A Review on Cloud-Based Disaster Recovery and Management System

Sahil Rampal[1*], Archie Sinha[1], Amit Kumar Tiwari[1], Syed Asif Akhoon[1]

[1] School of Computer Application, Lovely Professional University Punjab, India
sahil.rampal@gmail.com*, archie23sinha@gmail.com,
amitkumartiwari502@gmail.com, saasif51120@gmail.com

Abstract. Both natural catastrophes and human-created emergencies introduce significant operational disruptions across technological systems. Within information security frameworks, disaster recovery technologies play a vital role in safeguarding data during crisis events. These frameworks encompass diverse methodological approaches and tools designed to help organizations recover after disruptive incidents, highlighting the critical nature of strategic recovery planning. While examining various recovery methodologies in both conventional and cloud environments, this study provides evidence supporting cloud-based solutions are better over traditional approaches. Our review demonstrates that cloud implementations offer enhanced business continuity capabilities, significantly faster recovery periods, and more economical operating costs. This paper introduces an innovative virtual private disaster recovery architecture specifically designed for cloud environments, which researchers have evaluated through industry-centric Recovery Time Objective and Recovery Point Objective measurement criteria. Technology professionals have assessed various frameworks and confirmed its effectiveness in addressing security concerns, meeting business continuity requirements, and enabling swift organizational recovery from disruptions. Additionally, we provide a comprehensive examination of available cloud service offerings and demonstrate the key benefits of implementing recovery management approaches.

Keywords: Cloud Technology, Catastrophe Recovery Management, Data Encryption, Secure Cloud Backup, AI-Driven Disaster Recovery, Multi-Cloud Architecture

1 Introduction

Cloud computing represents a technological framework where distributed resources are shared over the internet. As organizations increasingly incorporate cloud technologies into their core operations, many have begun utilizing these patterns for recovery from a disaster. Cloud recovery functions both as a preventive safeguard and as a protective mechanism through the maintenance of redundant data copies across distributed cloud storage locations. Recovery metrics including RTO and RPO serve as essential perfor-

M. Sharma et al. (eds.), *Proceedings of the Third International Conference on Recent Advances in Computing Sciences (RACS 2025)*, Advances in Intelligent Systems Research 212,
https://doi.org/10.2991/978-94-6239-768-2_13

mance indicators for disaster recovery management. The RTO which is the maximum amount of time a system, application, or service can be down after a failure before it must be restored to avoid unacceptable consequences, while RPO is the maximum amount of data loss (in time) that is acceptable during a disruption [1]. Effective disaster recovery strategies aim to continuously reduce both metrics. Recovery Service in terms of a disaster [1,2] has introduced valuable cloud offering for organizations seeking cost-effective disaster recovery solutions compared to traditional approaches.

Organizations should carefully evaluate DRaaS while developing strategies for recovery or backup of their data. The service allows flexible replication in physical and virtualized environments while supporting rapid recovery with minimal manual intervention. However, security vulnerabilities can originate from the computing environment, network infrastructure, and internet-based communication channels. Therefore, comprehensive security assessment and planning must precede any cloud implementation. Numerous researchers have developed frameworks addressing these security considerations [3,4]. This review contributes to the field in three significant ways: It demonstrates the comparative advantages of cloud-based DR solutions over conventional approaches. It focuses on various frameworks for implementing secure cloud- based disaster recovery. It examines contemporary cloud service offerings with particular attention to disaster recovery applications. The paper is structured as Part II provides a literature review. Part III describes the disaster management life cycle. Part IV categorizes cloud computing service models. Part V examines disaster recovery strategies and the secured virtual private cloud architecture. Part VI analyzes the model. Part VII summarizes the paper.

2 Literature Review

Srinivas, Ramayya, and Venkatesh [2] have investigated disaster-related data loss patterns and backup methodologies for recovery of the data in their study in 2013. Wang et al. in their studies [5] have categorized backup approaches as hot, cool, or warm and demonstrated integration methodologies between DRaaS and business continuity frameworks. Some commercial entities have developed and tested recovery plans on their respective cloud platforms, with particular focus on optimizing RTO and RPO metrics. These publications highlight platform-specific advantages and outline recommended practices for disaster recovery planning and testing. Other studies have focused on comprehensive information collection regarding actions taken during previous disaster management phases to mitigate future risks. The primary objective of such research has been reducing organizational response times by developing deeper understanding of stakeholder involvement in recovery processes, with recommendations for enhanced preparedness across all participating entities. Researchers have also examined the critical role of data centers in maintaining operational continuity. Their work has identified database backup categorization systems, examined recovery technology classifications, and discussed various replication methodologies.

