International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Implementation of Geographically Redundant Disaster Recovery Solutions

Pavan Nutalapati

pnutalapati97[at]gmail.com

Abstract: ***This research study has discussed the importance of disaster management for fintech industry organizations. It has discussed the key components of disaster recovery solutions for fintech industry organizations that are geographically redundant. The discussion part has discussed the benefits of redundant Disaster recovery solutions and the challenges that negatively impact the practical implementation. It has critically discussed the importance of redundant infrastructure and cloud integration including software, network infrastructure and hardware including storage systems, networking equipment and servers. The problem statement has discussed how fintech industries face challenges in handling financial transactions and sensitive and confidential data. It has also discussed that hoe natural calamities negatively impact the timely safe and secure transaction of data. This research study has discussed several possible solutions that can provide fintech industry organizations with a safe and secure way to save their databases from all these threats mentioned here. It has discussed why cloud integration is important to manage disastrous situations and how that can enhance the trust and reliability of fintech companies in front of their clients and consumers. It has discussed data integration technology in the following research study. This research study has discussed some positive impacts of the use of duster recovery solutions. It has discussed optimized data protection, enhanced organizational resilience, cost efficiency, and optimized consumer satisfaction and trust followed by scopes and conclusions.***

Keywords: Cloud data services, Database management, Fintech industry, Cybersecurity, Incident Response, Advanced Persistent Threat

1.Introduction

Geographically redundant disaster recovery comes under the strategies that are intended to involve duplicating critical data in geographically diverse locations to ensure the business community in a disastrous event. DR (Disaster recovery solutions) in geographically redundant areas is known as geo-redundancy where data are located in different regions that are stored in the same data and can take over each other's functions in cases of needs. The physical distance between the data centers is intended to prevent failures caused by disasters, accidents, storms, and any other hazardous conditions. This research study will discuss key components of geographically redundant disaster recovery solutions for fintech industry organizations. It will discuss what problems fintech industry organizations face during natural disasters and calamity. It will critically discuss the importance of cloud integration and redundant infrastructure including software, network infrastructure and hardware including storage systems, networking equipment and servers. This will discuss the benefits of redundant DR solutions and the challenges for implementation.

2.Discussion

Problem Statement

Implementation of the redundant disaster recovery system in the fintech industry organizations involves addressing several unique challenges because of the sensitive nature of financial data, and regulatory requirements that are important for uninterrupted services. Data safety and security, regulatory compliances, latency and performance, cost management, testing and validation, complexity and integration, data consistency and integrity. These are some concerning issues for the management of the disaster recovery management system for fintech industry organizations. Industries that are related to fintech industries are highly sensitive in handling financial transactions, and sensitive and confidential data. This is important to ensure data safety and security from unwanted incidents such as email phishing and unauthorized entry into the database management system. Additionally, natural calamities negatively impact the timely safe and secure transaction of data. This research study will discuss possible solutions that can provide fintech industry organizations with a safe and secure way to save their databases from all these threats mentioned here. It will also discuss the way of implementation strategies so that those organizations can operate their business activities related to their operational management seamlessly.

Solution

Implementation of geographically redundant recovery solutions involves the use of creating strategies that ensure business continuity in case of an event of disaster. Some of the best practices and solutions such as Cybersecurity threat solutions and cloud integration processes have been provided here. These are effective in addressing key challenges with geographically redundant Disaster recovery implementation. Geo redundancy is the distribution of critical components such as multiple data centers, and mission-critical components across different areas in different geographical locations.

Cybersecurity threat solutions

Cybersecurity threats are concerning matters that are specially designed to mitigate and design for ransomware attacks. Fintech industry organizations take service from IT solution service-providing organizations to ensure the safety and security of the systems including regularly updated with the latest security patches and DR sites. Isolation of DR sites to prevent the spread of cyber-attacks primary sites are cybersecurity threat solutions for fintech

industry organizations. Implementation of CDP (Continuous data protection software) to provide real-time data replication to ensure data consistency and the use of blockchain technology to ensure data integrity are some major cybersecurity solutions to deal with the issues related to cybersecurity threats.

Cloud integration

Cloud integration in the implantation of geographically redundant disaster recovery solutions involves to leverage of technologies. This is to ensure the effective and quick recovery of data in the event of a disaster. This approach is used to utilise the scalability, flexibility, and cost-effectiveness of cloud resources to create a DR strategy that will be resilient and less impacted by external factors. Cloud replication helps to do continuous data replication and data backup. Cloud technology ensures fintech industry organizations make an automatic data backup system so that in case of failures and system damage data consistency can be backed up without intervention by manually.

