International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AUTOMATING DISASTER RECOVERY AND BACKUP STRATEGIES FOR ENHANCED RESILIENCE IN LARGE-SCALE RETAIL IT SYSTEMS

Suresh Gangula[1], Chandrashekar Kola[2], Manoj Kumar Chokkakula[3]

[1]Software Engineer, Nike, Inc. Portland, OR, USA-97229

[2]Sr Systems Engineer, AutoZone Inc. Delaware, OH, USA-43015

[3]Sr Software Engineer, Expedia Group, Seattle, WA, USA- 98119

Abstract

This paper discusses disaster recovery (DR) and automation of backup processes for big retail IT infrastructure, focusing on the significance of the processes towards ensuring operational continuity and data consistency. The review of 41 papers highlights key strategies, including setting backup schedules based on policies, using Infrastructure as Code (IaC) for deployment, automating failover and failback tasks, and incorporating Artificial Intelligence (AI) and Machine Learning (ML) to make backups more efficient. These approaches reduce downtime, improve system redundancy, and simplify recovery processes. In addition, the paper describes how automation can help optimize disaster recovery efficiency and effectiveness, particularly in the advanced retail environments that demand high availability and quick recovery time. The research also examines the issues and limitations of automating DR and backup in big retail IT environments, including scalability problems, real-time processing problems, and integration problems with existing IT infrastructure. It also details the tools and platforms used to facilitate these automated processes, presenting a general overview of the current state of practice and research. By projecting the possibility of automation in disaster recovery, this article provides real-world advice for companies willing to maximize their IT resilience and guarantee ongoing business activities despite interruptions.

Keywords: Disaster Recovery; Backup Strategies; DevOps; Automation; Retail IT Systems; IaC; AI and Machine Learning; Failover and Failback.

1. Introduction

With the rapid pace of retailing in the contemporary world and the high level of interconnectedness characterizing it, the availability of IT systems round-the-clock is indispensable in achieving business continuity, customer confidence, and competitiveness. Retail businesses depend upon sophisticated, large-scale IT infrastructures that manage everything from point-of-sale transactions and inventory control to web ordering and customer relationship management [1, 2]. Due to the size and complexity of these operations, disruption by whatever means, whether through cyberattacks, hardware malfunctions, software bugs, or

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

natural disasters, can lead to substantial financial loss, damage to reputation, and business disruption. Hence, disaster recovery (DR) and backup planning are not best practices or regulatory requirements in isolation; they are included in business continuity planning [3, 4]. Traditional disaster recovery and backup interventions are typically manual and susceptible to human inefficiency and lengthy system recovery times. As retail ecosystems become increasingly intricate, manual approaches are not enough to meet the needs of quick recovery, minimized downtime, and continuous data consistency. Automation is a revolution that can resolve these problems, allowing organizations to automate backup processes, continuously monitor systems in real-time, and recover key operations with minimal human intervention [5, 6]. With automated disaster recovery and backup solutions, retailers can realize improved recovery time objectives (RTO) and recovery point objectives (RPO), enhance compliance with data protection regulations, and improve resiliency against a wide range of threats [7].

Automation in disaster recovery planning means using technologies like cloud backups, orchestration tools, machine learning, and infrastructure as code (IaC) practices. The aforementioned technologies enable the development of innovative, self-recoverable systems that can predict potential failures, start backup processes, and orchestrate failover processes without the involvement of humans. Furthermore, automation enables regular testing of recovery processes to ensure recovery plans work as systems grow and change [10]. This paper outlines the essential role of automated disaster recovery and backup practices in large-scale retail IT infrastructures. It outlines the limitations of traditional methods, defines the leading technologies and frameworks that enable automation, and offers best practices to build solid, efficient, and scalable disaster recovery infrastructures. By embracing automation, retail businesses can shield themselves from disruption and create the foundation for digital innovation and transformation in the future, making customer experience seamless and sustaining growth despite unexpected circumstances.

