been suggested in some studies, e.g., [3,4]. Those models suggest effective solutions to replace the traditional strategies of DR with cloud-based.

The disaster recovery planning is a documented process of assessing risks that may cause a damage to an organization. It aims to develop, document, implement, test, and specify a set of procedures for recovering and protecting the IT infrastructure and returning to the normal operation [5,6]. Robust planning needs two key metrics, which are the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). The RTO refers to the maximum time in which the application can be offline after a Major Incident (MI) has occurred. The RPO refers to the maximum acceptable length of time in which the data might be lost according to MI [7,8]. The main objective of the DR plan is to minimize the down time, data loss, RPO and RTO. Every part of the DR plan requires both the RTO and RPO. This paper contributes to illustrating the importance of cloud computing in the DR instead of the traditional DR.

Hence, this paper reviews some cloud-based disaster recovery models and compares them with the traditional one. It also demonstrates the importance of developing the

necessary plans that could avoid and mitigate many different disasters. Furthermore, it clarifies the cloud-based DR strategies.

The outline of the paper is organized as follows. In Section 2, the literature search is introduced. In Section 3, the importance of the disaster recovery planning is presented. In Section 4, the cloud-based DR strategies are illustrated. Finally, the conclusion of the paper is given in Section 5.

2. **Literature Search.** The principles of disaster recovery plan, and the steps of the process of disaster recovery planning are all explained in [5] where the implementation of the Fuzzy Cognitive Maps (FCM) is included and which form a structured graph for capturing the complex relationships between the disaster recovery plan for IT systems. Also, FCM provides facilities and improving methods to understand systems and their associated risks. The FCM model can be used to identify and perform risk analysis that may arise for a given organization.

In [9], a multilocation recovery model from a selected economic theory is proposed. The recovery model has two main sectors: internal and external sectors. These sectors need information to sort out the transactions and time for determining the location of the transactions. The transaction level can be simple, compound and complex. Moreover, the friction and uncertainty are also studied in [9] where they are prevented from completing the transactions. The friction occurs in five categories: communication, engineering, information, procedure and political action. These categories represent a set of areas that need recovery. Multilocational recovery studies can lower the friction cost, and can proceed a better understanding of a general recovery model in different geographical spaces.

In [3], the diversification problems of storage subsystem structure, infrastructure and security backup problems are all tackled. This paper suggests the technology of disaster recovery backup that is based on a virtual network storage research, which could solve the previous problems and protect the backup data by using the transparent encryption mechanism. Additionally, a double live cloud computing data center is produced in [3] by using the Net App 3250 double live disaster Metro storage technology Cluster. Consequently, when any fault occurs, another main memory will rapidly and automatically take over the business in order to achieve continuity.

In [4], the researchers propose the enriched multi objective optimization model by using the enriched genetic algorithm for an efficient disaster recovery within a cloud computing environment. This paper performs an analysis of massive data storage process, and calculates the data storage cost based on the communication cost, data storage cost and data migration cost through a cloud computing environment. This model could ensure high data storage reliability, reduce small recovery time, and lower the backup cost.

Some factors that influence IT risk management are studied in [10] to assure the organization business continuity. The researchers concern on the risk of disaster recovery center. They utilize several aspects of information theory to derive a mathematical function for IT risk management. Decision support could be implemented in an organization based on particular mathematical equations in order to understand the tiers for the disaster recovery center.

In [11], four different approaches of backup and disaster recovery solutions are introduced. The Amazon Cloud (AWS) uses a mixture of these approaches in order to ensure business continuity. These approaches comprise backup and recovery, pilot light approach, warm standby approach and multi-site approach. The AWS also offers a business continuity with minimum cost. Table 1 summarizes the above discussed studies of disaster recovery models.

