Disaster Recovery in Cloud Computing Systems: An Overview

Abedallah Zaid Abualkishik[1]
College of Computer Information Technology
American University in the Emirates
Dubai, United Arab Emirates

Ali A. Alwan[2]
Department of Computer Science
Kulliyyah of Information and Communication Technology
International Islamic University Malaysia, Selangor, Malaysia

Yonis Gulzar[3]
Department of Management Information Systems
College of Business Administration
King Faisal University
Al-Ahsa, Saudi Arabia

***Abstract*—With the rapid growth of internet technologies, large-scale online services, such as data backup and data recovery are increasingly available. Since these large-scale online services require substantial networking, processing, and storage capacities, it has become a considerable challenge to design equally large-scale computing infrastructures that support these services cost-effectively. In response to this rising demand, cloud computing has been refined during the past decade and turned into a lucrative business for organizations that own large datacenters and offer their computing resources. Undoubtedly cloud computing provides tremendous benefits for data storage backup and data accessibility at a reasonable cost. This paper aims at surveying and analyzing the previous works proposed for disaster recovery in cloud computing. The discussion concentrates on investigating the positive aspects and the limitations of each proposal. Also examined are discussed the current challenges in handling data recovery in the cloud context and the impact of data backup plan on maintaining the data in the event of natural disasters. A summary of the leading research work is provided outlining their weaknesses and limitations in the area of disaster recovery in the cloud computing environment. An in-depth discussion of the current and future trends research in the area of disaster recovery in cloud computing is also offered. Several work research directions that ought to be explored are pointed out as well, which may help researchers to discover and further investigate those problems related to disaster recovery in the cloud environment that have remained unresolved.**

Keywords*—*Cloud computing; data backup; disaster recovery; multi-cloud

I. Introduction

Since its introduction in the commercial sector, cloud computing has undergone a significant change in storing and securing information. With cloud computing, data are run in a collection of nodes including servers and remote computers, which enables users to remotely access the data at any time and from any location. The cloud service providers wish to ensure the delivery of flexible services offered in such a way that keeps users separated from the underlying infrastructure. Cloud computing is important when applied to data recovery due to its flexibility, cost-effectiveness, reliability, and scalability. However, since the internet constitutes an open network for sharing information and conducting transactions, it possesses many security and privacy risks as well as availability issues, particularly for businesses [1,2]. This problem has been addressed using many different approaches including distributed computing, server clustering, and wide-area networking [3].

Small and Medium Business (SMB) corporations are progressively coming to terms with the fact that the cloud service offers many benefits in terms of managing and facilitating their business. They can acquire immediate access to effective business applications and significantly expand their infrastructure resources, all at a minimal expense[4]. Cloud computing is understood as a strategy to enhance existing capabilities and to dynamically introduce new functionalities without investments in different infrastructures, offer training to new employees, and ensure the accreditation of new software packages to expand IT abilities [5]. In today's business environment, the data services operated by CPs encounter many challenges in ensuring a high level of reliability of data services before and after disasters [6]. Data services must ensure reliability and flexibility through an effective and practical DR plan. The data reliability and flexibility are essential requirements for any firm to maintain financial success and sustain the future growth of the organization [6]. The main issue concerning disaster recovery in the cloud computing context is how to provide an effective plan for data backup and recovery that guarantees high data reliability at a reasonable cost prior to a disaster. Thus, a number of solutions have been offered focusing on disaster recovery and data backup in a single-cloud paradigm [6-9].

This paper attempts to highlight and discuss the existing research done on disaster recovery in cloud computing including single and multi-cloud environments. The surveyed studies are thoroughly evaluated to identify the strengths and limitations of each work. Besides, the current and future trends related to disaster recovery in the cloud environment are discussed. In the focus of the discussion are the major issues concerning data backup and recovery in the cloud paradigm.

The remainder of this paper is structured as follows: Section II explains the four categories of disasters that are most likely to occur. In Section III, an overview of disaster recovery is outlined while its different types are explained in Section IV. The discussion covers the three current recovery techniques of cold site recovery, warm site recovery, and hot site recovery. Section V examines the concept of DR in the

This work is fully supported by the Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia

cloud computing context. The research challenges linked to DR in cloud computing are discussed in Section VI. The most noteworthy research done on data DR in cloud computing is reported and discussed in Section VII. Furthermore, a descriptive summary of the related works covered in this survey is given outlining the merits and demerits of each work. Subsequently discussed are the current challenges such as the number of replications, storage cost, and data reliability in a multi-cloud DR process in Section VIII. Moreover, several future work directions deserving to be explored further are included in observations throughout the paper. The research conclusions are presented in the final Section IX.

II. Types of Disaster

Disasters, whether man-made or natural, can result in costly service interruption. For many organizations, adopting cloud computing constitutes the most reliable way of obtaining a dedicated and shared model that can serve DR at low cost and sustain a high speed of access [10-12]. Disaster is defined as any kind of event that leads to critical or devastating damage to a system and results in compromising the availability and the continuity of the system's operations and services for an unknown period. Thus, due to the huge negative impact of any kind of such disaster on the essential services of the system, many businesses, and public services strive to install effective disaster recovery mechanisms that can preserve the sensitive data and decrease the downtime to the minimum level (service disruption). Disasters can be classified into four main classes based on their nature and type, namely climate disaster deliberated and/or intended disruption, damage or loss of utilities and services, and system equipment malfunction. These four types of disasters are further elaborated in Table I.