This paper is organized into five main sections. Section 2 gives a detailed overview of existing research, discussing why disaster recovery and backup are crucial for retail IT systems, how automation helps, important strategies like policy-driven backup scheduling, real-time data replication, IaC, automated failover processes, and the use of AI and ML to improve backups. It also reviews technology tools and platforms supporting automation. Section 3 discusses the challenges and limitations of these methods. Section 4 offers a detailed discussion of their advantages and disadvantages. Finally, Section 5 concludes the paper with key findings and future research directions.

2. Literature Review

2.1. Importance of Disaster Recovery and Backup in Retail IT Systems

In 2015, Yang and others created a combined model using DEMATEL and ANP to evaluate and select modern IT disaster recovery sites. Due to the complexity of the disaster situation and IT growth, recovery site selection nowadays is conducted based on various factors, such as availability, recovery time, and performance. This framework details the most crucial

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

evaluation criteria, defines influence relations, and assigns weights to all criteria. It is a convenient utility for public or private organizations tasked with data center resiliency.

Schätter et al. [12] created a new decision-support methodology 2019 to support Business Continuity Management (BCM) for supply chain risk management, especially under extreme disruptions. This methodology, included in the Reactive Disaster and Supply Chain Risk Decision Support System (ReDRiSS), helps decision-makers when they face uncertainty, complexity, and tight deadlines. It integrates scenario planning, optimization, and decision theory to offer robust resource allocation solutions without complete information.

In 2014, Marshall and Schrank [13] developed a dynamic model of research that examines the neglected role of exogenous, non-normative occurrences like natural disasters in influencing small businesses. Unlike previous research, which is biased to perceive business recovery as one, unified, binary experience, this model positions recovery as an iterative process of repeated iterations. It situates business recovery within a larger model of individual, household, and community resilience across time. The approach provides an integrated framework and lexicon through which to describe the dynamic, adaptive small business recovery process operating in a disaster context.

In 2021, Chatterjee [14] examined the private sector, which is made up of big, medium, small, and micro enterprises, each individual but complementary. However, disaster recovery policy always approaches the sector as a collective since data are scarce, overlooking unique issues that small-scale enterprises encounter. While big and medium enterprises are actively involved in recovery, micro and small enterprises manage risks primarily individually.

Du and Jiang [15] published a paper in 2019 that looks at how a manufacturer can manage their supply to lower the risk of low production in a changing supply chain using multi-agent modeling and reinforcement learning. The manufacturer can choose either to improve reliability or to have a backup strategy. The manufacturer chooses either a reliability improvement or a backup strategy. The outcome indicates that reliability improvement is optimal with fewer immediate consumers, a higher mean yield, and lower yield uncertainty. Conversely, a backup strategy is best under conditions of high uncertainty or many immediate consumers. The supplier's adaptive pricing impacts the manufacturer's optimal strategy and the order decisions.

2.2. Role of Automation in Disaster Recovery and Backup

Nasurudeen et al. [16] 2019 described how machine learning and artificial intelligence can provide cloud backup systems for small businesses with enhanced cost-effectiveness and dependability. The study presumes a seed block algorithm and Rivest-Shamir-Adleman (RSA) encryption-based hybrid strategy to enable secure access and cloud system disaster recovery.

Abieba et al. [17] summarized Infrastructure as Code (IaC) as the secret to enhanced business continuity and disaster recovery of cloud computing in 2019. IaC, which provisions infrastructure using code, improves automation, consistency, and scalability. The study demonstrates how IaC simplifies backup, failover, and restoration processes, thus making

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

operations more robust. It also recognizes IaC's contribution to maintaining essential services while on the move during outages.

Reina and Sanguino [18] introduced a new framework of network management, DRACSC (Device for Automatic Recovery and Configuration of Communication Systems), in 2014 for disaster recovery and short-term configuration of communications devices. DRACSC, with portability, automation, and a repository in the cloud, outshines other tools. It was experimented with by 89 assessors comprising ICT experts and teachers and significantly improved task productivity and user understanding.

Martin [19] emphasized the implementation of Disaster Recovery (DR) and Business Continuity Planning (BCP) to prevent such risks in 2021. It takes into account cloud-based DR systems with Recovery Time and Point Objectives (RTO/RPO), cost, and regulation. In consideration of real case studies and a literature review, research necessitates active, automated, and multi-dimensional solutions in business resilience.

