ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Review Article

Open Access

An Automated Disaster Recovery Strategies for Fintech Infrastructure

Ankur Mahida

Subject Matter Expert, Barclays, USA

ABSTRACT

This paper aims to present an extensive and well-defined review of the automatic disaster recovery strategies for fintech infrastructure. Since financial operations are gradually relying more on technology, business continuity, and data protection in case of disasters have become fundamental matters. The automation of disaster recovery systems relies on well-designed technologies and methods to reduce downtime, data loss, and financial damage. Organizations are, therefore, able to maintain business continuity and regulatory standards. The article covers AR, deep learning, and AI robotics that will be used for disaster recovery automation. It examines cloud disaster recovery systems' application benefits and deployment considerations, featuring elastic resources, redundancy, and automated failover process. Also, the document surveys the replication set of technologies such as storage level replication, database replication, and file system replication, facilitating real-time cross-site synchronizations. Moreover, the study looks into automated failover operations that detect and execute failure recovery courses, such as load-balancing traffic redirecting to backup sites. In addition, the guide highlights the part played by the operation/automation framework in centralizing control and coordination of disaster recovery processes, linking them with monitoring and alerting systems, and guaranteeing that the recovery methods are properly executed. By looking into the issues, best practices, and consequences of making these automated strategies, this paper hopes to give fintech organizations many valuable hints and practical recommendations about how to improve the level of their disaster management, the amount of lost data, and the continuity of their business in unfamiliar damaging episodic situations.

***Corresponding author**

Ankur Mahida, Subject Matter Expert, Barclays, USA.

Received: May 05, 2023; **Accepted:** May 09, 2023; **Published:** May 19, 2023

Keywords: Disaster Recovery, FinTech Infrastructure, Business Continuity, Data Protection, Cloud Computing, Replication, Failover, Automation

Introduction

The Fintech sector has undergone a real transformation and innovation process spearheaded by digitization and digital integration. Nevertheless, the ties between businesses and technologies have become more complex, allowing malicious actors to exploit technological advantages, resulting in new risks and vulnerabilities. So, disaster recovery planning is a prerequisite for uninterrupted business operations and financial system protection. Disasters can take different shapes, such as natural disasters, cyber-attacks, and breakdown of hardware or human errors, and the resultant consequences can be extremely serious, ranging from prolonged system breakdown and unrecoverable data loss to gigantic cash losses. Old-school disaster recovery processes typically involve manual procedures, which can be slow, mistake-prone, and not precise, causing so much waste of time and resources. To address these challenges, automatic disaster recovery strategies have been dealt with as game changers, which, through the use of sophisticated technologies and processes, have helped to ease the burden of disaster recovery. These strategies have been created to have the least downtime, sustain no data loss, and keep the business running even when the worst disasters happen, making responding to disaster scenarios more efficient and effective.

Problem Statement

Fintech companies and other organizations face many challenges when building a potent disaster recovery plan. The first problem to overcome is the self-evident complexity and many components of their structural environment [1]. Fintech companies tend to depend on a myriad of interoperable systems, software, and services; thus, network recovery planning is more complicated than it is for physical money. This complexity is further increased by maintaining continuity of services and responding to the needs of individuals in different physical locations and managed entities.

Compliance, which includes rigorous regulatory requirements and mandates, is the last and equally significant contender. The financial services industry is subject to a variety of regulations and standards [2]. For example, the level of data security that businesses dealing with payment card processing must adhere to is covered by the Payment Card Industry Data Security Standard (PCI-DSS), the General Data Protection Regulation (GDPR), and numerous banking and financial regulations. An important component of disaster recovery compliance is to ensure that the regulation is complied with during the Providing secure, consistent, and privacy-protected access is crucial to avoid violations and data leaks that can erode trust during disaster recovery operations relief activities to avert any legal liability and reputation damage.

For instance, FinTech businesses exist in a sphere with high availability and low latency operational environment [3]. Some important supply chain factors are instantaneous finance transactions, trading activities, and real-time data processing, which require minimal downtime and response time [3]. Interruption or delay of these missions poses the risk of hefty financial losses and customer dissatisfaction. One of the most critical challenges of disaster recovery is the implementation of strategies that would monitor and achieve strict performance measures.