Some studies have proposed innovative approaches of data backup and recovery, such as preventive strategies that optimize replica numbers. The approach used by Y. Meduri [6] recommend specific replication strategies for different backup timeframes, presenting recovery frameworks for multi-cloud environments and testing their recommendations through various scheduling algorithms. By increasing the involvement of many stakeholders in disaster recovery activities, the main objective is to reduce response times. To effectively manage catastrophe recovery, all stakeholders should be well-prepared. This study emphasizes how important the preparedness phase is, which involves quick efforts to reduce fatalities. A prior study by T. Zhu et al. [7] highlighted how important data centers are for maintaining continuous operations. It covered disaster recovery (DR) classification, replication technologies and described the various kinds of database backups, including cold, warm, and hot standby. The study also covered distributed disaster tolerance and highlighted its advantages, including lowering application recovery time goals (RTO), improving business continuity, avoiding single points of failure, and optimizing network traffic loads. M. Alshammari et al. [8] put forward a plan to back up and recover data while cutting down on copies. This plan called the Preventive Disaster Recovery Plan with Minimum Replica (PRPMR), advised keeping one copy for short-term backups (up to a week) and two copies for long-term backups (over a week). The team created and checked their disaster recovery method in a multi-cloud setup using three ways to schedule: COST-first, RTO- first, and a mix of COST/RTO-first. Their approach turned out to be cost-effective bringing down the needed number of copies to less than three.

The Bamboo system introduced by Alwan AA et al. [30] separated system components from the core by using a design based on microkernel technology, allowing dynamic addition, removal, and modification during runtime. However, despite its widely recognized benefits, this approach introduced significant challenges, particularly in facilitating interaction between components developed in different programming languages. Additionally, achieving extensibility requires a deep understanding of programming languages. The Java Adaptive Dynamic Environment (JADE) was created by Alhazmi OH [31] using Java design concepts as inspiration. The lightweight, cross-platform core of JADE facilitates system evolution while the application is running. Nevertheless, despite its flexibility, it did not effectively address the challenges of expanding Collaborative Virtual Environment (CVE) systems. A communication-based solution using IoT technology was presented by Nordin A et al. [32]. The advantage of the proposed approach was that the transmission of data between all devices did not require any existing network infrastructure. In a study, Lenk A, Tai S, and Chang et al. [33,43] presented the Geographic Redundancy Approach (GRA) for cloud systems disaster recovery with the analysis of the Markov model. According to the results, GRA maintained minimal costs and downtime while achieving excellent availability and survival. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) have not however, been used to assess the strategy, which are crucial for assessing any disaster recovery solution. Additionally, the proposed solution is designed for single-cloud systems and may not be suitable for multi-cloud environments, where multiple independent cloud platforms are interconnected. In their review of disaster recovery plans and techniques

Alshammari et al. [34] highlighted the critical factors influencing the healing process. The three main types of disaster recovery procedures are hot backup sites, warm backup sites, and cold backup sites. The study also examined the challenges of failover and failback catastrophe scenarios, emphasizing how important it is to preserve continuity for vital business operations and return to the original location with ease.

Khoshkholghi et al. [35] examined the difficulties associated with online data backup in cloud computing systems, emphasizing cost reduction through on-premises backup management. With a focus on removing dependency on outside cloud providers, the suggested method aimed to tackle complicated problems pertaining to cloud-based data backup and disaster recovery (DR). According to the authors, this technology streamlined data migration between cloud providers and successfully reduced backup expenses. Nevertheless, the study only looked at disaster recovery in single-cloud settings and ignored the need to continue operating a business during or following a disaster. One important factor is the cost-benefits of cloud-based disaster recovery. Scalability of the service and network bandwidth have a significant impact on the effectiveness of the recovery process; in other words, a high-bandwidth network and scalable services enable a faster recovery process. Depending on how well the cloud-based disaster recovery system works with the IT infrastructure, operations can typically resume within a few hours after a disaster. The majority of data backup and recovery procedures are now completely automated, requiring little to no human intervention [15, 24, 25, 36–37].

