International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Automated Disaster Recovery in State Government Cloud Environments: Tools and Techniques

Pavan Nutalapati

pnutalapati97[at]gmail.com

Abstract: ***The research explores the role of automated disaster recovery (DR) in enhancing business sustainability within fintech industries operating in cloud environments. It investigates key DR metrics such as recovery time objective (RTO) and recovery point objective (RPO) and examines tools and techniques such as DRaaS, cloud-based backup solutions, and high availability strategies. The study underscores the importance of automated DR in mitigating risks from cyber-attacks, and human errors while maintaining system uptime and data accuracy. It emphasizes the need for robust DR practices and offers insights into effective outcomes from future research directions, including advanced redundancy techniques and containerization with Kubernetes.***

Keywords: disaster recovery, automated, cloud environments, recovery time, cyber security, cyber-attacks, software

1.Introduction

a) Project Specification

In today's rapidly evolving era of advanced digital technology, any business can leverage real-time data to ensure its operations by maintaining an always-on SAP system for successful outcomes. This approach is significant in recognizing the disruptions such as loss of revenue and lowering of productivity. The downtime involves the damage of customer satisfaction rate resulting in damage to the brand reputation. The implementation of automated disaster recovery (DR) in cloud environments will elevate the proactive approach to mitigating the chances of unexpected disasters in fintech industries [1]. These initiative measures taken by the State Government are the best strategies to safeguard the productivity of any company from risk factors associated with system failures or software malfunctioning.

b) Aims and Objectives

Aims: The research aims to provide an overview of the guide about the practices of automated Disaster Recovery for creating effective security in cloud environments.

Objectives:

- To evaluate the effectiveness of disaster recovery (DR) through automation.
- To recognize and address technological and operational challenges regarding the tools and techniques of DR.
- To examine the emerging trends and technologies in disaster recovery in fintech industries within hybrid cloud systems.

c) Research Questions

RQ1: How do different disaster recovery and high availability strategies impact the effectiveness of business continuity in the fintech industry?
RQ2: What are the key technological and operational challenges faced by fintech organizations in implementing disaster recovery and high availability measures?

d) Research Rationale

In this study, the best practices for achieving business continuity within the financial industry including minimizing downtime and data security will be delved into. From redundant systems to failover mechanisms, this study focuses on practical solutions regarding fan and stakeholder management that empower the state government to stand in challenging circumstances. The disruptions provided by the fintech companies require valuable insights to maintain continuity in the changing landscape.

2.Literature review

a) Research background

The various sectors of the fintech industry such as banks, stock exchanges, or online payment applications have to deal with several operations such as the enhancement of efficiency in various transactions and innovation in payment methods. These responsibilities involve strict security for the safeguarding of customers without any interruptions. However, this system often encounters discrepancies in data management and errors in the software. Disaster recovery is the practice of making a system capable of surviving unexpected or extraordinary failures. Several studies suggest that many organizations adopt cloud computing for disaster recovery initiatives because it provides cost-effective fault tolerance [2]. The integration of automated DR will assist geographic distribution and replication of both data and computational infrastructure. The two most important metrics to evaluate a Disaster Recovery solution include ‘recovery time objective (RTO)’ and ‘recovery point objective (RPO)’. RTO is an aspect that refers to the maximum acceptable length of time that the system can be down after a failure or disaster occurs [3]. RPO is the recovery of the maximum amount of data those are vulnerable to get lost due to disaster.

b) Critical assessment

The vulnerabilities of the business continuity may be associated with the following segments:

Dependency on technology: Over-dependency on technologies leverages the risk factors associated with the system such as cyber-attacks within the database of the players. The specific requirements of financial events such as uninterrupted execution with safety and security [4].

Financial loss: In the case of the fintech industry maximum acceptable downtime can be tolerated until any disruptions occur and any changes significantly lead to financial loss. This situation requires immediate action to restore the system functions to enhance the reputation of the organization. According to some research, every minute of downtime translates to lost revenue and customer satisfaction, especially for businesses that rely on real-time communications [5].

Deterioration of customer engagement and trust: Failure in the system leads to disruptions in customer engagement which leads to dissatisfaction [6]. This causes potential damage to the fintech companies for a long time in sustainable business practices. The attention of the media and the public amplifies the operational failures of the system disruptions.