The next major issue that fintech companies must address is that they are dealing with large amounts of financial data regarded as sensitive. Financial institutions must handle many of their customers' personal data, transaction records, and other sensitive information [4].

FinTech enterprises must address the difficulty of fulfilling RTOs and RPO requirements to resume after a disaster [5]. RTOs stand for the recovery time objective, which needs to be within an acceptable limit of downtime if the operations have to be restored, while RPOs are the recovery point objective, which specifies the limit of data loss that can be tolerated. Along with the fact that FinTech deals with all financial transactions in a short period, and there is a possibility of big money losses, FinTech organizations often have strict RTOs and RPOs, which makes disaster recovery planning even more difficult to complete.

Solution

Solving disaster recovery for fintech companies is often complicated, and automated disaster recovery strategies can usually solve it comprehensively. These approaches use modern technology and techniques to speed up and automate different phases of the post-disaster relief efforts.

An important step is moving disaster recovery solutions to cloud service. Fintech firms can achieve this by implementing automated data replication, failover, and recovery options across various geographic locations using the cloud infrastructure [6]. The elastic and flexible feature of cloud resources allows organizations to dynamically allocate the needed computations, storage, and networking resources for disaster recovery operations. Besides that, cloud providers usually have geo-redundancy and distributed data centers, so they ensure high availability and resistance to local disasters.

While replication technologies are key elements in automated disaster recovery strategies, these technologies provide high-speed data replication and synchronization between multiple sites. So that the data is replicated and up-to-date in second or backup sites. Storage-level replication policies, including SAN replication and object storage replication, will ensure efficient and consistent replication of storage volumes and data objects; at the application level, replication technologies like database and file system replication ensure that the particular applications and their particular data are replicated and synchronized [7]. Minimal data loss and faster recovery times are ensured in this way.

Automated failovers constitute another pillar of the automatic disaster recovery strategy. The failover process is initiated through these measures, including failure and disruption detection [8]. Load balancing and (traffic) redirecting techniques ensure that the incoming queries and traffic are redirected smoothly to other (data center) sites or backup infrastructure. On top of that, automated spin-up of backup infrastructure and services will reduce time and effort for manual intervention, allowing faster recovery and less downtime.

Organizations can use orchestration and automation to facilitate and supervise complex disaster recovery operations [9]. These frameworks are centralized in managing and coordinating disaster recovery operations, but they also automate recovery workflows and runbook execution. Combining these frameworks with monitoring and alerting tools makes them proactive in detecting the risks and initiating recovery processes, which will help boost the efficiency and effectiveness of disaster recovery tactics.

Therefore, by implementing these automated solutions for disaster recovery, organizations in fintech can deal with the issues associated with complicated infrastructure, the implementation of stringent rules and regulations, the need to maintain high availability of services, large data volumes, and stringent recovery objectives. Through these advanced technology and techniques, businesses can eliminate downtime, decrease the risks of data loss, and preserve business continuity, even during disasters or prevention of disruptive events.

Uses

Automating disaster recovery strategies is important for FinTech organizations since they are one of the most critical tools for business continuity and downtime reduction. Financial services are massively dependent on a steady run, and any disruption can cause huge financial loss, customer dissatisfaction, and brand destruction [10]. FinTech companies can recognize and solve incidents via automatic recovery operations. They can switch to the backup systems seamlessly, run the operations again and do not waste the time of the outage.

It is also important to highlight that the FinTech industry lays special emphasis on the safeguarding of primary financial data and the transactions. In order to help with tracking and recovery of data automation are used powered by technologies like duplication and backup of systems which can handle trouble accessed and download large amounts of data like customer information, transaction records, and financial reports [11]. It not only preserves data's validity but also provides confidence in customers and stakeholders, demonstrating the organization's accountability in handling sensitive information.

Having good regulatory compliance is one of the other things that these automated disaster recovery techniques for the FinTech industry deal with. The financial services industry will mainly have to comply with the specific regulations and standards, for instance the Payment Card Industry Data Security Standard (PCI-DSS), the General Data Protection Regulation (GDPR) and various banking and financial policies. Automated disaster recovery strategies are vital to organizations as they ensure that data is always safe, private, and no interruption in the business is possible, even during disruption. Straying away from the regulations results in a stiff fine, legal implications, and the brand’s incurable image damage of desecration.