TABLE 1. A summary of some researches on disaster recovery

Author	Year	Model	Usage	Results
Mohammadian [5]	2012	Fuzzy cognitive maps for risk prediction	Disaster recovery planning	• Provide facilities to represent complex relationship in implementing a disaster recovery plan. • DR plan can be regularly reviewed, improved and controlled. • Help CIO's and managers to analyze the risks.
Siembieda [9]	2012	Multilocational recovery using analogs from economic theory	Disaster recovery interactions over large geographical areas and over time	• Multilocational recovery can lower friction cost. • Also it can perform a better understanding of recovery in different geographical spaces.
Yu and Yang [3]	2017	Double live cloud computing data center	Cloud-based disaster recovery based on virtual storage	• Solve the traditional data replication existing in two centers that cannot read and write at the same time. • Data availability is more and higher. • Protect data using transparent encryption mechanism. • Lower costs.
Suguna and Suhasini [4]	2015	Enriched multi objective optimization using enriched genetic algorithm	Cloud-based disaster recovery	• Efficient DR in a cloud environment. • This model can guarantee short recovery time, low backup cost and high reliability.
Sembiring and Siregar [10]	2013	IT risk management on disaster recovery center	Decision support in case of risk	• The model will help an organization to decide which Tier of disaster recovery center should be developed based on risk factors. • This model uses mathematical functions for decision support.
Roy [11]	2017	Amazon Web Services Cloud Computing	Cloud-based disaster recovery using 4 types of backup and DR solutions	• The Amazon cloud mixes four approaches of DR and backup. • Ensure business continuity with minimum cost.

3. **Importance of the Disaster Recovery Planning.** Because of the increasing number and intensity of disasters, the organization should take care of designing the disaster recovery planning. This disaster recovery plan is designed to ensure the continuation of business processes in the event that a disaster occurs. It is considered as an important part of the whole business planning to avoid the possible risks that may occur in organizations [1,6]. Some of the above mentioned studies focus on DR planning; for that reason this study emphasizes on the importance of DR planning.

Organizations could not always avoid disasters, but with robust and comprehensive planning, the effect of disaster could be minimized. The disaster recovery planning should be able to determine the recovery strategies either they were cloud-based DR or the traditional ones. In the event of a natural or a man-made disaster, the continued operations of the organization depend on the ability to replicate IT systems and data. The disaster recovery planning provides information on how an organization will prepare for a disaster, what response will be, and what steps it will take to ensure that operations could be restored. As a result, the preparation for continuation and recovery needs to be importantly taken.

The benefits of the disaster recovery plan comprise:

- Minimizes any expected risk.
- Prevents a disaster event from its occurrence.
- Provides data and information security.
- Provides a standard for testing disaster recovery plan.
- Ensures business continuity.
- Reduces the damage cost.
- Assists organizations in minimizing the amount of loss and downtime while simultaneously creating its most effective and fastest chance to recover after a disaster.
- Minimizes decision-making during a disaster.

4. **Cloud-Based Disaster Recovery Strategies.** The traditional disaster recovery involves the cut-over or switch-over recovery systems. An organization has a remote recovery location and backup to preserve the information and technology. This implies that there are two locations: primary data center and separate location that works when the main site fails. The traditional DR can be either dedicated approach or shared approach. In the dedicated approach, the DR site is assigned for one customer, while the shared approach is assigned for multiple customers [12]. The traditional model is expensive, complex and time-consuming because it needs to update the technology continuously, and you need many resources such as hardware, storage devices, bandwidth and manpower. Therefore, the cloud-based DR could reduce the costs that are associated with both the RTO and RPO. The cloud-based systems are more efficient and offer several advantages. In this section, some cloud-based DR strategies for backup and disaster recovery are introduced.

4.1. **Private cloud for DR.** It is only accessible by a single organization, and it provides more privacy, control and more secure. The private cloud computing for disaster recovery is the restoration of data to the IT infrastructure, data need to be reloaded to obtain the system and return it back to its previous state. Additionally, the private cloud can store the backup pertaining to the system off-site. A more common type of the private cloud computing is the virtual private cloud, which is another method for managing a backup. The private cloud provides security for data storage in cloud [2,13]. Figure 1 depicts the private cloud for the DR.