Uses

Implementation of geographically redundant disaster recovery solutions involves setting up processes and systems. This ensures business continuity in the event of a disaster by replicating data and applications across multiple business channels. This also replicates data and applications across multiple geographical locations all over the world. Some detailed guidelines have been provided below about how to implement such solutions in an effective manner.

Assessment and Planning

Accessing requirements of businesses

This is important to identify what data and applications are critical to operations and need to be included in the Disaster recovery (DR) plan. Recovery point objectives (RPO) and recovery time objectives are business requirements for all these critical components.

Analysis of risks

Threat assessment: Evaluation of potential risks such as natural calamities and cyber-attacks from hackers both individually and collaboratively. Analysis of impacts to conduct business impact analysis in order to understand both operational and financial impacts related to the potential disruptions. Choosing the right service and technology providers such as cloud providers that offer robust DR capabilities which is a global network.

Choosing the right technology and service providers

This is important to choose a cloud provider that offers effective and robust disaster recovery capabilities. A global network of data centres and compliances related to industry standards. Consideration of Disaster Recovery as Services (DRaaS) for a totally managed and optimized disaster recovery solution comes under the uses of disaster recovery solution.

Data replication Technology

The data replication technology is related to the choosing between asynchronous and synchronous replication based on RPO and RTO requirements. Uses of cloud storage solutions that offer ample availability and durability. Such Cloud storage management software are Google Cloud Storage, Amazon Cloud Storage and Azure Blob Storage. These can provide data replication services where important data can be stored within the cloud storage. Such options for cloud storage solutions provide huge available options for cloud services.

DR architecture

This is important to ensure that applications are replicated across multiple geographical regions to mitigate to risks of regional disasters. The management of the fintech industry organizations needs to establish their database's serious centers at different locations all across their market operational areas so that cases of failure of data services and data storage in one area can be dealt with within the database management system of that organization. Software designing and IT solution service-providing organizations such as TCS (Tata consultancy service), Deloitte, Capgemini and other big multinational organizations in this segment provide fintech services to banks, Non-banking and other financial service-providing organizations.

Implementation of redundant disaster management solutions involves the effective planning, and choices of robust technologies. Fintech industry organizations can ensure that through all these stages mentioned above can maintain resilience, sustainability and quick recovery from disasters. The management of fintech industry organizations can also protect the confidential data and data and financial information of their clients by the implementation of all these entities discussed above.

Impact

Effective implementation of redundant disaster management solutions for fintech service-providing organizations has a significant positive impact. Enhanced business continuity and optimized business operational management are some positive impacts of the use of disaster Recovery solutions. Optimized organizational resilience to counter sudden changes in marketing patterns and government regulation can be accomplished through the use and implementation of disaster management solutions.

Optimized data protection

Data storage in multiple geographical locations helps to protect intact industry organizations from potential data loss and access of confidential data of clients from unauthorized systems. Data storage in multiple places reduces the chances of disruption in services. Cloud storage

services from Google, Amazon and AZURE Blob provide data replication facilities that safeguard from data loss. In the cloud storage application software data can be saved in cloud memory without the use of system hardware which is relatively safer. Cloud data can only be accessed by limited authorized systems which enhance the safety and security of confidential data of fintech service industry organizations.

Enhanced organizational resilience

Geographically redundant Disaster management service provide an enhanced organizational resilience. It minimizes downtime with DR solutions. Organizations can quickly switch operations to backup site in the disastrous events. Uninterrupted services as well as minimised downtime are some positive impacts that are effective in enhancing the business resilience of fintech companies.

Cost efficiency

Cost efficiency is another positive impact or importance for fintech companies for the use of DR solutions to manage their databases. Disaster recovery solutions provide alternative data backup systems and they need not invest in purchasing new computers and hardware devices for data backup. Additionally, the ability to recover from disastrous situations reduces the potential financial impact of data loss and downtime. Cloud-based disaster recovery solutions offer cost-effective alternatives to traditional DR set-ups through the use of cloud cloud-based data replication and database management systems.

Optimized consumer satisfaction and trust

Disaster recovery services help to improve consumer trust and satisfaction with resuming service during a disaster. Access to services in disastrous situations enhances the credibility of organizations in from of their consumers. Financial services such as financial transactions and access of getting data related to financial services need high data safety and security. Effective disaster recovery management helps to maintain consumer satisfaction and trust as they feel safe. In such scenarios continue their subscription plans.

Stakeholder confidence and engagement

Consumers, venture capital investors, employees and business collaboration partners are stakeholders for fintech organizations. The use of disaster recovery software and data-based management systems helps to fulfill the vested interests of all stakeholders and thus keep stakeholder engagement constant. Business professionals and research scholars opine that if the case if the vested interest of stakeholders is not being fulfilled by the management, then the organization can never accomplish sustainable growth and development.