Mehra [20] in 2021 explained the huge need for data backup and replication to minimize data loss, enable quick recovery, and minimize system downtime. Mehra [20] explains the problems organizations encounter in applying efficient data protection, provides best practices, and addresses emerging solutions such as cloud-based solutions and AI-based analytics to enhance resilience in dynamic data environments. Fig. 1 shows the DR and Backup Strategies for Retail IT Systems.

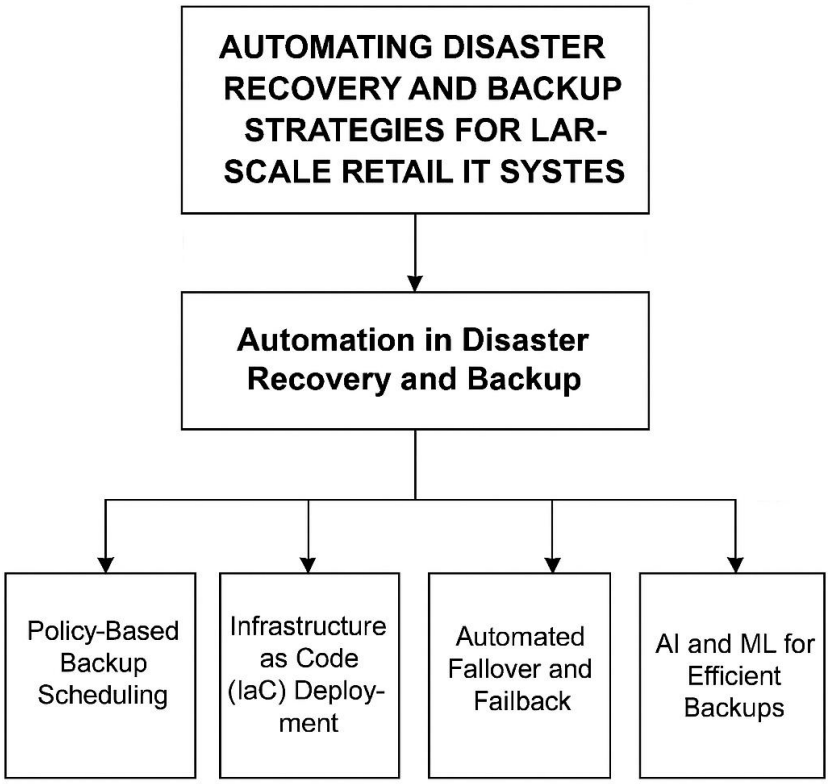

Figure 1: DR and Backup Strategies for Retail IT Systems

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.3. Mechanisms for automating disaster recovery

In 2024, Kim et al. [21] investigated how manufacturing IT managers create effective disaster recovery (DR) plans. The authors conducted interviews with experts from six leading U.S. companies. Braun and Clarke's thematic analysis was used, and five main themes were found: contingency planning, testing, recovery levels, time requirements, and concurrent costs, highlighting the strategic importance of DR planning to avert societal and economic impacts.

Andrade and Nogueira [22] introduced 2020 an auto-disaster recovery mechanism integrating Kubernetes management systems and backup and recovery mechanisms for further data protection within cloud environments. It is efficient in disaster detection and application recovery within 15 seconds, using a standby Kubernetes cluster to achieve less latency and human interaction. It is also employing Long-Short-Term Memory (LSTM) in CPU usage prediction to improve efficient scheduling.

Sartwell [23] applied a Petri net-based disaster recovery (DR) solution model and IoT infrastructure analysis in 2020. Mission-critical applications like health care and traffic monitoring increasingly employ IoT devices, making real-time fault tolerance extremely critical. The existing model considers some of the most significant DR factors, like system availability, recovery time objective (RTO), and cost.

2.3.1. Policy-Driven Backup Scheduling

Syed [24] charted future directions for next-generation disaster recovery in 2024. This process places heavy emphasis on safeguarding data throughout the digital-first era. Transferring the data to two or more cloud providers forms an inefficient, insecure, and compliance-based backup process. AI analytics, automated data backup, and next-gen features such as edge storage and immutable backup transform data recovery. They reduce downtime and cut costs, latency, and compliance barriers.