4.2. **Public cloud for DR.** Public cloud is based on the standard cloud computing model in which resources could be efficiently shared. Applications, storage and data run on the same public pool of resources, and available to the general public over the Internet. This
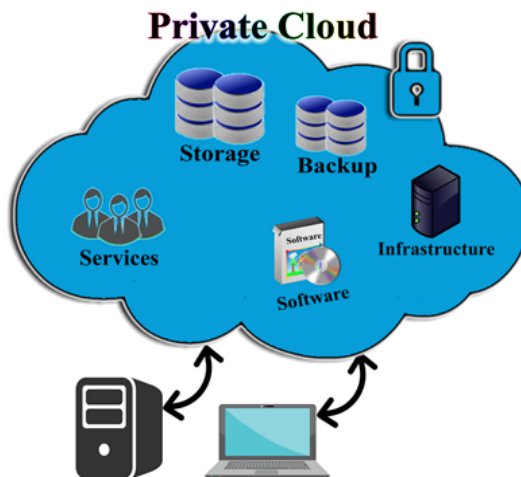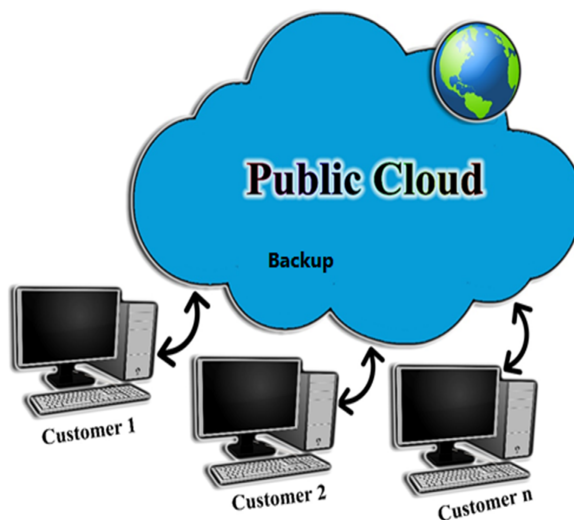
FIGURE 1. Private cloud-based DR

FIGURE 2. The public cloud DR

environment is only suitable for certain public applications, such as e-commerce applications. Customers require that their data could be possibly recovered within a determined time. The public cloud is a great place to set up your backup and DR [2,13]. Figure 2 represents the public cloud for the disaster recovery.

4.3. **Hybrid cloud for DR.** A hybrid cloud is another solution for disaster recovery. It is a composition of at least one public and at least one private cloud computing [14]. Public cloud resources are integrated with private or virtual private cloud to perform distinct functions within the same organization. Hybrid cloud models could be implemented by separate cloud providers for private and public services, or by individual cloud providers for complete hybrid package. Hybrid cloud is flexible and contains a wide range of applications, including backup and disaster recovery [13,15]. Figure 3 introduces the hybrid cloud for the DR.

Table 2 summarizes the main advantages of cloud-based DR.

Regardless of whether your primary systems are in your own premises or on the cloud, it should be ensured that the business continuity is taken into account. The cloud-based DR solution can achieve the reliability, scalability and availability better than the conventional model. Whether or not the system is private, public, hybrid or virtual cloud, there are four main benefits of cloud-based DR [13,16]:

- Lower costs: all resources are shared, and by considering the "pay-as-you-go" system, the cost could be certainly reduced where the company will not have to store many backup tapes.
- Faster recovery: the cloud-based DR can reduce the RTO and RPO from days or weeks to hours or minutes.
- Security: cloud server provider can provide you with more security features in comparison to the conventional model. Different security algorithms could be used for more security.
- Scalability: increasing or decreasing your storage capacity as your business demands are easier than the conventional model.
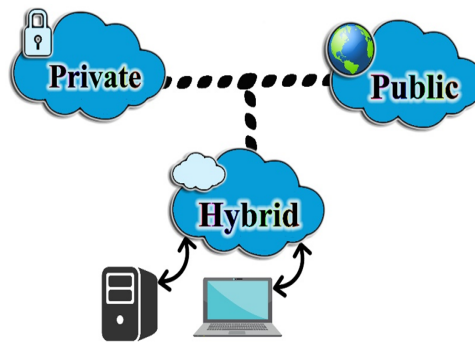

FIGURE 3. Hybrid cloud-based DR

TABLE 2. Cloud-based DR and advantages

Cloud type	Advantages
Private cloud for the disaster recovery	- Lower cost. - Minimize the recovery time, which is the time required to obtain the entire backup of systems and to run after a disaster. - Data is kept safe and secure. - More control. - Scalability and providing automatic scaling to grow. - Data is automatically mirrored in multiple locations. - More compliance.
Public cloud for the disaster recovery	- Ensuring security for long-term backup. - Best utilization of IT resources, there are fewer wasted resources. - It enables scalability. - Financial savings, customer can use "pay-as-you-go" model, or "pay-per usage".
Hybrid cloud for the disaster recovery	- Cost efficiencies. - Simplified disaster recovery management. - Ideal backup where more than one backup could be performed. - Compliance made easily where you can replicate and encrypt the data into your own private network before sending it to the recovery site. - Scalability: IT infrastructure can be able to grow as your business grows. Using the public cloud for backup could be possible, while another work uses a private network.