Sengupta and Annervaz [16, 38] introduced the Data Distribution Plan for multi-site disaster recovery (DDP-DR), which enabled backup data to be stored across different data centers, including shared cloud facilities. Before determining the optimal data distribution idea, the approach took into account customer policy constraints and infrastructure limitations. This method was particularly effective for safeguarding critical business data by distributing backups across geographically diverse and data-centric areas. Usage of knowledge acquisition and delivery to simplify the integration process was proposed by Grolinger, Capretz, Mezghani, and Exposito [39]. However, the design phase for Disaster Cloud Data Management (Disaster-CDM) is still a work in progress. So far, most of the research has focused on acquiring simulated data, while other areas remain underdeveloped. One of the main challenges in delivering knowledge is achieving semantic integration across diverse data sources. An important outcome of this approach is the creation of Knowledge as a Service (KaaS). In the same way, Togawa and Kanenishi [40] introduced a framework of disaster recovery using Moodle e-learning model. Their research focused on the potential impact of a high-level natural catastrophe like an earthquake which is likely to hit Japan in the next 30 years. They emphasized the importance of having a disaster recovery plan in place of e- learning. While they presented findings on their proposed framework, their evaluation did not consider key performance criteria such as cost, time of recovery objective or point of recovery objective.

Saquib et al. [41,16] proposed a cloud-based disaster recovery (DR) solution for database applications, designed to ensure fast recovery and prevent data loss. Their approach achieved a zero Recovery Point Objective (RPO) and minimal Recovery Time Objective (RTO) by utilizing a database server, iSCSI-based synchronous and semi-synchronous block replication, along with automated failover and failback. The scalability of their solution made it a cost-effective option for Disaster Recovery as a Service (DRaaS). Gu et al. [42] proposed a multi-cloud disaster recovery model that consolidates access to various cloud providers via a single interface. However, their research did not address how data operations and service reliability would be maintained during or after catastrophic events such as cyberattacks, natural disasters, or infrastructure failures.

A study comparing cloud storage management was conducted by Sakhardande et al. [44] with traditional non-cloud storage, focusing on biomedical scientists as users. The aim was to find ways to improve competence and accuracy. They discovered that job failures, file size, and network latency were essential elements that adversely affected performance. To assess these impacts, they conducted experiments while applying Organizational Sustainability Modeling (OSM) to ensure fair comparisons. However, the study had some limitations—it only considered a Single Cloud environment and did not evaluate service performance during or after a disaster. Sambrani and Rajashekarappa [45] focused on the role of security in data retrieval. They initiated an algorithm designed to achieve some key objectives: delivering the maximum security for cloud users and guaranteeing data recovery following a natural disaster. Along with this, the study also took into account factors such as data integrity, cost, recovery time, and overall efficiency. To evaluate their approach, they conducted experiments using two primary performance metrics: Recovery Time Objective (RTO) and cost.

3 Disaster Management Cycle

In organizational contexts, a disaster represents an unexpected catastrophic event causing significant disruption to normal operations and potentially resulting in substantial losses. As depicted in Figure 1, organizations must implement comprehensive disaster recovery planning, which requires understanding the complete disaster cycle. The disaster management process encompasses four interconnected phases [9,10].

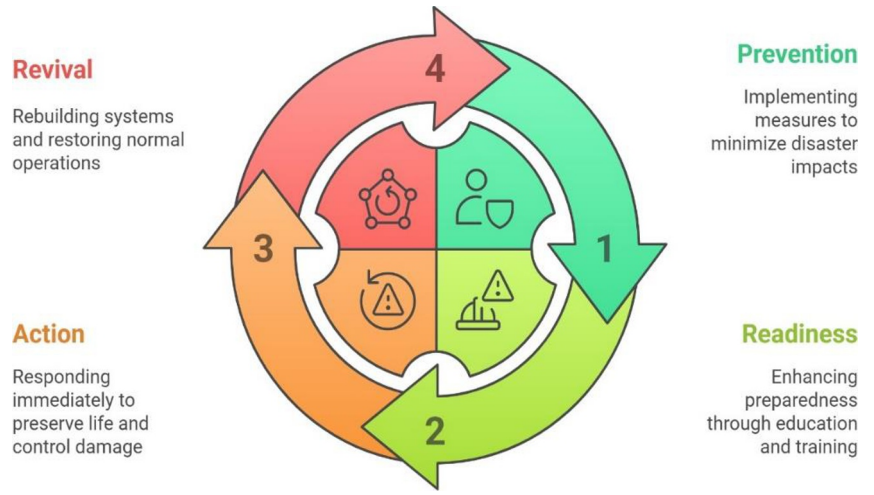

Fig. 1. Disaster Management Cycle

Prevention: This stage involves implementing measures to eliminate or minimize vulnerability to disaster impacts, including potential injuries, fatalities, and property damage. This includes strengthening infrastructure to withstand specific natural hazards. Effective prevention requires organizing resources, conducting thorough risk assessments, producing protective plans, documenting comprehensive plans, as well as establishing implementation and evaluation protocols. Through strategic prevention planning, decision-makers can leverage reliable danger evaluation and risk management data to systematically reduce exposure in the future.