TABLE I. Disaster Events Categories

Category	Incident Type	Description
Climate disasters	Flood Fire Subsidence and landslides Windstorm Contamination and environmental hazards	• Rapid and uncontrolled increment in water level in a stream, natural or artificial lake, dam, or coastal area. • Fires that cause severe and serious damage in properties can be ignited by inadvertent acts such as lightning, arsonists, smokers, or burning wood or any other inflammable materials. • Natural disasters may occur in certain areas on earth. This includes landslides due to heavy rain or heavy objects falling from high places such as rocks. • Strong winds with high speed that might strike some regions especially in low atmospheric pressure areas like deserts. • The source of this type of natural disaster includes any substances such as chemical, airborne radioactive particles that compromise the surrounding environment and threaten the population, particularly in urban areas. This type of disaster also includes pollution of the air due to the emission of some toxic substances in the event of earthquakes and hurricanes.
Deliberated and/or intended disruption	Arson Labor dispute/ Industrial Action Act of terrorism Act of sabotage	• Arson is a deliberate act of setting fire with the intention of vandalism that causes damage to property such as buildings, bridges, vehicles, and private homes. • When a group of workers are dissatisfied with their work conditions and want to show a form of refusal to perform work through collective action such as demonstration or strike. • This type of disaster comes in a form of threatening others using violence to create fear to accomplish personal, political, or ideological goals. Acts of terrorism do not distinguish between civilians and/or government officials and may target anyone in society. • Deliberate destruction or damage of equipment to hinder a particular group.
Loss of utilities and services	Electrical power failure and Network services breakdown	• This type of disaster encompasses several harmful activities that lead to the interruption of normal electrical power services. Furthermore, a disruption in network services is not considered as an immediate disaster; however, network breakdown is problematic if the outrage negatively affects the ability of the company to provide services to its clients, vendors, and business partners.
Equipment or system failures	Cooling plant failure A/C failure Fire suppression failure Internet failure Equipment failure	• Interruption of the cooling plant that can cause the unavailability of services and facilities. • Interruption of the air conditioning system that can cause the unavailability of services and facilities. • Interruption of fire suppression that can cause the unavailability of services and facilities. • Internal power outage. • Piece of equipment that physically fails in such a way as to impair its availability and performance.

IV. An Overview of Disaster Recovery

DR refers to planning the minimization of data loss and recovery when such losses occur in terms of the expected legal, regulatory, financial, and reputational effects. Regardless of the type of industry, unforeseen events can bring business operations to a standstill and incur extensive financial loss and/or reputational damage to an organization [3, 12-16]. Therefore, a data recovery plan is critical to maintaining continuity by providing all the solutions and steps needed to restore normal operations as soon as possible. Most business organizations throughout the world rely on data to derive competitive advantage and thrive in the marketplace yet give little thought to potential data losses and the consequences thereof. DR is usually the responsibility of the IT department as it is principally concerned with the recovery of computing systems and data after a breach. A breach may be caused by a natural disaster such as a fire, storm, or flood, yet it can also have man-made causes, such as a power outage, malware, data theft, or other malevolent practices. DR preparedness usually requires the implementation of a Disaster Recovery Plan (DRP) so that the steps and procedures to be followed after an incident and can be codified beforehand [8,12, 17-18].

Thus, a DRP constitutes an essential and necessary aspect of any functional enterprise [3, 8, 17-21]. It consists of a set of procedures and predefined policies that attempt to ensure the continuity of the critical business services and sustain the organization's mission by providing the usual services to the target clients during and after the disaster. One of the essential tasks of any effective DRP is to help firms rebuild and restore their system after the failure of their software and hardware components. Unlike fault tolerance that ensures the continuity of the operations due to a failure occurring in one of the system components, DR is more concerned with serious damage and long-term disruption of the business services [8,17, 20]. A DRP intends to manage and maintain the system that is affected by events that have an immediate impact on the availability and the continuity of the services. This includes but is not limited to recovery against cyber-attacks that threaten security, natural disasters, and server outages. A typical disaster recovery plan includes certain steps that ensure the rapid implementation of the DRP to restore the system to its normal state. Many critical parameters should be considered when designing a DRP, which encompasses Critical Business Functions (CBFs), Maximum Acceptable Outage (MAO), Recovery Time Objective (RTO), and Business Impact Analysis (BIA). The most critical parameter in the case of a disaster is CBFs, which include a set of functions very critical in sustaining the business continuity of the services by the organization. Any long-term interruption of these services means that the organization fails to execute its critical operations. There is also a strong relationship between the service disruption and the maximum time that a function can be unavailable without affecting the main mission of the organization, which is called (MAO). Also, to ensure smooth continuity in the organization's service, the maximum time before recovery should be computed accurately. It should be noted that for any DRP the RTOs must be either greater than or equal to the MAO since the RTO represents the timeframe for the recovery process to be completed. Similarly, the BIA represents the risk analysis that examines the CBFs and the MAO in order to determine the impact the function failure has on a business. The BIA can also be used to specify the priority of recovery attempts that need to be accomplished [8,17].