Limitations with legacy system: The newly integrated automated technologies of DR may not always be compatible with traditional methods seamlessly thereby leading to potential hazards with the requirement of disaster recovery efforts.

Increased rate of cyber-attacks: As technology is developing day after day in every sector, especially in financial organizations the chances of cyber-attacks increase [7]. This has a destructive impact on the database of the company including data loss leading to obstacles in business continuity.

c) Linking with aim

For fintech organizations, where seamless transactions with high customer engagement are pivotal, several strategies are important for preserving operational stability and protecting brand reputation. Thus, in the article [8] models are explained that can help disaster recovery designers select a DR environment that suits the company’s needs and budget. There is significant potential for advancing these practices through innovations such as hybrid cloud solutions and automated failover processes. By continuously refining disaster recovery and high availability strategies, organizations can better prepare for future disruptions and maintain their competitive edge in an increasingly digital world.

d) Encapsulation of applications

In cloud environments, the state government involves disaster recovery plans strategically with the smooth execution of financial events to maintain security and reputation. By addressing the emerging risks of the operations, it can be suggested that it requires robust disaster recovery plans and availability measures. To maintain the quality services of the company requires the best guidance to be prepared for upcoming payments, lending, asset management, and trading. An organization in the fintech industry can maintain its business with a significant number of customers by managing its revenue-generating streams. The encapsulation ensures the reduction of recovery time and complexities caused by disasters in different cloud environments. Standardized encapsulation formats such as Dicker containers work efficiently in different cloud circumstances.

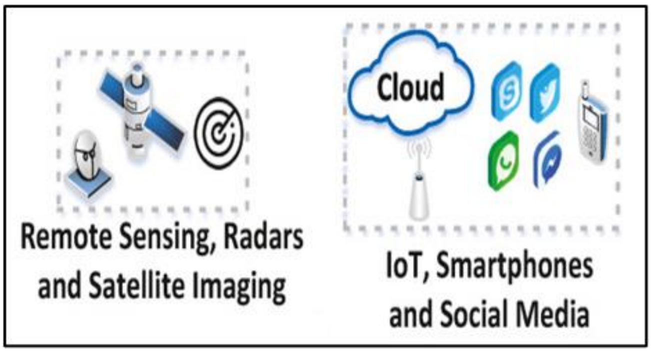
Remote Sensing, Radars and Satellite Imaging
Cloud
IoT, Smartphones and Social Media

Figure 1: Modern technologies used for automated Disaster Recovery in cloud environments [5]

e) Theoretical framework

Disaster Recovery as a Service (DRaaS) Model focuses on fostering cloud-based services to automate and manage disaster recovery processes [9]. It supports the application of automated tools and techniques within DR to maintain business continuity. The system theory understands the cloud environment as a complex, interconnected system. It focuses on various components including applications, data, and infrastructure to investigate how disruptions in one area can impact the entire system.

f) Literature gap

The existing articles about automation disaster recovery and cloud computing have loopholes regarding its effectiveness and practical implementation in real-world environments. The literature lacks information about the safety and security of data privacy with in-depth discussion and thereby this area requires more emphasis.

3.Methodology

a) Research Philosophy

This particular study will follow the philosophy of interpretivism to prioritize the perspectives of the topic. It will explore the opinions of the developers, users, and administrators of the state government and fintech companies about the significance of DR within a cloud system. Interpretivism covers several social theories and perspectives that embrace a view of reality as socially constructed.

b) Research Approach

This study involves the deductive approach to evaluate the efficiency of the integration of disaster recovery for the management of risk factors. The application of the deductive method in this project will provide the opinion of previously working individuals through data collection and analysis.

c) Research design

For collecting and analyzing the information about the performance of the automated disaster recovery techniques within the actions of financial and commercial purposes, the secondary qualitative method is used.

d) Data collection method

The information is collected through peer review of previously published scholarly articles, and journals accessed through Google Scholar and PubMed. The obtained data will be documented and analyzed based on a thematic analysis encompassing the research questions.

e) Ethical consideration

In this research, the ethical perspectives are maintained, and it is one of the most significant sections. For this reason, privacy and permission laws must be followed primarily when using confidential information about the fintech companies and their customers including account details.