Optimized data safety and security

Fintech service-providing organizations are intended to provide data related to financial services. The fintech companies have made money transfers from one account and another account easier through the implementation of digital technologies. This is a concerning matter to provide safety and security to consumers. Uses of disaster recovery tools in the database management system now are optimizing data safety and security. This is enhancing the credibility of financial services and fintech industry organizations.

Scope

Network and connectivity, data centers and cloud services, data storage and data replication are related to the technical infrastructure of disaster recovery management. These are related to the implementation of a redundant network within the database management system for fintech companies. Planning related to disaster recovery, testing and validation, Failure and feedback are related to the process and procedures of a disaster management system. Data security such as data encryption, and compliance such as regulatory adherence and audit readiness are related to data security and compliance. Monitoring and reporting, feedback and optimization are related to continuous improvement. Resource management is related to human resource management and financial resources are scopes that are related to the implementation of Redundant disaster recovery. In the process and procedure disaster recovery plan is intended to create a comprehensive disaster recovery plan to outline steps for data failover, replication, recovery and failback. Testing and validation are related to regular DR drills that are used to schedule and perform regular DR drills to test the effectiveness or efficiency of disaster recovery management plans.

3.Conclusion

From the above study, it can be concluded that a Geographically redundant disaster management strategy comes under the activities of disaster management for the organization of all industrial sectors. It has discussed the importance of disaster management for fintech industry organizations. Based on the discussion this can be said that there are some limitations and challenges of disaster management for fintech industry organizations. Data safety and security are the most concerning factors related to the implementation of disaster management systems to manage databases of fintech organizations. Additionally, regulatory compliances, cost management, data consistency and integrity are concerning matters for effective disaster management. This study has also concluded that the use of cloud data services can help to make an alternative source of data storage so that fintech companies can recover their databases in case of disaster or system failure. Although cloud data storage is not fully safe but allocation of different data storage enhances data safety and security from data loss because of malfunction or disastrous conditions. This also can be concluded that optimized data protection, enhancement of organizational resilience, cost efficiency, and increasing consumer trust and satisfaction are some advantages of the use of disaster management systems. An effective disaster management system helps to enhance the stakeholder management system. Effective

disaster management system helps to enhance the trust and credibility of the fintech companies.