V. Types of Disaster Recovery

The various types of DR upon which others are built include cold site recovery, warm site recovery, and hot site recovery. As shown in Table II, the current technology standards for platform recovery can be implemented using one of the following techniques [3, 7, 17, 22]:

Hot site: Computers are configured and equipped with a list of software and data to accept the production load when the primary server is down. The fail-over is typically (if required) obtained through cluster configuration. The standby cluster configuration is separate and distinguished from the master database configuration.

Warm site: Computer hardware is pre-configured and supplied with a list of software. Once a disaster occurs, the Domain Name System (DNS) is switched and redirected to the backup site, and the server accepts the production load. The services have to be restarted manually.

Cold site: In cold site, the hardware elements of the computer need a set of software associated with a set of data to be generated or restored before promoting the system into a productive state.

Generally, if a disaster occurs at one of the sites, the business is successfully switched to other sites. DR for large-scale hazards usually requires shutting off the power to all utilities and evacuating the facility if required, with the exact tasks to be performed to protect personnel and save lives as identified in the DRP. Many natural disasters, such as flooding or major fires, can cause extensive damage to storage media, in which case specialized and professional data recovery techniques must be used. The physical recovery of data is conducted through different means depending on the extent of the damage, and it may require the use of custom hardware and software recovery systems such as spin-stand data recovery from physically damaged media and data carving [7, 22-23].

TABLE II. Standards Platform Recovery

Option	RTO Coverage	Description	Cost Indication
Hot Site	Minutes (5 min – 4 hrs)	The hot site option needs a high attention level from the administrative staff of the organization. The age of data is dependent on the data recovery strategy.	High
Warm Site	Hours (4 – 24 hrs)	The warm site option denotes that the organization has sufficient resources to recover the system. Nevertheless, some extra work is needed to make it live.	Medium
Cold Site	Days (1 – 7 days)	The cold site needs to reconstruct the system in a way the recovered data is transferred to another location.	Low

Another type of DR concerns the backing up of critical business data into one or more geographically distributed DCs so that there is a very low probability of all the sites being affected at once. An important aspect of DR is information assurance, which is implemented through multiple Network Attached Storage (NAS) and Storage Area Networks (SANs). Information assurance and recoverability can also be ensured using grid computing and cloud storage. The DRP developer considers the cost involved (including an evaluation of the cost of planning against the cause of failure), the optimal facility location, the optimal data allocation units and the method to be followed for data replication. In consequence, autonomous and semi-autonomous remote data backup and recovery processes have proven to be more popular as storage costs have decreased and bandwidth increased.

VI. An Overview of Disaster Recovery in Cloud Computing

A proactive disaster recovery plan constitutes an essential requirement to sustain long-term success for organizations. A set of well-planed measures that system recovery in the case of a disaster is necessary to ensure the continuity of the services and ensure the availability of daily business activities. A well prepared DRP is very beneficial and can be considered as a long-term investment for many organizations. It is disputable, however, if we acknowledge the fact that the immediate impact of the DRP is unclear and its potential benefits may be rejected. However, cloud-based data backup and recovery has become predominant and proven to be a cost-effective strategy compared to other non-cloud-based approaches [7]. In the cloud environment, the idea of virtualization is no longer relevant to the specifications of the hardware on which it runs. This independency between virtualization technology and hardware often means that organizations are able to safely migrate their data, OS, and software tools to the cloud taking into consideration the financial advantages. The performance of the recovery process is considerably influenced by the network bandwidth and the scalability of services. In other words, high network bandwidth with sustainable scalability of services ensures the rapid commencement of the recovery process. After a disaster, all operations can be re-executed again within a few hours according to the compatibility of the IT structure and the cloud-based DR. It is worth noting that most of the data backup and recovery processes are fully automated and requires either minimal or no human intervention [7,24,25, 37 - 38].

The primary importance of utilizing cloud architecture for implementing a DR strategy is the consequent increase in the overall resilience of the organization's processes and applications. Most CSPs use the geographically distributed model of data backup and redundancy so that companies experiencing widespread outages in their networks due to a disaster can recover within a few hours and with minimal disruption [10]. For example, the Amazon cloud stores mission-critical customer applications at multiple geographically dispersed DCs and uses the "fail gracefully" design philosophy. If there is a momentary outage in an application at one location, the customer is notified immediately. The application is then automatically switched to another location while downstream circuit breakers prevent any failure of processes and interfaces that rely on that application [26]. An important concern in DR service delivery is continuity of service to enable applications to come back online very soon after a disaster [3, 15, 18, 21, 25, 27- 28, 37].

There are numerous benefits of adopting disaster recovery in the cloud. Nevertheless, several weaknesses may prevent people from exploiting disaster recovery in the cloud. Table III summarizes the advantages and disadvantages of DR in the cloud [17, 29 - 30,38].

TABLE III. Advantages and Disadvantages of Disaster Recovery in the Cloud

Advantages	Disadvantages
• The arrival and maturity of cloud computing represent a paradigm shift where many of the same functionalities can be shifted to the cloud. • DRPs using cloud architecture are attractive for small and medium-sized enterprises. • Companies can "outsource" their computing requirements and continuity planning to CSPs. • The cloud has a rapid turnaround time with outages lasting no more than a few hours. • In-house personnel can work with the CSP to redirect customers to the cloud during a disaster. The entire process remains transparent to customers worldwide who do not experience the effects from the disruption.	• Customers may be concerned about security and data confidentiality since company data are transferred to a third party. • A company has no control over where its data will be stored. • There have been many incidents of company insiders engaging in malpractice. • Companies become dependent on CSP. The long-term viability of the CSP becomes a source of concern for the company.