The automated disaster recovery approach employs automation and modern technologies to shorten the recovery time and reduce data loss [12]. A damage hunter may require a lot of time and be vulnerable to errors, leading to long downtimes and data loss. Automated solutions support quick switchover, data replication, and recovery, reducing the amount of lost data and time to bring the operations to restore. Therefore, this minimizes financial losses and increases a customer's satisfaction and faith in the company.

In addition, automated recovery strategies from disasters lead to improving both the efficiency and scalability of operations in FinTech organizations. Human errors will be minimized via the automation of failover, resource provisioning, and recovery procedures. Organizations can now streamline disaster recovery operations in no time. Moreover, the scalable characteristics of cloud-based disaster recovery systems and the automated resource provisioning let companies expand their recovery infrastructure as required, which helps to maintain operational resilience and business agility.

Impact

Integrating disaster recovery pursuits by automation is significant to fintech businesses in increasing customers' trust and satisfaction. In the finance services industry, customer trust depends on the organization's ability to securely manage customers' data and transactions, whether sensitive or financial [13]. The ability to show customers that the company has a solid and functional business continuity plan helps to reassure them that their transactions and data will be safe even in such disasters. Therefore, the obtained trust level can raise customer satisfaction, loyalty, and total growth.

Automated disaster recovery solutions also bring in the great benefit of saving financial losses during downtime and data loss. Downtime in the fintech industry can create millions of dollars in financial losses, causing no transactions and disrupting operations critical to the company. Automated disaster recovery solutions can quickly restore normal operations by enabling quick failover, data replication, and recovery processes, minimizing disruptions' financial damage [14]. Furthermore, protecting sensitive data and minimizing data loss can solve the problem of regulatory fines, legal consequences, and costly data breaches or recovery practices.

The use of automated disaster recovery strategies, in turn, helps boost operational resilience and improve the competitive position of FinTech companies [15]. With disaster preparedness, organizations can sustain business operations by reducing the impact of disruptions, meeting customer demands, and continuing uninterruptedly in delivering services. This operational resilience can allow fintech enterprises to achieve a competitive advantage by overcoming rivals that do not have strong disaster recovery strategies, resulting in holding the market position and gaining a bigger market share.

There is also automation of disaster recovery strategies that speed up disaster recovery processes and eliminate manual work. The old manual recovery process would be tedious, full of errors, and resource-demanding [16]. Automation solves these issues by replacing failover, replication of data, and recovery procedures with special software, eliminating the need for human intervention and the relationship with human errors. It fosters speed and, at the same time, saves resources, which can then be used to prop up other internal initiatives.

Scope

Automated disaster recovery strategies are very important and can be applied to the various sectors in fintech with different challenges and requirements. In banking and financial services, these strategies are the mainstream of keeping business operations running, for instance, transaction processing, customer account management, and financial reporting. Financial institutions are data custodians who deal with the high level of regulation so they should be very meticulous. That is why, data integrity and regulatory compliance systems along with the trust of the customers is a necessity for the autonomy of disaster recovery automation.

This sphere of automated disaster recovery is essential considering one is to offer efficient payment processing and digital wallet platforms. These automated systems are used to handle a majority of the day-to-day transactional issues on a scale of millions of financial transactions per day, any interruption or down-time would result in serious wealth loss and displeased customers. Automated disaster recovery solutions emplace failover reserves to critically process payments and stand for the highest standards of security and compliance in industries. The solutions protect against transaction delays or loss of data.

Digitalized currency and integration of blockchain apps technology also needs for automatic disaster recovery models. These highly distributed systems usually cope with a great volume of transactions and they keep the data safe. So, what is required is an efficient disaster recovery plan and not only that. In the event of such failures, cloud services can be automated by banking on multiple block chain nodes, data replication, and recovery mechanisms to maintain integrity and continuity of these distributed ledgers.

Disaster planning that involves investment and wealth management applications is one area where the automatic approach is especially important. This data ranges from clients' sensitive financial information, their investment portfolios, and their trading activities – such a disruption can be seen as not a great feat in drama by the clients and the company. Automated disaster recovery solutions will defend the critical data, the operations will be back in business quickly, and regulatory compliance will be maintained even during catastrophic events.

InsurTech, regulatory compliance systems, and disaster recovery strategies are the best places for automation. These systems deal with big customer data, policy information, and regulatory reporting requirements on a routine basis. Automated disaster recovery software can guarantee the continuity of the systems, the security of the confidential data, and compliance with many different insurance and financial regulations, which protect the organization from possible legal and financial liabilities.