References

[1] Khan, M. (2023). Cloud Disaster Recovery: Planning and Implementing Business Continuity. https://osf.io/936kr/download
[2] Abualkishik, A. Z., Alwan, A. A., & Gulzar, Y. (2020). Disaster recovery in cloud computing systems: An overview. International Journal of Advanced Computer Science and Applications, 11(9).https://core.ac.uk/download/pdf/350765431.pdf
[3] Baker, M. C., Witschorik, C. A., Tuch, J. C., Hagey-Espie, W., & Mendiratta, V. B. (2004). Architectures and disaster recovery strategies for survivable telecommunications services. Bell Labs Technical Journal, 9(2), 125-145.
[4] Das, S., Panda, K. G., Sen, D., & Arif, W. (2020). A survey of national disaster communication systems and spectrum allocation-an indian perspective.https://www.researchgate.net/profile/Shrayan-Das/publication/330474867_A_Survey_of_National_Disaster_Communication_Systems_and_Spectrum_Allocation_-_an_Indian_Perspective/links/63d42fe7c97bd76a823f346d/A-Survey-of-National-Disaster-Communication-Systems-and-Spectrum-Allocation-an-Indian-Perspective.pdf
[5] Alshammari, M. M., Alwan, A. A., Nordin, A., & Abualkishik, A. Z. (2021). Data backup and recovery with a minimum replica plan in a multi-cloud environment. In Research Anthology on Privatizing and Securing Data (pp. 794-814). IGI Global. https://www.researchgate.net/profile/Ali-Alwan-8/publication/339599566_Data_Backup_and_Recovery_With_a_Minimum_Replica_Plan_in_a_Multi-Cloud_Environment/links/5e5b466a299bf1bdb847f45f/Data-Backup-and-Recovery-With-a-Minimum-Replica-Plan-in-a-Multi-Cloud-Environment.pdf
[6] Delilah Roque, A., Pijawka, D., & Wutich, A. (2020). The role of social capital in resiliency: Disaster recovery in Puerto Rico. Risk, Hazards & Crisis in Public Policy, 11(2), 204-235. https://www.mdpi.com/2071-1050/13/6/3133/pdf
[7] Wang, W. L., & van de Lindt, J. W. (2021). Quantitative modeling of residential building disaster recovery and effects of pre-and post-event policies. International Journal of Disaster Risk Reduction https://www.sciencedirect.com/science/article/am/pii/S2212420921002259
[8] Upadhyay, A., Mukhuty, S., Kumari, S., Garza-Reyes, J. A., & Shukla, V. (2022). A review of lean and agile management in humanitarian supply chains: analysing the pre-disaster and post-disaster phases and future directions. https://research.brighton.ac.uk/files/13018058/PPC_Revised_Manuscript_Clean_copy_with_Authors_details_Copy.pdf
[9] Farahani, R. Z., Lotfi, M. M., Baghaian, A., Ruiz, R., & Rezapour, S. (2020). Mass casualty management in disaster scene: A systematic review of OR&MS research in humanitarian operations. European Journal of Operational Research
[10] https://eprints.kingston.ac.uk/id/eprint/45189/1/Reza-Z-F-45189-PreProof.pdf
[11] Bethune, E., Buhalis, D., & Miles, L. (2022). Real time response (RTR): Conceptualizing a smart systems approach to destination resilience. Journal of Destination Marketing & Management, https://eprints.bournemouth.ac.uk/36546/7/Real%20Time%20Response%20-%20RTR%20%28002%29.pdf
[12] Fan, C., Zhang, C., Yahja, A., & Mostafavi, A. (2021). Disaster City Digital Twin: A vision for integrating artificial and human intelligence for disaster management. International journal of information management, 56, 102049. https://www.sciencedirect.com/science/article/am/pii/S0268401219302956
[13] Sun, W., Bocchini, P., & Davison, B. D. (2020). Applications of artificial intelligence for disaster management. Natural Hazards, 103(3), 2631-2689. https://drive.google.com/file/d/1AFBYmvF11B96jcDbnlQUc8lW1C7Q9NDq/view
[14] Bixler, R. P., Lieberknecht, K., Atshan, S., Zutz, C. P., Richter, S. M., & Belaire, J. A. (2020). Reframing urban governance for resilience implementation: The role of network closure and other insights from a network approach. Cities, https://lbj.utexas.edu/sites/default/files/Bixler_et_al_2020_Reframing_urban_governance_for_resilience_implementation.pdf
[15] Qadir, Z., Ullah, F., Munawar, H. S., & Al-Turjman, F. (2021). Addressing disasters in smart cities through UAVs path planning and 5G communications: A systematic review. Computer Communications https://www.academia.edu/download/71650163/1_s2.0_S0140366421000116_main_1_.pdf
[16] Parker, D. J. (2020). Disaster resilience–a challenged science. Environmental Hazards, https://www.tandfonline.com/doi/pdf/10.1080/17477891.2019.1694857
[17] Saraereh, O. A., Alsaraira, A., Khan, I., & Uthansakul, P. (2020). Performance evaluation of UAV-enabled LoRa networks for disaster management applications. Sensors, 20(8), 2396. https://www.mdpi.com/1424-8220/20/8/2396/pdf
[18] Esposito, M., Palma, L., Belli, A., Sabbatini, L., & Pierleoni, P. (2022). Recent advances in internet of things solutions for early warning systems: A review
[19] https://www.mdpi.com/1424-8220/22/6/2124/pdf
[20] Munawar, H. S., Qayyum, S., Ullah, F., & Sepasgozar, S. (2020). Big data and its applications in smart real estate and the disaster management life cycle: A systematic analysis. Big Data and Cognitive Computing, 4(2), 4. https://www.mdpi.com/2504-2289/4/2/4/pdf
[21] Kavis, M. J. (2014). Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). Wiley.
[22] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology.

[23] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.
[24] Chandrasekaran, K. (2014). Essentials of Cloud Computing. CRC Press.
[25] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.
[26] Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly, 28(2), 239-251.
[27] Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud Computing: Implementation, Management, and Security. CRC Press.
[28] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599-616.
[29] Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39(1), 47-54.
[30] Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69-73.
[31] Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. Information & Management, 51(5), 497-510.
[32] Voorsluys, W., Broberg, J., & Buyya, R. (Eds.). (2011). Cloud Computing: Principles and Paradigms. Wiley.
[33] Lin, H., & Chen, Y. (2012). Cloud computing as an innovation: Perception, attitude, and adoption. International Journal of Information Management, 32(6), 533-540.
[34] Carlin, S., & Curran, K. (2011). Cloud computing security. International Journal of Ambient Computing and Intelligence, 3(1), 14-19.
[35] Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.
[36] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.
[37] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.
[38] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5.
[39] Marinos, A., & Briscoe, G. (2009). Community cloud computing. Cloud Computing, 5931, 472-484.
[40] Luo, X., & Warkentin, M. (2004). End-user computing: Cloud computing and security challenges. Communications of the ACM, 47(9), 76-82.