VII. Issues and Challenges of Disaster Recovery in the Cloud

Since its adoption by a large number of corporations in the world, cloud computing has become an indispensable element in running the essential business operations for large, medium, and small-scale organizations. This is due to its unique ability to ensure the availability of the services and provide resources that are efficient and reliable while maintaining a reasonable cost. The cloud model relies on the concept of pay-as-you-go, which means the user can request the needed resources from the cloud service provider and be billed according to the used resources. Many service models have been incorporated in cloud computing. This includes but is not limited to Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). Other service models are also provided by the cloud providers, for instance, Database as a Service (DBaaS). Despite the tremendous benefits of cloud computing in running the essential business operations for organizations, some are reluctant to fully adopt the cloud paradigm due to security and privacy issues. Thus, cloud computing has not been fully exploited by many organizations.

A variety of reasons and challenges may prevent many organizations from moving towards disaster recovery planning in cloud computing. In the following, we outline the most critical factors that contribute to rejecting cloud computing [2, 13, 17, 22, 24- 28, 31, 36 - 38]:

Lack of Full Control of Data: Sharing data with cloud providers can result in losing the full control of data. Since the data backup is executed by the cloud service provider, clients may feel concerned about their data dependency with the CPs and the risk of data loss. Hence, it is crucial for these organizations that they select the most reliable service provider who can guarantee the integrity and the privacy of their data. Given these concerns, many organizations may be reluctant to move their businesses on the cloud.

Operation Cost: Operation cost to run the organization's business on the cloud constitutes a critical factor that influences the decision to adopt it. However, the actual cost of running user business on the cloud after switching to a data recovery service is reduced. This reduction in the operating cost may attract many users to adopt the cloud as their preferred platform to run their businesses. The goal of any cloud service provider is to always propose an effective data recovery plan with the least cost. The operating cost of disaster recovery comprises of the following components:

1) Setting up and implementation costs, which denotes the cost of migrating and implementing the organization's business on the cloud. This cost will reduce in the long-term run for the business.

2) Operation cost represents the estimated cost for the daily activities to operate with the data. This includes the operating costs of data storage, transfer, and processing.

3) Disaster costs indicate the total cost of data recovery in the event of a disaster as well as the estimated cost of the damage for unrecoverable disasters. The potential cost of the disaster has a significant impact on the total cost of the services on the cloud.

Speed of Response in Failure Detection: The duration of the time to detect and report to the system failure is very crucial to sustain a high level of availability and reliability. The speed of response to system failure reflects the period in which the system is down and all services are inoperable. Therefore, it is an essential objective for any cloud provider to ensure a fast reaction to the service disruption of the system. However, in certain cases, multiple backup sites are engaged, which makes it difficult to immediately distinguish between service disruption and network failure and take the necessary action for detecting and reporting the problem.

Security: A cyber-terrorist attack is a typical example of a man-made disaster whereby the system resources are attacked for a variety of reasons. Such attacks may cause data corruption and destroy the system. Hence, any form of data protection must ensure a high level of security and rapid data recovery. They constitute the key elements that influence any decision to adopt disaster recovery services.

Replication Latency: The concept of a disaster recovery plan relies on performing data backup through replication. There are two different strategies of data replication that can be utilized, namely synchronous and asynchronous replication strategies. Synchronous replication strategy aims at ensuring a high probability of fulfilling the requirements of the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). Nevertheless, the synchronous replication strategy incurs higher cost than the asynchronous replication strategy, which in turn may negatively affect the system performance. A larger number of tiers in the web application leads to a significant increment in the Round Trip Time (RTT) between the primary site and the backup site. Although the asynchronous replication strategy is cheaper, it does not deliver the same level of quality service for disaster recovery. Thus, organizations should strike a balance between cost and desired performance taking into consideration the requirements of their particular situation. Furthermore, the latency in data replication constitutes a major concern when deciding whether to adopt the cloud as their preferred platform to run the business.

Security of Data Storage: One of the essential benefits of cloud services is that it offers an adequate solution to the issue of data storage. It allows organizations to store their data by providing unlimited space at a reasonable cost. The extensive usage of cloud services leads to a steady increment in the amount of data required for storage. Cloud storage services offer greater flexibility and thus save the budget. Using cloud storage requires less investment than purchasing conventional data storage devices. The architecture of a cloud storage system comprises of four layers, namely physical storage, infrastructure management, application interface, and access. The smooth and reliable running of the applications requires a distributed computing environment that ensures availability, reliability of services, and balancing the workload among all servers. However, data security requires centralized storage in which data are placed in one single storage point. This means that the security of the stored data is at high risk if any failure occurs on the cloud service provider.