Readiness: This phase encompasses initiatives that enhance disaster preparedness for organizations and business communities. These programs focus on understanding potential impacts and developing appropriate educational resources, outreach programs, and training initiatives to support effective response and recovery. Comprehensive disaster preparedness requires considering worst-case scenarios and developing appropriate organizational response capabilities.

Action: This stage addresses immediate response following a disaster, including preservation of life and addressing humanitarian needs. Organizations must attempt to control and limit damage while coordinating appropriate emergency assistance. Following initial response activities, organizations enter the resumption phase, which represents the transition from emergency response to service restoration.

Revival: This phase involves comprehensive rebuilding of affected systems and emphasizes returning to normal operations. Recovery primarily focuses on restoring less time- sensitive organizational functions and encompasses both activities like long and short. Short recovery typically involves providing quick services to business operations, while long recovery describes the comprehensive rebuilding of organizational

capabilities and infrastructure. All of these combines to form the management of disaster-based recovery using cloud technologies and expertise.

4 Cloud Computing Service Models

Cloud Computing products are designed to meet diverse end user requirements. Service providers offer various solutions to customers with the principal offerings including [11,12]:

Infrastructure as a Service (IaaS): This category provides computing hardware components, including system and storage, networking equipment, virtual, IP addresses, and operational work. It offers organizations access to computing infrastructure while reducing capital expenditures. Major providers in this category include Amazon Web Services, Microsoft Azure, and Google Cloud.

Platform as a Service (PaaS): This offering gives cloud-based development platforms and environments for application creation and deployment. It includes additional components such as systems like database, analysis tools, and intelligent business capabilities. These services are used remotely and accessible via internet connections. Examples include Google App Engine and Red Hat OpenShift.

Software as a Service (SaaS): This widely adopted service category which provides remote access to software applications and features through internet connections. Common examples include Facebook, Dropbox, Salesforce, Microsoft Office 365, and Tableau.

Disaster Recovery as a Service (DRaaS): This specialized offering helps organizations protect applications and data from disaster impacts, whether from security breaches or environmental events. Examples include Zerto, Axcient and iland DRaasS. These service categories continue expanding as cloud adoption increases, allowing organizations to select appropriate solutions based on specific workload requirements and desired outcomes.

IaaS enhances business continuity capabilities, while PaaS supports recovery planning through various methodological approaches. DRaaS provides comprehensive recovery solutions ensuring technology availability for business operations.

4.1 STRATEGIES OF DISASTER RECOVERY

Cloud-based disaster recovery enables remote system backup and restoration while reducing costs associated with recovery metrics. Research indicates that cloud-based approaches offer greater effectiveness and numerous advantages that organizations should consider when establishing disaster recovery strategies. Cloud environments are typi-

cally categorized as private, public, community, or hybrid each with specific characteristics [13,14] as discussed in the following section.

5 Disaster Recovery Strategies

For disaster recovery purposes, private cloud implementations involve restoring data to organizational infrastructure, as system recovery requires data restoration to previous operational states.

Public cloud represents another implementation category, characterized by efficient resource sharing that optimizes technology asset utilization. In this model, applications, storage, and data operate on shared resource pools accessible to general users through internet connections [18,19]. Public clouds provide suitable environments for organizational backup and recovery implementations, offering cost efficiency and high availability.

Community clouds are managed by and distributed among specific firms with common goals and information needs. Group participants share access to cloud-based resources and applications. These implementations enhance user experiences and facilitate communication while incorporating disaster recovery capabilities that ensure business continuity at reduced operational costs [20].

Hybrid clouds combine more than two cloud types to do different roles in the same organization. This approach integrates shared cloud resources with internet, remote private, or collaborative clouds [21,22]. Hybrid implementations are highly adaptable and encompass various services and applications, including comprehensive backup and recovery solutions.

Virtual private cloud is isolated private cloud hosted within a public cloud offers enhanced durability and security can be one of the best options for disaster recovery [46]. Multi-tenant private cloud architectures can reduce expenses through hardware slice purchasing and isolation techniques. Disaster recovery frameworks typically incorporate multiple recovery levels, including system and application layers [23]. These levels are established according to specific system requirements as shown in Table 1.