Distributed in different FinTech areas, automatized disaster recovery strategies represent a holistic and strong solution that ensures business continuity, data protection, and regulatory compliance. By utilizing futuristic technologies coupled with strong automation frameworks, FinTech companies can avoid downtime data loss and maintain the high resistance required to face disruption or disaster, eventually contributing to their long-term success and happy customers.

Conclusion

Automated disaster recovery approach is the primary factor that would ensure the business continuity, data security, and compliance with the regulations in the drift-prone market of FinTech. Through the use of high-end technologies and automation platforms, fintech companies can shorten periods of downtime, downsize data loss, and maintain robust operational resilience in the case of emergencies. This extensive review addressed the statement of the problem, solutions, uses, implications, and range of autonomous disaster scenarios. It emphasizes the need to implement these techniques in the face of issues such as complex infrastructure, rigid regulation, and availability at all times. In the future, fintech companies will continue to embrace digital transformation and innovative technologies. Archive disaster recovery will be critical in dealing with risks, building customer loyalty, and adding a competitive advantage in the market.

References

1. Tian MW, Wang L, Yan SR, Tian XX, Liu ZQ, et al. (2019) Research on Financial Technology Innovation and Application Based on 5G Network. IEEE Access 7: 138614-138623.
2. Graef I, Prüfer J (2021) Governance of data sharing: A law & economics proposal. Research Policy 50: 104330.
3. Haddad C, Hornuf L (2019) The emergence of the global fintech market: economic and technological determinants. Small Business Economics 53: 81-105.
4. Kakarlapudi PV, Mahmoud QH (2021) A Systematic Review of Blockchain for Consent Management. Healthcare 9: 137.
5. Keyun Ruan (2019) Digital asset valuation and cyber risk measurement: principles of cybernomics. London: Academic Press, An Imprint of Elsevier 1-200.
6. Guo H, Polak P (2021) Artificial Intelligence and Financial Technology FinTech: How AI Is Being Used Under the Pandemic in 2020. The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success 169-186.
7. Liu J, Wang K, Chen F (2019) Reo: Enhancing Reliability and Efficiency of Object-based Flash Caching. IEEE Xplore 39th International Conference on Distributed Computing Systems (ICDCS) 578-588.
8. Anders Lisdorf (2021) Cloud computing basics: a non-technical introduction. New York City: Apress https://www.oreilly.com/library/view/cloud-computing-basics/9781484269213/html/499675_1_En_1_Chapter.xhtml.
9. Leng J, Ye S, Zhou M, Leon Zhao J, Liu Q, et al. (2021) Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. IEEE Transactions on Systems, Man, and Cybernetics: Systems 51: 237-252.
10. Arslanian H, Fischer F (2019) The future of finance: the impact of FinTech, AI, and crypto on financial services. Cham, Switzerland: Palgrave Macmillan https://wbaforum.org/upload/The%20Future%20of%20Finance%20-%20The%20Impact%20of%20FinTech,%20AI,%20and%20Crypto%20on%20Financial%20Services_zsw.pdf.
11. Mendonça J, Andrade E, Endo PT, Lima R (2019) Disaster recovery solutions for IT systems: A Systematic mapping study. Journal of Systems and Software 149: 511-530.
12. Nawari NO, Ravindran S (2019) Blockchain and Building Information Modeling (BIM): Review and Applications in Post-Disaster Recovery. Buildings 9: 149.
13. Ally AM, Dwivedi Y (2020) The state of play of blockchain technology in the financial services sector: A systematic literature review. International Journal of Information Management 54: 102199.
14. Zaid A, Alwan A, Gulzar Y (2020) Disaster Recovery in Cloud Computing Systems: An Overview. International Journal of Advanced Computer Science and Applications 11: 702-710.
15. Chen X, You X, Chang V (2021) FinTech and commercial banks' performance in China: A leap forward or survival of the fittest?. Technological Forecasting and Social Change 166: 120645.
16. Khan A, Gupta S, Gupta SK (2020) Multi-hazard disaster studies: Monitoring, detection, recovery, and management, based on emerging technologies and optimal techniques. International Journal of Disaster Risk Reduction 47: 101642.