Lack of Redundancy: When a disaster occurs on the primary site running the services, the cloud service provider immediately activates the secondary site and redirects the incoming requests and services toward the secondary site to ensure the continuity of the business. Running services on the secondary site will have negative implications on the future data backup process as no replication technique (synchronous or asynchronous) can be performed. Failure in running future data backup due to the outage of the primary site thus increases the risk of data loss since one single local storage (secondary site) is available. However, this issue can be easily resolved once the primary site is restored. Overall, any disaster recovery strategy should provide the best solution possible to ensure the precise assessment of all the potential types of risk and examine their negative implications.

VIII. Solutions of Disaster Recovery in Cloud Computing

This section examines several of the proposed solutions that are relevant to disaster recovery in the cloud computing environment. We attempt to evaluate these solutions by highlighting the merits and limitations of each approach. A summary table given at the end describes some characteristics of the works considered.

The study completed by Pokharel et al. [32] introduces the Geographical Redundancy Approach (GRA) to disaster recovery in the cloud system. GRA is analyzed using the Markov model, and the experiment result shows that it

accomplishes a high availability and survivability while sustaining a low downtime and low cost. However, the proposed approach is not evaluated in terms of measuring the RTO and the RPO that are considered an important measure in evaluating any DR solution. Most importantly, the proposed solution fits only single-cloud systems and may not apply to multi-cloud systems where multiple remote independent clouds are interconnected.

A comprehensive survey is offered by Wood et al. [27] who list the current disaster recovery solutions and practices concentrating on the most critical factors that affect the disaster recovery process. The three categories of disaster recovery mechanisms that are defined are the hot backup site, warm backup site, and cold backup site. The study also discusses the issue of failover and failback that may occur in the event of a disaster, emphasizing on how to restore the control to the primary site and ensure the continuity of the business-critical services.

The study completed by Jian-hua and Nan [33] describes the typical cloud storage architecture that consists of a storage layer, an infrastructure management layer, an application interface layer, and an access layer. It also explains the typical architecture of disaster recovery deployment in the cloud system that manages the cloud storage in the inter-private cloud model. It stores the application data in the server, remotely connected to another set of backup servers distributed over different areas. Each backup server has another two backup servers, the local backup server (LBS) and the remote backup server (RBS). An incremental data backup approach is used to progressively update the data in order to decrease the usage of network bandwidth and accelerate the data backup process. Several enhancements in the service experience lead to reduced data traffic and transmission cost, which includes carrying out data compression and encryption before the data backup process. The model is designed to work in a single-cloud environment that replicates the original data. Creating one single replica is very crucial and increases the risk of data loss particularly in the event of a disaster.

The work introduced by Javaraiah [34] highlights the issue of online data backup in cloud computing systems. The approach concentrates on managing the data backup process on the consumer's premises to reduce cost. The approach is designed to handle complicated issues associated with the online data backup process in the cloud along with DR. Among the critical issues considered is eliminating the dependency on other cloud providers when performing the data backup operation. Various experiments are conducted, and the results have shown that the proposed solution achieves low costs data backup and simplifies the migration process of data from one CP to another. Nevertheless, this work is limited as it focuses exclusively on the issue of data DR in a single-cloud environment and does not address the maintenance of business services during and after a disaster.

Sengupta and Annervaz [31] address the issue of disaster recovery in multi-sites architecture where the data backup resides in multiple distributed locations. Data Distribution Plan for multi-site Disaster Recovery (DDP-DR) is proposed that offers different plans for data distribution based on Protection Level (PL) and Placement Constraint (PC). PL denotes the degree of reliability required by the client against the simultaneous datacenter failures while PC denotes the constraint on some DC locations either to be included or excluded from the list of potential locations for the data backup. DDP-DR derives the optimal plan based on the most critical business and operational factors such as cost of data storage and replication, Recovery Time Objective (RTO), and Recovery Point Objective (RPO). Several experiments are conducted to evaluate the efficiency of the proposed solution in different scenarios. However, the proposed solution does not include computing the network cost for data transmission during the backup process and is limited to one client. In some real-life scenarios, there may be more than one client within the same DR architecture.

Grolinger et al. [35] discuss the problem of disaster data management. They emphasize that most of the current data management solutions designed for disaster recovery lack the integration capabilities in order to minimize the negative impact on user data. The proposed framework called Knowledge as a Service (KaaS) handles the cloud data management process during a disaster. It stores as much as possible from the disaster-related data, thus sustaining the interoperability and the integration of the data. Facilitating data integration relies on using knowledge acquisition and knowledge delivery. Knowledge acquisition includes information extraction and retrieval to develop a sound structure for the disaster data while knowledge delivery is used to integrate information from different data sources and forward it to the target clients. However, the proposed framework is not tested and evaluated empirically in order to determine its efficiency and effectiveness. Moreover, not discussed is the issue of disaster recovery in multi-sites where backup data need to be distributed among several remote locations. Lastly, the proposed solution does not incorporate the issue of deriving the optimal plan for data backup during the disaster.

Saquib et al. [6] proposed a new model named Disaster Recovery as a Service for database applications in cloud computing systems. The proposed model provides a solution for disaster recovery with zero data loss and fast recovery. The proposed model exploits the synchronous technique for data replication to ensure minimum RPO and RTO. However, the study lacks the empirical comparison with other cloud-based disaster recovery solutions that would determine its effectiveness. Moreover, the solution is limited to single cloud systems and may not fit multi-cloud systems.