Ailamaki [25] examined mainstream trends and architectures for enabling cloud significant data system resiliency in 2025. It addresses distributed platform issues, data replication, checkpointing, and healing aspects to ensure system availability and reliability. Uncovering new trends and conventional practices, the paper incorporates best practices, current issues, and research topics of business continuity.

Song et al. [26] introduced 2014 an intelligent enterprise backup management system to enable smarter data protection with business continuity and designed explicitly for future Big Data situations. The paper proposes a data analytics-elastic architecture for enterprise backup infrastructure to achieve an access mechanism to valuable information from a massive volume of backup job metadata in gigantic data centers. The architecture proposed enables intelligent decision-making, optimization, and proactive backup management. Some use cases are elaborated to establish how big data analytics can be leveraged in enterprise backup environments.

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Patel and Kansara [27] introduced dynamic multi-cloud infrastructure orchestration in 2024 to improve the scalability, fault tolerance, and efficiency of AI/ML applications. The platform utilizes cloud providers such as Azure, GCP, and AWS for cost-effective scheduling, failover automation, and resource flexibility. Single cloud vs. multi-cloud designs Large-scale comparison demonstrates significant benefits, such as redundancy, elasticity, and disaster recovery.

2.3.2. Infrastructure as Code (IaC)

Batu [28] in 2024 suggested applying approaches for backing up cloud data, such as Warm Standby, Backup & Restore, and Pilot Light with Infrastructure-as-Code (IaC) deployment, to offer countermeasures to impending security and data integrity attacks. Decision-making improves the value of information, but risk due to software or hardware failure, nature, and human mistake reduces its accessibility.

Ajiga et al. [29] of 2024 explains planning techniques for strong architecture that is capable of handling heavy loads and dynamic loads. Modularity, flexibility, and performance are emphasized as practices. Microservices applications are based on the isolated development, deployment, and scalability of services that must be seen.

Sicoe et al. [30] applied an automated provisioning method of virtual router network topology to cloud infrastructure in 2022—Terraform provisions virtual machines with Cisco pre-configured routers. By using a method for managing configurations and the principle of Infrastructure as Code, we created a fully automated system for setting up virtual router infrastructures on different cloud platforms. The process is saving human effort, eliminating repetitive work, and eliminating errors.

2.3.3. Automated Failover and Failback Mechanisms

Elgdamsi and Embarak [31] approached other organizations in 2023 as a continuity strategy; DR solutions must be disaster-resistant, ransomware-resistant, security breach-resistant, and compliant. Official DR processes are insufficient for delivering adequate protection. For that purpose, a virtual network mirroring enterprise business, i.e., corporations and banks, on an HPE server utilizing VMware will be created to test VMware's DR solution to offer minimum downtime for disasters.

Alwan and Alshammari [32] in 2017 suggested a multi-cloud model disaster recovery (DR) to offer better data availability and business continuity before, during, and after a disaster. More prone to outages, data loss, and insider attacks, the model is less susceptible to being outed. With two or more cloud providers providing their services, the model offers better data reliability at lower costs on backups. An emphasis on significant recoveries in business continuity and disaster recovery, like Recovery Point Objective (RPO) and Recovery Time Objective (RTO), indicates that the model is shifting towards proper, economically sound disaster recovery and business continuity.

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.3.4. AI and ML for Backup Optimization

In 2022, Lohani et al. [33] asserted that artificial intelligence (AI) has revolutionized all major industries and operations in the past decade, with disaster recovery (DR) planning being the most affected. Improved computing power and AI capacity to analyze in real-time, as well as increased DR management to make it efficient and swift. AI has the ability to automate disaster recovery processes by relocating critical processes to a second site within seconds, without any human intervention, triggering an alarm, and presenting descriptive data. The paper addresses the advantages and disadvantages of AI deployment of DR processes in pre-disaster and post-disaster phases.

Khan et al. [34] used a future framework that was machine learning and artificial intelligence-based in the year 2022 to leverage supply chain resilience for nationwide disaster recovery due to pandemics, natural disasters, cyberattacks, and geopolitical crises. The framework has four pillars with rudimentary elements that include emergency threat detection, dynamic impact simulation, adaptive response engineering, and resilience monitoring and automation. ML operations streamline logistics, provide live asset deployment, and provide transparency through blockchain tracing to avert downtime and establish public confidence.