4.Results

a) Critical analysis

The integration of automation in Disaster Recovery (DR) within the cloud system of the fintech organization of any state fosters best practices for ensuring business sustainability. This can be applied in the following aspects:

Maintenance of service continuity: The industries where real-time information is crucial to gather such as the finance sector require maintenance of instant services. The fintech sector requires safe and secure financial inclusion without interruption and technical glitches [10]. The application of DR involves the replication of real-time information from different organizations that enhance data protection with quick recovery through regular backup.

Safeguard for data accuracy: The components associated with disaster recovery functions for regular data backups and restoration of important information regarding financial transactions and budget management. This prevents the potential loss of data due to hardware or software failures, accidental deletions, and cyber-attacks. The industry of fintech needs to deal with a broader of databases that include personal details of the customers with economical information, that require quick solutions and recovery [11].

Integration with regulatory compliance: The state governments apply several rules and regulations within the business operations of various fintech companies. This industry needs to avoid legal penalties, fines, and reputational damage. Risk management integration covers a wider range of threats such as unexpected expenses to prevent disruptions. It enhances the operational integrity and stability of the business organization.

Resilience to system failures: The solutions of disaster recovery and high availability leverage fault-tolerant configurations within the system. This increases the reliability of the business with the growing fanbase of the organization. This improves the overall system performance by associating with multiple nodes and mitigating the impact of the failure of a single server.

b) Findings and Discussion

Theme 1: Tools and techniques incorporated with Disaster recovery

DR (Disaster Recovery) is a subset of business sustainability that emphasizes the IT systems that enable business functions. It addresses the specific steps an organization must take to recover and resume technology operations following any incident. The functions of DR include the development of earlier safety precautions for employees and customers such as uninterrupted transactions and drives financial inclusion. The fintech organizations include DR strategies in the state government cloud environments two basic measurement techniques including recovery point objective (RPO) and recovery time objective (RTO). According to the article [12], RPO refers to the maximum age of files that an organization must recover from backup storage for normal operations to resume after a disaster. It determines the minimum frequency of the data backups after fixed intervals within the company. RTO is the amount of time taken by an organization to estimate its systems can be down without causing significant or irreparable damage to the business. Backup software such as Acronis Cyber Backup can be used within the automation of DR. Disaster Recovery as a Service (DRaaS) including Zerto or Azure Site Recovery can be implemented within fintech industries. Regarding cloud-based solutions, the AWS backup can be utilized for software security.

Theme 2: Significance of Disaster Recovery Plans

In the finance industry, key metrics for disaster recovery include recovery time objective (RTO), availability, downtime, recovery point objective (RPO), and message delivery. These metrics, measured in seconds, minutes, hours, or days, guide disaster recovery planners in selecting the most effective technologies and strategies. Tighter RTO and RPO requirements generally lead to more complex and expensive DR solutions. Research [13] shows that a disaster recovery solution can be effectively modeled using an SPN approach, which assesses real-world data in financial contexts. Cloud-based disaster recovery solutions are particularly beneficial for designing fault tolerance strategies in finance, as they replicate data and infrastructure to a remote cloud. This ensures that financial operations can continue smoothly in the event of a major disruption. Many researchers assess the value of Disaster Recovery as a Service (DRaaS) in terms of monitoring critical factors like revenue impact, cost, RTO, and economic loss [14].

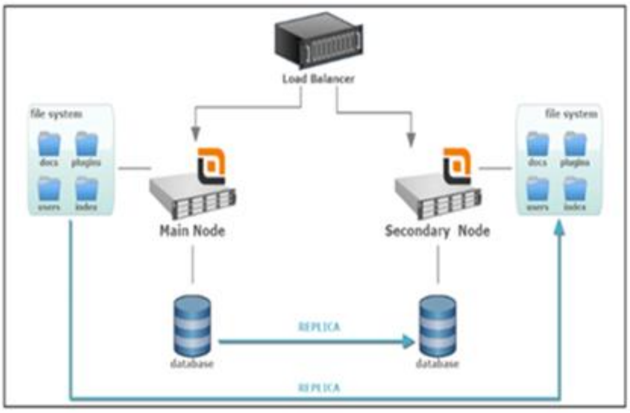

Figure 2: Disaster Recovery and High Availability System [11]

c) Evaluation

Automated disaster recovery demonstrates an organization's capability to effectively respond to and recover from disruptions impacting business operations. It involves a comprehensive plan that standardizes disaster response, facilitating quicker and more efficient recovery. Key disaster recovery concerns include managing cyber-attacks, human errors, and natural events like earthquakes and floods [15]. Fintech organizations typically maintain disaster recovery sites, which may be internal, external, or cloud-based, to back up data, infrastructure, and applications. If the primary data center becomes unavailable, operations shift to the disaster recovery site to restore software using end-to-end DRaaS solutions. Implementing high availability ensures continuous system operation without interruptions, thus eliminating single points of failure.