Satoshi Togawa and Kazuhide Kanenishi [14] introduce a new framework of disaster recovery for e-learning systems that sustain business operations during natural disasters such as earthquakes and tsunami. A prototype that works in a private cloud model is developed based on IaaS architecture. The proposed framework incorporates a distributed storage system to ensure that the framework continues sustaining e-learning services even after the disaster. Several experiments are conducted that prove its effectiveness. However, the work fails to examine the framework in terms of the critical business operational metrics of cost, RTO, and RPO. In addition, it is tailored to work in a single cloud environment

where only one single data backup is performed. Any failure in the backup site may thus result in data loss and long- term service disruption.

Lenk [8] focuses on the issue of data deployment for distributed systems in the event of a disaster. The proposed deployment method utilizes the Cloud Standby Disaster Recovery for warm standby in the cloud and runs on different clouds with many cloud providers. The method enables independent and automated data deployment. The method is tested in several experiments, and the results show that the recovery time is reduced significantly. Nevertheless, the fault-tolerance of the deployment method is not investigated.

Jena and Mohanty [9] investigate the issue of disaster recovery in intercloud systems exploiting the genetic algorithm for resource allocation. The main aim is to provide fast track and balanced mapping procedures for impatient tasks in the cloud system. The proposed approach utilizes the genetic algorithm and Pareto optimal mapping to manage resource allocation while sustaining a high utilization rate of the processors, high throughput, and producing a low carbon footprint. A variety of experiments are conducted to evaluate the performance of the proposed approach. The proposed solution is tested by producing the optimal plan for resource allocation for impatient tasks. Nevertheless, the proposed solution is limited to a single cloud with multiple data centers distributed over many remote locations. Besides, not considered are managing the replication plan to generate a minimum number of data backup without compromising the reliability requirements for the user. Also, the algorithm is not evaluated in terms of Recovery Time Objective and Recovery Point Objective. These two parameters are very essential in the investigation of disaster recovery solutions in cloud computing systems.

Sabbaghi et al. [3] propose a framework formed by integrating five essential types of proven redundancy techniques that have a major impact on the uptime of services in cloud DCs. This work focuses on how disasters can be controlled in a cloud computing DC and how to keep the organization's business running in the event of a disaster. The proposed framework is evaluated through a survey of networking professionals and experts. The results are provided for evaluation but do not include the performance metrics RTO and RPO. Table IV summarizes the previous approaches of DR in the cloud computing environment.

TABLE IV. SUMMARY OF PREVIOUS APPROACHES OF DISASTER RECOVERY IN THE CLOUD

Author and Year	Type of DR Cloud	Scope	CP No.	Parameters	Limitations
Pokharel et al. [32]	Single Cloud	DR	1	Infrastructure cost, Downtime	Did not discuss RTO and RPO
Wood et al.[27]	Single Cloud	DR	1	Cost, RTO, RPO, Performance	Did not provide RTO and RPO analysis to ensure continuity
Jian-hua & Nan [33]	Single Cloud	DR	1	Storage cost	Did not present RTO and RPO analysis; no experimental result
Javaraiah[34]	Single Cloud	DR	1	Infrastructure cost	Did not discuss the parameters RTO and RPO; did not ensure continuity
Sengupta & Annervaz[31]	Single Cloud	DR	1	Storage cost, Protection level, RTO, RPO	The proposed model only considered the case of one customer, single-cloud multiple DCs.
Grolinger et al.[35]	Single Cloud	DR	1	Storage space	Did not discuss data recovery; did not provide the full framework; did not use the performance metrics RTO and RPT to test the framework
Saquib et al.[6]	Single Cloud	DR and BC	1	Infrastructure cost, RTO, RPO	Did not provide performance analysis; did not ensure BC
Togawa & Kanenishi[14]	Single Cloud	DR and BC	1	Migration Time	Did not discuss the parameters RTO and RPO; did not ensure BC
A. Lenk[8]	Single Cloud	DR	1	Cost, Time, RPO	Did not discuss the parameters RTO and RPO
Jena & Mohanty[9]	Single Cloud	DR	1	Cost, Time	Did not discuss the parameters RTO and RPO
Sabbaghi et al.[3]	Single Cloud	DR	1	Cost, Time	Did not discuss the parameters RTO and RPO

IX. DISCUSSION AND FUTURE WORK RECOMMENDATION

This section highlights and discusses the issues and challenges relevant to DR examined in this paper. Also, this section presents the future directions towards DR in cloud computing. Most of today's company services rely on IT systems, some of them being of critical importance to society such as financial services and health care services. Even a very short period of downtime or a very small amount of data loss may result in huge economic losses or social problems. Therefore, most important business and public services use DR mechanism in order to protect their critical data and minimize the downtime caused by catastrophic system faults. Among the types of technologies adopted in DR, systems are asynchronous backup or continuous synchronization of data and preparing standby systems in geographically separated places. During the past decade, cloud computing has emerged as the new service paradigm and is gaining in popularity. A vast number of services are now being built on the cloud platform. These services utilize the resources of a cloud platform with a pay-as-you-go pricing model. The on-demand nature of cloud computing vastly reduces the cost and RTO of