2.4. Mass Retail IT Systems

It was the responsibility of Cinque et al. in 2015 [35] to outline requirements for reliability, read literature and process, and provide an innovative solution for improving the reliability of the crisis information system for the EU-funded DESTRIERO project platform.

In 2020, Tsubaki et al. [36] proposed a mechanism for selecting data backup points from distributed sets of TCOs to save resources economically while minimizing network delay during disaster recovery without data loss.

In 2018, Chen et al. [37] employed a bi-layered parallel training (BPT-CNN) model to accelerate the resource-consuming task of training deep convolutional neural networks (CNNs) on distributed computing systems. BPT-CNN has two main parts: the outer layer, where different groups of data are handled by separate CNN subnetworks, and the inner layer, where these subnetworks are trained at the same time. An Incremental Data Partitioning and Allocation algorithm, which considers different types of data, cuts down on how data is assigned, and an Asynchronous Global Weight Update helps to lessen the waiting time for synchronization.

2.5. Technology Tools and Platforms Supporting Automation

Borukaiev et al. [38] of 2022 have conducted research on mathematical and computer modeling professional software issues development to accomplish enabling automated decision-making activity in the competitive electricity market OMS. The unique nature of market operations necessitates the use of advanced simulation tools to assist players in designing strategies for various market elements. It presents a new way to understand the DDM paradigm and proposes

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

a general design for decision support systems that emphasizes market entities, classifiers, and optimization algorithms.

Kirpalani [39] outlined a series of technology solutions in 2024 to aid disaster response and recovery operations. It begins by identifying geospatial technologies like GIS, remote sensing, and satellite imagery to enable information gathering, situational awareness, and management of resources. Equally empowered are AI-based uses of UAVs and autonomous robots to perform damage assessments, clear debris, and inspect infrastructure. Mobile social networking and messaging facilitate coordination and information exchange. Finally, predictive modeling and analytics support planning and decision-making for proactive disaster management and more effective, resilient recovery.

Johnson [40] in 2021 clarified the manner in which computer-based systems integrated into the process of disaster recovery simplify it, access it faster, and reduce human error. Some of the important technologies on which this process hinges are automated backup of information, system tests, and management of faults. Business firms are able to leverage them to help develop more advanced disaster recovery plans through enabling the saving of data alongside business resiliency.

Aliya and Nicola [41] in 2024 stressed that a good disaster recovery plan (DRP) should also be an inclusive one for comprehensive IoT planning, wherein data security concerns, real-time monitoring, and advanced features like end-to-end encryption and secure device authentication are part of it. It is designed with failover automation capability, continuous threat monitoring, and the use of machine learning to identify threats as priorities. Furthermore, vendor relationships, employee orientation, and communication procedures must be regulated for multi-tiered solutions in order to achieve seamless running during interruption.

2.6. Multi-Cloud Orchestration

In 2021, Tomarchio et al. [42] introduced TORCH, a TOSCA-based framework for orchestrating classical and containerized applications across multiple cloud platforms. TORCH uniquely decouples the provisioning workflow from cloud API calls, simplifying integration with various providers. A prototype and initial tests demonstrate TORCH’s flexibility and low integration cost.

In 2023, Sekar [43] presented a framework for optimizing distributed AI workflows using multi-cloud strategies to enhance performance, scalability, and reliability. It integrates cloud service selection, data distribution, and orchestration techniques tested across real-world AI applications. Results show significant improvements in latency, throughput, and cost-efficiency. Dynamic switching between providers boosts fault tolerance and resilience.

In 2022, Zeydan et al. [44] proposed a secure approach using BCNs with post-quantum cryptography (PQC), specifically NTRU, for managing services across multiple administrative domains. Leveraging Toom-Cook computations for efficiency, our results show Quorum

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

achieves lower time-to-write than Ethereum and Hyperledger. We conclude with insights on PQC-BCN integration for future secure service orchestration.