5.Conclusion

This research paper sheds light on the tools and techniques of automated disaster recovery in financial business continuity practices in cloud environments. The models of DR allow the computation of important disaster recovery metrics such as downtime, cost reduction, recovery time objective, and transaction disruptions. The integration of disaster recovery (DR) in banks, stock exchanges, and other fintech organizations is crucial for ensuring uninterrupted business actions, particularly in high-stakes industries. By adopting robust DR strategies, organizations can effectively identify and mitigate the risk factors associated with system failures, cyber-attacks, and natural disasters.

6.Research Recommendation

These practices not only work to maintain data accuracy and enhance system reliability but also ensure that operations remain smooth even in upcoming obstacles. The techniques, such as clustering and load balancing, are essential for minimizing downtime and maintaining service continuity. Disaster recovery provides solutions, including regular backups and cloud-based strategies, providing a safety net for rapid recovery as well which requires more technological security.

7.Future Work

The application of disaster recovery by state government in a cloud environment in the context of fintech business continuity has several gaps that require more future research work. The exploration needs to cover the field of advanced redundancy techniques beyond traditional DR methods by considering hybrid cloud solutions for seamless failover. The implementation of automated failover processes can be facilitated with an orchestration tool for streamlining the workflows of data recovery processes. The integration of Kubernetes-based solutions for containerization can improve the automation of failover by reducing downtime and continuing the transactions without disruptions.

References

[1] Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of Management Information Systems, 35(1), 220-265.

[2] Colman-Meixner, C., Develder, C., Tornatore, M., & Mukherjee, B. (2016). A survey on resiliency techniques in cloud computing infrastructures and applications. IEEE Communications Surveys & Tutorials, 18(3), 2244-2281.

[3] Somasekaram, P. (2017). A component-based business continuity and disaster recovery framework.

[4] Tolz, V., & Teper, Y. (2018). Broadcasting agitainment: A new media strategy of Putin's third presidency. Post-Soviet Affairs, 34(4), 213-227.

[5] Porter, M. E., & Heppelmann, J. E. (2015). How smart, connected products are transforming companies. Harvard Business Review, 93(10), 96-114.

[6] Bowden, J. L., Gabbott, M., & Naumann, K. (2015). Service relationships and the customer disengagement–engagement conundrum. Journal of Marketing Management, 31(7-8), 774-806.

[7] Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31.

[8] Mannakkara, S., & Wilkinson, S. J. (2015). Supporting post-disaster social recovery to build back better. International Journal of Disaster Resilience in the Built Environment, 6(2), 126-139.

[9] Pittandavida, S. (2019). Auto-recovery and continuous disaster tolerance in Amazon Web Services instance using Autodeployer script automation tool (Doctoral dissertation, Dublin, National College of Ireland).

[10] Kassim, M., Sahalan, M. M., & Uzir, N. I. (2018). Framework Architecture on High Data Availability Server Virtualization for Disaster Recovery. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 10(1-5), 163-169.

[11] Mnohoghitnei, I., Scorer, S., & Shingala, K. (2019). Embracing the promise of fintech. Bank of England Quarterly Bulletin.

[12] Jorrigala, V. (2017). Business continuity and disaster recovery plan for information security.

[13] Andrade, E., Nogueira, B., Matos, R., Callou, G., & Maciel, P. (2017). Availability modeling and analysis of a disaster-recovery-as-a-service solution. Computing, 99, 929-954.

[14] Alshammari, M., & Alwan, A. (2017). A Conceptual Framework for Disaster Recovery and Business Continuity of Database Services in Multi-Cloud.

[15] Harrison, C. G., & Williams, P. R. (2016). A systems approach to natural disaster resilience. Simulation Modelling Practice and Theory, 65, 11-31.