DR whose peak resource demands are much higher than average demands. However, data DR represents a kind of service that possesses the highest data reliability requirements. How to perform data DR service using the cloud computing paradigm to maximize data reliability while reducing cost and RTO still constitutes a challenge. Similar to other computer systems, cloud computing systems also risk dependency, failure detection, security, human-caused damage, natural disasters, and the like. All of these risks may lead to cloud service interruption or even loss of data. To ensure high data reliability, CSPs deploy several data protection strategies. For example, popular distributed storage systems currently used in cloud platforms such as Amazon S3, Google GFS, and Apache HDFS have adopted 3-replicas data redundant mechanism by default. However, in the case of an entire data center failure, data may still be lost. In order to avoid this problem, some CSPs use geographical data dispersion to protect the most critical data, while data centers in distinct locations owned by one CSP use similar software stack, infrastructures purchased in bulk, operation mechanism, and management team. There are still risks of multiple data center failures due to common causes shared across data centers. Also, the number of data centers owned by one CSP is limited. In case some of them become unreachable, the surviving data centers may not apply to customers due to geographical distance, especially in the event of emergency data restoration. Thus, no matter how many preventive measures are being taken, the possibility of data reliability disruption in a cloud cannot be ignored. According to public reports, even the most advanced cloud services have encountered several instances of wide-area outages and the shutting down of public services. Therefore, the best solution for DR service is to utilize multiple data centers from different CSPs. Some researchers focused on how to backup data in a cloud computing environment. Javaraiah [34], for example, introduces online backup and DR and eliminates the dependency on CPs. Sengupta and Annervaz [31] proposed a plan for multi-site DR where backup data can reside in multiple data centers, including the public cloud.

DR in cloud computing has the potential to become a frontrunner in promoting a secure, virtual, and economically viable IT solution in the future. One of the challenges for data management in a cloud environment is how to design a model that tests data storage at low cost, and RTO with high data reliability. Below are summarized the most critical issues relevant to DR in cloud computing that can be observed:

Cloud Data Storage: DR in the cloud possesses potential side effects that affect data availability and data access performance. Moreover, it inevitably reduces the replication level of cloud data, and the location of replicas becomes more important which needs further research focusing on data access performance.

Cost-effective: The cost-effective cloud data storage solution is still at its validation stage, where the approaches provided are based on experimental environments. Therefore, effective solutions are needed to focus on implementing a prototype of the solution in the cloud.

Privacy and Confidentiality: A significant and critical issue is that cloud data storage must guarantee privacy and confidentiality of the data used for DR. Therefore, an effective approach that addresses the issue of privacy and data confidentiality in the cloud data storage is required.

X. Conclusion

This paper has discussed and examined the issue of disaster recovery in the cloud computing environment. An in-depth analysis of the state of the art for DR in cloud computing has been given, together with an overview of the process of disaster recovery for computer systems. The elements of DR in cloud computing have been reported, which includes overview, definition, and types of DR. Also discussed were the details of cloud-based DR analyzed using traditional approaches. In addition, we also identified the main issues and challenges of DR mechanisms that need to be resolved. Several disaster recovery platforms have been described. A comprehensive review of the previous studied of DR in the cloud in both public cloud and privately-owned resources has been conducted. The paper concludes that data DR services must ensure reliability and flexibility through an effective and practical DR plan that constitute vital initiatives for any organization to prosper and sustain growth. Finally, the paper has examined the current trends in the area of disaster recovery in cloud computing and has pointed out future work directions in the field of cloud-based DR to identify the most recent issues and challenges that need to be explored further.

References

[1] Alzain MA, Soh B, Pardede E (2011). MCDB: Using Multi-clouds to Ensure Security in Cloud Computing. 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, Sydney, NSW, Australia.

[2] Tebaa M, Hajji SEL (2014). From Single to Multi-clouds Computing Privacy and Fault Tolerance. IERI Procedia, 10, 112-118.

[3] Sabbaghi F, Mahboubi A, Othman SH (2017). Hybrid Service for Business Contingency Plan and Recovery Service as a Disaster Recovery Framework for Cloud Computing. Journal of Soft Computing and Decision Support Systems, 4(4), 1-10.

[4] Chen D, Zhao H (2012). Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China.

[5] Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A (2011). Cloud computing — The business perspective. Decision Support Systems, 51(1), 176-189.

[6] Saquib Z, Tyagi V, Bokare S, Dongawe S, Dwivedi M, Dwivedi J (2013). A new approach to disaster recovery as a service over cloud for database system. 2013 15th International Conference on Advanced Computing Technologies (ICACT), Rajampet, India.

[7] Suguna S, Suhasini A (2014). Overview of data backup and disaster recovery in cloud. International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India.

[8] Lenk A (2015). Cloud Standby Deployment: A Model-Driven Deployment Method for Disaster Recovery in the Cloud. IEEE 8th International Conference on Cloud Computing, New York, USA.

[9] Jena T, Mohanty J (2016). Disaster recovery services in intercloud using genetic algorithm load balancer. International Journal of Electrical and Computer Engineering (IJECE), 6(4), 1828-1838.

[10] Prazeres A, Lopes E (2013). Disaster Recovery – A Project Planning Case Study in Portugal. Procedia Technology, 9, 795-805.

[11] Matos R, Andrade EC, Maciel P (2014). Evaluation of a disaster recovery solution through fault injection experiments. 2014 IEEE

International Conference on Systems, Man, and Cybernetics (SMC), San Diego, CA, USA.