2.7. Multi-region deployments to support DR strategies

In 2023, Damaševičius et al. [45] explored the application of IoES in disaster management, focusing on the role of sensors and IoT devices in delivering real-time situational awareness to responders. It also examines the benefits, challenges, and risks of IoES implementation. By enhancing response speed and public safety, IoES offers significant potential but requires careful deployment to ensure effective and responsible use in crises.

In 2021, Wang [46] presented a multiperiod optimization model for emergency resource allocation that integrates regional self-rescue with cross-regional collaboration. Aiming to minimize delivery time and costs while maximizing coverage, the model uses an objective weighting fuzzy algorithm based on Euclidean distance. A case study of the 2008 Wenchuan Earthquake validates the approach.

In 2023, Qu et al. [47] used an environmentally aware, energy-efficient multi-drone coordination scheme using a reinforcement learning-based location prediction algorithm and two packet forwarding strategies (heuristic and learning-based). This approach improves connectivity and efficiency, evaluated against existing methods in both rural and urban DRM scenarios.

3. Challenges and Limitations

While integrating DR and back-end processes into large retail IT infrastructures presents a multitude of challenges, it can significantly save time and minimize downtime. There is the greatest challenge of bringing complexity to massive retail IT infrastructures, which generally means an astronomical web of connected systems, e.g., point-of-sale (POS) systems, inventory systems, customer databases, and supply chain systems. DR operations in such diverse environments must be converged seamlessly from diverse platforms and technologies, which is impossible without large-scale customization and high-impact automation software in the literal sense. The second step involves maintaining data consistency and completeness across various geographies and systems. Real-time business transactional data is of extreme importance, and inconsistency in recovery or backup will lead to data corruption, business downtime, or financial errors. Synchronization of a distributed system is a complex operation, particularly in geographically distant locations, and hence, it is even more challenging to automate backup and supply it to execute automatically.

Security is a top priority when doing automated disaster recovery. High-commerce retail systems contain a gigantic amount of sensitive financial and customer data, and it is crucial to protect such data from leakage during automated backup processes. Automating systems presents challenges in implementing prerequisites such as end-to-end encryption, secure authentication procedures, and access control. Cost and scalability problems also act as constraints. While DR operations may be made easy by automating them, the upfront expense

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of high-tech equipment and machinery is too much and will keep small retailers away from the latest technology. Further, since retail systems are continuous and expensive, automation infrastructure must catch up with them on a day-to-day basis, and that introduces complexity and cost.

4. Case Studies in Large-Scale Retail IT Systems

This section presents real-world case studies from major retailers that have implemented automated disaster recovery (DR) and backup strategies in their IT infrastructure. These case studies illustrate how the strategies discussed in this paper are applied in practice, highlighting the challenges faced and the benefits realized in large-scale retail environments.

4.1 Walmart—Policy-Based Backup with IaC

Walmart, a global leader in retail, leverages a policy-based backup system integrated with infrastructure as Code (IaC) to automate disaster recovery and backup operations. Walmart uses tools like Terraform and Ansible to define their infrastructure and backup policies, ensuring consistency and quick recovery during system outages. The automated approach reduces human intervention, minimizes downtime, and supports the company's stringent SLA requirements. Walmart's solution features geo-redundant systems that can automatically fail over to a secondary site if the primary site is compromised, ensuring business continuity and high availability.

Key Outcomes

- Reduced failover time to under 30 minutes
- High availability and quick recovery using IaC tools
- Seamless integration of backup scheduling with other automation systems

4.2 Amazon—AI-Driven DR Planning and Cloud-Based Backup

Amazon's retail infrastructure is built on AWS, and it takes advantage of AI-based backup automation and cloud disaster recovery (DR) systems. Through tools like AWS CloudEndure and AWS Backup, Amazon ensures that all customer and business-critical data is consistently backed up and can be restored instantly in the event of a disaster. AI models predict potential system failures based on historical data and system behavior, allowing Amazon to take proactive measures before any disruption. This process reduces downtime significantly, helping Amazon maintain its near-zero Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Key Outcomes

- AI-driven predictive failure models for preemptive action
- Near-zero RTO and RPO, improving system reliability.
- Fully automated backup scheduling and failover operations

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4.3 Target—Multi-Cloud Orchestration for Disaster Recovery

Target, a leading retail chain, utilizes a hybrid cloud strategy that combines AWS and Microsoft Azure to ensure high availability and disaster resilience. By leveraging multi-cloud orchestration, Target achieves both redundancy and load balancing across different cloud providers, improving its ability to recover quickly from failures. Target's DR and backup solution includes automated failover and failback operations, which are tested regularly to ensure seamless recovery. Additionally, real-time monitoring and automated recovery drills ensure that the systems are always prepared for a disaster scenario. A comparative table 1 summarizing Walmart, Amazon, and Target's approaches.