Table 1. Data Tiers

DR level	System Needs
Data level	Protection of app data
System level	Minimizing recovery time to the greatest extent feasible.
Application level	Application continuation

Replication represents a critical component of disaster recovery implementations. Data must be distributed across multiple geographic regions, utilizing various concurrent

backup repositories from different service providers. Replication methodologies can be either synchronous or asynchronous, with synchronous approaches potentially reducing recovery metrics through virtual mirroring techniques.

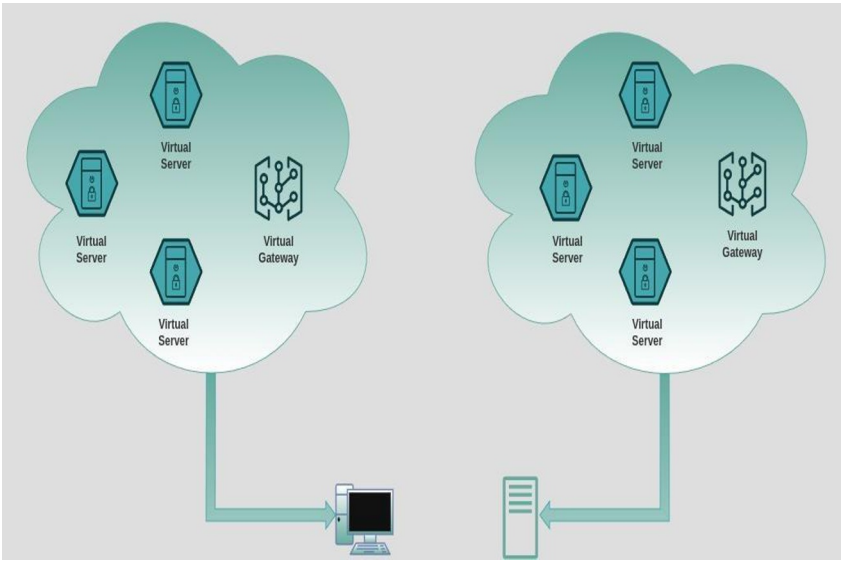

Fig. 2. Virtual Disaster Recovery Management System

As depicted in Figure **2**, asynchronous replication provides backup capabilities across various locations. During disaster events, primary sites become inaccessible. To ensure operational continuity, the synchronous site must activate first. If this site also experiences failure, additional backup sites must be activated. This architecture is particularly suitable for small to medium enterprises, while larger organizations may benefit from hybrid implementations incorporating our virtual model.

- Benefits of the Virtual Private Cloud for Disaster Management:
- Reduced operational expenses
- Improved recovery metrics
- Enhanced security controls
- Continuous business operations
- Improved scalability and flexibility
- Accelerated recovery capabilities

By this we come to know that disasters come to restoration by using backup techniques like parallel multi-model locations with different cloud owners. The main site becomes unavailable when any catastrophe occurs as well as the first site of backup also gets ruined up. The stimulated site needs to get activated checking the security and the data retrieval levels. Such an architecture is amazing for a small-scaled to large -scaled firms which require multi- model design and structure for the remote users which will accelerate the comeback capabilities even quicker [28,29].

According to the industry research, whether an organization's core systems operate in cloud environments or on-premises, business continuity must remain a priority. Compared to traditional approaches, cloud-based disaster recovery offers numerous significant advantages, including enhanced reliability, improved scalability, and increased availability. While implementations may utilize various cloud types, several key benefits apply across all recovery approaches based on cloud [26,27]:

- Faster Response: Recovery based on cloud services significantly reduces recovery timeframes from days to hours.
- Amount Savings: By leveraging shared resources and minimizing traditional backup infrastructure through consumption-based pricing models, cloud-based disaster recovery offers improved affordability.
- Resource Preservation: Organizations avoid capital expenditures for establishing dedicated backup data centers, eliminating responsibility for maintaining these facilities.
- Enhanced Security: Advancements in cloud security technologies facilitate services that protect critical data, allowing providers to implement robust security features. Cloud services incorporate various cryptographic algorithms for data protection.
- Greater Flexibility: Organizations gain independence from specific recovery facility locations, as these can dynamically relocate to different global regions within distributed cloud environments.