[12] Andrade E, Nogueira B (2018). Performability Evaluation of a Cloud-Based Disaster Recovery Solution for IT Environments. Journal of Grid Computing, 16(2), 1-19.

[13] Yang P, Kong B, Li J, Lu M (2010). Remote disaster recovery system architecture based on database replication technology. 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering, Chengdu, China.

[14] Togawa S, Kanenishi K (2013). Private Cloud Cooperation Framework of E-Learning Environment for Disaster Recovery. 2013 IEEE International Conference on Systems, Man, and Cybernetics, Manchester, UK.

[15] Chang V (2015). Towards a Big Data system disaster recovery in a Private Cloud. Ad Hoc Networks, 35, 65-82.

[16] Alshammari MM, Alwan AA, Nordin A, Al-Shaikhli IF (2017). Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges. 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), Bahrain.

[17] Alhazmi OH (2016). A Cloud-Based Adaptive Disaster Recovery Optimization Model. Computer and Information Science, 9(2), 58.

[18] Alshammari MM, Alwan AA, Nordin A, Abualkishik AZ (2018). Disaster Recovery with Minimum Replica Plan for Reliability Checking in Multi-Cloud. Procedia computer science, 130(C), 247-254.

[19] Lenk A, Tai S (2014). Cloud Standby: Disaster Recovery of Distributed Systems in the Cloud. New York, USA.

[20] Osama E-T, Munir M, Lela P (2016). Assessing IT disaster recovery plans: The case of publicly listed firms on Abu Dhabi/UAE security exchange. Information and Computer Security, 24(5), 514-533.

[21] Alshammari MM, Alwan AA (2018). Disaster Recovery and Business Continuity of Database Services in Multi-Cloud. International Conference on Computer Applications & Information Security, ICCAIS, Riyadh, Saudi Arabia.

[22] Khoshkholghi MA, Abdullah A, Latip R, Subramaniam S, Othman M (2014). Disaster recovery in cloud computing: A survey. Computer and Information Science, 7(4), 39-54.

[23] Ameigeiras P, Ramos-Muñoz JJ, Schumacher L, Prados-Garzon J, Navarro-Ortiz J, López-Soler JM (2015). Link-level access cloud architecture design based on SDN for 5G networks. IEEE network, 29(2), 24-31.

[24] Chintureena SV (2014). Ensured Availability of resources in a highly reliable mode through Enhanced approaches for Effective Disaster Management in Cloud. International Conference on Electronics and Communication System (ICECS), Coimbatore, India.

[25] Aobing S, Tongkai J, Qiang Y, Song Y (2013). Virtual machine scheduling, motion and disaster recovery model for IaaS cloud computing platform. IEEE Conference Anthology, China.

[26] Jaiswal V, Sen A, Verma A (2014). Integrated Resiliency Planning in Storage Clouds. IEEE Transactions on Network and Service Management, 11(1), 3-14.

[27] Wood T, Cecchet E, Ramakrishnan KK, Shenoy PJ, van der Merwe JE, Venkataramani A (2010). Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges. HotCloud, 10, 8-15.

[28] Liu G, Shen H (2017). Minimum-Cost Cloud Storage Service Across Multiple Cloud Providers. IEEE/ACM Transactions on Networking, 25(4), 2498-2513.

[29] Shi X, Guo K, Lu Y, Chen X (2014). Survey on Data Recovery for Cloud Storage. International Conference on Trustworthy Computing and Services, Beijing, China.

[30] Attiya I, Zhang X (2017). Cloud Computing Technology: Promises and Concerns. International Journal of Computer Applications, 159(9), 32-37.

[31] Sengupta S, Annervaz KM (2012). Planning for Optimal Multi-site Data Distribution for Disaster Recovery. International Workshop on Grid Economics and Business Models, Paphos, Cyprus.

[32] Pokharel M, Lee S, Park JS (2010). Disaster Recovery for System Architecture Using Cloud Computing. 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, Seoul, South Korea.

[33] Jian-hua Z, Nan Z (2011). Cloud Computing-based Data Storage and Disaster Recovery. 2011 International Conference on Future Computer Science and Education, Xi'an, China.

[34] Javaraiah V (2011). Backup for cloud and disaster recovery for consumers and SMBs. 5th IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), Bangalore, India.

[35] Grolinger K, Capretz MAM, Mezghani E, Exposito E (2013). Knowledge as a Service Framework for Disaster Data Management. 2013 Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Hammamet, Tunisia.

[36] Sengupta S, Annervaz KM (2014). Multi-site data distribution for disaster recovery—A planning framework. Future Generation Computer Systems, 41, 53-64.

[37] Mohammad M. Alshammari, Ali A. Alwan, Azlin Nordin, Abedallah Zaid Abualkishik (2020). Data backup and recovery with minimum replica plan in multi-cloud environment. International Journal of Grid and High Performance Computing. 12(2). 201-120.

[38] Mohammad Matar Al-Shammari and Ali A. Alwan. Disaster Recovery and Business Continuity for Database Services in Multi-Cloud. Proceedings of the 1st International Conference on Computer Applications & Information Security (ICCAIS' 2018), 4 – 6 April 2018, Riyadh, Saudi Arabia.