Key Outcomes

- Seamless failover and failback between AWS and Azure
- Real-time monitoring of cloud resources to detect potential failures
- Automated DR testing and compliance with SLAs

Table 1: Comparative Analysis of Disaster Recovery Strategies in Leading Retail IT Systems

Retailer	**Approach**	**Key Tools/Tech**	**Main Benefits**	**Notable Outcomes**
Walmart	Policy-based backup via IaC	Terraform, Ansible	Automated failover, SLA compliance	Failover < 30 min, geo-redundancy
Amazon	AI-driven backup & DR	AWS CloudEndure, AWS Backup	Predictive DR, proactive response	Near-zero RTO/RPO
Target	Multi-cloud orchestration	AWS, Azure	Redundancy, real-time monitoring	Seamless failover, SLA compliance

5. Discussion

DR automation of large-box retail IT infrastructure backups becomes increasingly significant as the retail business keeps on growing and becoming more technology-reliant for continuous operation. Automation improves speed, uniformity, and effectiveness significantly, but it also presents a range of issues that require proportionate compensation. The minimization of human touch at the point of criticality is one of the strongest reasons for disaster recovery through automation. Busy retail environments, whose lost sales and customer frustration could be the consequence of downtime, have their recovery process carried out instantaneously and accurately with no room for human error. Automatic backup processes also benefit from frequent data backup, lessening the risk of data loss and maintaining up-to-date key business information, i.e., transaction history and inventory. However, it is easy to automate backup and DR procedures in a large retail setup. One of the biggest challenges there would be the

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

complexity of the IT infrastructure of such an environment. Retail IT infrastructures are usually mixes of legacy and new tools, on-premises servers, and cloud applications that may not be that easy to automate. They are likely to be susceptible to significant tailoring in a bid to have all the pieces in the IT infrastructure where they belong so that disaster recovery can be made to work optimally, and it becomes a time-consuming and costly initial deployment.

Security is also of paramount concern. Giant retail stores handle enormous amounts of sensitive information, such as monetary and customer information. Backup procedures must ensure that the data is received encrypted and backed up so that it does not leak out. Also, the provision to demonstrate backup availability to the concerned parties and guard against unauthorized access during restoration is pertinent. Finally, flexibility and the scalability of automated processes are things to be considered. As retail businesses grow and mature, the disaster recovery (DR) plan should also expand to accommodate new technologies, increasing data volumes, and system complexities. It involves continuous monitoring and re-tuning of the automation structure to accommodate growing needs, which is time-consuming and expensive. Overall, mass automation of DR and backup planning in retail IT systems has advantages, but companies need to walk carefully when dealing with complexity in systems, security, scalability, and costs.

6. Conclusion

The article addressed automating DR and backup planning in enterprise retail IT environments, in contrast to the imperative need to do so for business continuity and data integrity sustainability. The review utilized 41 research papers to determine the most crucial strategies, including policy-based backup scheduling, IaC deployment, automated failover and failback operations, and the use of AI and ML in the direction of achieving maximum optimality for backups. The goal of these programs was to reduce downtime, boost system resilience, and simplify recovery. The document also described how automation would increase the effectiveness and efficiency of disaster recovery, particularly in sophisticated retail environments where they required high availability and rapid recovery. It provided solutions to the scalability, complexity, and problem of backing up and DR in massive retail IT environments, real-time data processing, and legacy IT infrastructure integration. Additionally, the paper illuminated tools and platforms that enable the process of automation, offering an overview that covers a considerable amount of terrain as far as research and practice are concerned. The study provided useful suggestions to organizations that want to enhance IT resilience and business continuity during disruptions.