6 Analysis and Evaluation

The virtual cloud model discussed in this paper offers a modern and flexible alternative to traditional disaster recovery approaches. This section presents an analytical evaluation based on performance, scalability, cost-effectiveness, availability and real-world applicability using insights gathered from professional researchers. This approach creates additional expenses, particularly when organizations upgrade primary systems and servers necessitating corresponding upgrades to recovery infrastructure. The virtual model provides organizations with comprehensive disaster recovery capabilities that protect critical data while minimizing operational costs. This approach ensures robust security, business continuity, and accelerated recovery while addressing limitations associated with traditional recovery methods. By implementing multi-cloud storage architectures, the model improves cost- effectiveness, performance, and security, enabling continuous data accessibility during significant service disruptions. This model aims to provide firms with a dependable recovery plan that uplifts cloud-based solutions for cost-effective data protection. Additionally, it fortifies security, guarantees business continuity, and speeds up recovery, all while addressing the difficulties associated with traditional ways of recovery from a disaster. Even though few drawbacks are the lack of time available and storage concerns.

7 Conclusion

This paper has examined cloud solution implementation for disaster recovery purpose. We have studied the innovative secure virtual private cloud architecture leveraging industry standard recovery metrics to maximize cloud advantages. This model employs data duplication to enhance storage capabilities and can utilize multiple parallel locations across different service providers. Our study has demonstrated several cloud-based recovery strategies providing improved information accessibility, cost efficiency, and faster response capabilities compared to traditional approaches. Additionally, we have performed comprehensive study of cloud recovery services, particularly recovery services for disasters, highlighting its suitability for organizational recovery implementations. Our study indicate that cloud-based recovery systems offer significantly greater effectiveness and scalability than conventional approaches.

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.
4. A. Dubey, G. Shrivastava and S. Sahu,‖Security in Hybrid Cloud‖, In *the Global Journal of Computer Science and Technology Cloud and Distrubuted, vol 13, no.2, pp.1-7,3013.*
5. Wang, L.; Harper, E.; Mahindru, R.; Ramasamy, V. Disaster Recovery for Cloud-Hosted Enterprise Applications. In Proceedings of the 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 27 June–2 July 2016.
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 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.
15. 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.
16. 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.
17. Tebaa M, Hajji SEL (2014). From Single to Multi-clouds Computing Privacy and Fault Tolerance. IERI Procedia, 10, 112-118.
18. 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.
19. 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.
20. Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A (2011). Cloud computing — The business perspective. Decision Support Systems, 51(1), 176-189.
21. 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.
22. 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.
23. 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.
24. 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), 1828-183.
25. 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.
26. 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.
27. 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.

28. 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.
29. Chang V (2015). Towards a Big Data system disaster recovery in a Private Cloud. Ad Hoc Networks, 35, 65-82.
30. 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.
31. Alhazmi OH (2016). A Cloud-Based Adaptive Disaster Recovery Optimization Model. Computer and Information Science, 9(2), 58.
32. 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.
33. Lenk A, Tai S (2014). Cloud Standby: Disaster Recovery of Distributed Systems in the Cloud. New York, USA. security exchange. Information and Computer Security, 24(5), 514-533.
34. 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.
35. 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.
36. 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.
37. 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.
38. Sengupta, S., & Annervaz, K. M. (2014). Multi-site data distribution for disaster recovery—A planning framework. Future Generation Computer Systems, 41, 53–64.
39. Grolinger, K., Capretz, M. a M., Mezghani, E., & Exposito, E. (2013). Knowledge as a service framework for disaster data management. Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE, 313–318.
40. 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, 4104–4109.
41. 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), 1–6.
42. Gu, Y., Wang, D., & Liu, C. (2014). DR-Cloud: Multi-Cloud based disaster recovery service. Tsinghua Science and Technology

43. Chang, V. (2015). Towards a Big Data system disaster recovery in a Private Cloud. Ad Hoc Networks, 35, 65–82.
44. Sakhardande, P.; Hanagal, S.; Kulkarni, S. Design of disaster management system using IoT based interconnected network with smart city monitoring. In Proceedings of the International Conference on Internet of Things and Applications (IOTA), Pune, India, 22–24 January 2016.
45. Sambrani, Y., & Rajashekarappa (2016). Efficient Data Backup Mechanism for Cloud Computing, 5(7), 92–95.
46. Hamadah, Siham, and Darah Aqel. "A Proposed Virtual Private Cloud-Based Disaster Recovery Strategy." *2019 International Conference on Computer and Information Sciences (ICCIS)*, IEEE, 2019, pp. 469–473.