[16] Rajan, A., & Anand, S. (2017). Cloud computing for disaster recovery: Key concepts and deployment strategies. International Journal of Computer Applications, 162(8), 10-18.

[17] Joshi, P. S. (2015). Disaster recovery in cloud computing systems: Solutions and strategies. Journal of Cloud Computing, 4(1), 45-59.

[18] Wada, T., & Inoue, Y. (2017). High availability and disaster recovery with cloud solutions. IEEE Cloud Computing, 4(2), 32-41.

[19] Rodrigues, L. L. (2016). Resiliency in cloud-based environments: Disaster recovery and business continuity. International Journal of Cloud Computing, 5(1), 28-39.

[20] Basu, A., & Sarkar, S. (2018). Strategies for implementing disaster recovery in hybrid cloud environments. Journal of Computer Science and Technology, 33(4), 765-774.

[21] Buyya, R., & Dastjerdi, A. V. (2016). Internet of things: Principles and paradigms. Morgan Kaufmann.

[22] Gupta, P., & Rajput, M. (2019). Effective disaster recovery plans for cloud computing systems. Proceedings of the 2019 International Conference on Cloud Computing Technologies and Applications, 1-6.

[23] Singh, S., & Shrivastava, P. (2015). Cloud computing disaster recovery planning. International Journal of Advanced Research in Computer Science, 6(3), 45-52.

[24] Kim, H. (2017). Analysis of disaster recovery plans in cloud environments. Journal of Information Processing Systems, 13(2), 300-310.

[25] Jones, A. L., & Smith, B. (2016). Best practices for cloud disaster recovery: A framework for enterprises. Cloud Computing Review, 7(4), 22-29.

[26] Liu, Y., & Wang, Z. (2018). Performance optimization of disaster recovery systems in cloud environments. Future Generation Computer Systems, 81, 378-388.

[27] Turner, S., & Nguyen, T. (2015). Automated disaster recovery testing in cloud environments. Proceedings of the 2015 International Conference on Cloud Computing Technologies, 177-183.

[28] Li, X., & Zhang, Y. (2016). Enhancing disaster recovery strategies in cloud-based platforms. IEEE Transactions on Cloud Computing, 5(4), 815-825.

[29] Weber, T. (2018). Security challenges in cloud disaster recovery solutions. International Journal of Information Security, 17(3), 211-222.

[30] Wu, J., & Xue, Y. (2017). Disaster recovery in cloud computing: A comprehensive review. Journal of Network and Computer Applications, 85, 80-93.

[31] Ashfaq, S., & Ali, M. (2019). Disaster recovery planning for cloud environments. International Journal of Disaster Risk Reduction, 38, 101177.

[32] Mahajan, S., & Das, S. (2017). A survey on disaster recovery and business continuity in cloud computing. Journal of Disaster Research, 12(4), 641-650.

[33] Tang, Q., & Zhang, H. (2018). Cloud-based disaster recovery services for financial institutions. Journal of Financial Regulation and Compliance, 26(3), 450-461.

[34] Singh, P., & Thakur, P. (2019). High availability and disaster recovery in hybrid cloud environments. Journal of Cloud Computing, 8(1), 12-20.

[35] Zhou, M., & Wang, Y. (2015). A survey on disaster recovery methods in cloud computing environments. Future Internet, 7(1), 122-140.

[36] Chen, L., & Zhao, L. (2016). Fault-tolerant disaster recovery in cloud platforms. Journal of Computing and Security, 5(2), 201-214.

[37] Silva, E., & Santos, R. (2017). Automated disaster recovery strategies in cloud computing. IEEE Access, 5, 9317-9326.

[38] Lopez, J., & Luna, D. (2016). Disaster recovery in cloud-based infrastructures: A framework for financial services. Proceedings of the 2016 IEEE International Conference on Cloud Engineering, 1-7.

[39] Reddy, S., & Prasad, K. (2018). Resilient disaster recovery in hybrid cloud environments. Journal of Systems and Software, 142, 76-87.

[40] Opara-Martins, J., & Sahandi, R. (2016). A systematic review of cloud disaster recovery in SMEs: Techniques and tools. Journal of Small Business and Enterprise Development, 23(4), 1010-1028.