5. **Conclusion.** The paper concentrates on improving the necessary plans that could avoid and mitigate many different disasters. It has also provided an illustrative study of some models for disaster recovery and their importance in planning and cloud-based DR. Some cloud-based DR strategies are highlighted since they are likely to achieve the reliability, scalability, and availability in a way that is more efficient than the conventional model. Further, a comparison is conducted among the conventional model and the cloud-based models. As a result, it can be shown to be proven that the cloud-based DR is better and easier than the conventional model. Finally, this work could be of a great help for future researchers who might be interested in cloud-based DR and planning.

REFERENCES

[1] E. Maiwald and W. Sieglein, *Security Planning & Disaster Recovery*, McGraw-Hill/Osborne, USA, 2002.

[2] V. Spoorthy, M. Mamatha and B. S. Kumar, A survey on data storage and security in cloud computing, *The International Journal of Computer Science and Mobile Computing*, vol.3, no.6, pp.306-313, 2014.

[3] J. Yu and L. Yang, The cloud technology double live data center information system research and design based on disaster recovery platform, *Procedia Engineering*, vol.174, pp.1356-1370, 2017.

[4] S. Suguna and A. Suhasini, Enriched multi objective optimization model based cloud disaster recovery, *The Karbala International Journal of Modern Science*, vol.1, no.2, pp.122-128, 2015.

[5] M. Mohammadian, Artificial intelligence applications for risk analysis, risk prediction and decision making in disaster recovery planning, in *Artificial Intelligence Applications and Innovations*, L. Iliadis et al. (eds.), Springer, 2012.

[6] B. C. Martin, Disaster recovery plan strategies and processes, *SANS Institute as Part of the Information Security Reading Room*, pp.1-12, 2002.

[7] Z. Yonga, C. Jiea, L. Leia and L. Jina, The design of data disaster recovery of national fundamental geographic information system, *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Suzhou, China, pp.353-356, 2014.

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

[9] W. J. Siembieda, Transactions and friction as concepts to guide disaster recovery policy, *The International Journal of Disaster Risk Science*, vol.3, no.1, pp.38-44, 2012.

[10] J. Sembiring and M. Siregar, A decision model for IT risk management on disaster recovery center in an enterprise architecture model, *Proc. of the 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013)*, pp.1142-1146, 2013.

[11] N. Roy, *Four Approaches Backup Disaster Recovery Explained Using Amazon Cloud*, 2017, https://blog.blazeclan.com/4-approaches-backup-disaster-recovery-explained-amazon-cloud/, accessed on Jan. 25, 2018.

[12] M. Khoshkholghi, A. Abdullah, R. Latip, S. Subramaniam and M. Othman, Disaster recovery in cloud computing: A survey, *Computer and Information Science*, vol.7, no.4, pp.39-54, 2014.

[13] R. Rajan and S. Shanmugapriyaa, Evolution of cloud storage as cloud computing infrastructure service, *The IOSR Journal of Computer Engineering*, vol.1, no.1, pp.38-45, 2012.

[14] A. Dubey, G. Shrivastava and S. Sahu, Security in hybrid cloud, *The Global Journal of Computer Science and Technology Cloud and Distributed*, vol.13, no.2, pp.1-7, 2013.

[15] P. Gapat, S. Khillare, A. Khiste and R. Pise, A survey paper on removal of data duplication in a hybrid cloud, *The International Research Journal of Engineering and Technology*, vol.3, no.1, pp.1327-1332, 2016.

[16] S. Challagidad, S. Dalawai and N. Birje, Efficient and reliable data recovery technique in cloud computing, *Internet of Things and Cloud Computing*, vol.5, no.1, pp.13-18, 2017.