References

[1] Hamadah, S. and Aqel, D., 2019, April. A proposed virtual private cloud-based disaster recovery strategy. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) (pp. 469-473). IEEE.

[2] Mohamed, H.A.R., (2014). A proposed model for an IT disaster recovery plan. *International Journal of Modern Education and Computer Science*, *6*(4), pp.57–67.

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[3] Tamimi, A.A., Dawood, R., and Sadaqa, L., 2019, April. Disaster recovery techniques in cloud computing. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) (pp. 845-850). IEEE.

[4] Soni, V.D. (2020). Disaster recovery planning: An untapped success factor in an organization. Available at SSRN 3628630.

[5] Sengupta, S. and Annervaz, K.M., (2014). Multi-site data distribution for disaster recovery—A planning framework. *Future Generation Computer Systems*, *41*, pp.53–64.

[6] Cook, J. (2015). A six-stage business continuity and disaster recovery planning cycle. *SAM Advanced Management Journal*, *80*(3), p.23.

[7] Al–shammari, M.M. and Alwan, A.A., 2018, April. Disaster recovery and business continuity for database services in multi-cloud. In 8, the 1st International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-8). IEEE.

[8] Chang, D., Li, L., Chang, Y., & Qiao, Z. (2021). Cloud computing storage backup and recovery strategy based on secure IoT and Spark. *Mobile information systems*, 2021(1), p.9505249.

[9] Chang, V. (2015). Towards a big data system disaster recovery in a private cloud. *Ad hoc networks*, *35*, pp.65–82.

[10] Alshammari, M.M., Alwan, A.A., Nordin, A., and Abualkishik, A.Z., 2018. Disaster recovery with a minimum replica plan for reliability checking in multi-cloud. Procedia Computer Science, 130, pp.247-254.

[11] Yang, C.L., Yuan, B.J., and Huang, C.Y., 2015. Key determinant derivations for information technology disaster recovery site selection by the multi-criterion decision-making method. Sustainability, 7(5), pp.6149-6188.

[12] Schätter, F., Hansen, O., Wiens, M., and Schultmann, F., 2019. A decision support methodology for disaster-caused business continuity management. Decision Support Systems, 118, pp.10-20.

[13] Marshall, M.I. and Schrank, H.L., 2014. Small business disaster recovery: a research framework. Natural Hazards, 72(2), pp.597-616.

[14] Chatterjee, R. (2021). Private sector: Under-appreciated actors in disaster response and recovery. Humanitarianism in the Asia-Pacific: Engaging the Debate in Policy and Practice, pp.85–89.

[15] Du, H. and Jiang, Y., 2019. A backup or reliability improvement strategy for a manufacturer facing heterogeneous consumers in a dynamic supply chain. IEEE Access, 7, pp.50419-50430.

[16] Nasurudeen, T.F.K., Shukla, V.K., & Gupta, S. (2021, June). Automation of disaster recovery and security in cloud computing. In *2021 International Conference on Communication, Information and Computing Technology (ICCICT)* (pp. 1–6). IEEE.

[17] Abieba, O.A., Alozie, C.E., and Ajayi, O.O., 2025. Enhancing disaster recovery and business continuity in cloud environments through infrastructure as code. Journal of Engineering Research and Reports, 27(3), pp.127-136.

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[18] Morillo Reina, J.D. and Mateo Sanguino, T.J., 2024. Cloud-Based Automatic Configuration and Disaster Recovery of Communication Systems Applied in Engineering Training. Electronics, 13(21), p.4203.

[19] Martin, S. (2024). Disaster Recovery and Business Continuity Planning for Enterprise Applications in the Cloud.

[20] Mehra, T. (2024). Next-gen data protection: Crafting seamless backup and replication strategies for unbreakable business continuity and disaster recovery. *International Journal of Scientific Research in Engineering and Management (IJSREM)*, *8*(12), pp.1–6.

[21] Kim, J.B., Choi, J.B., and Jung, E.S., 2024. Design and Implementation of an Automated Disaster-Recovery System for a Kubernetes Cluster Using LSTM. Applied Sciences, 14(9), p.3914.

[22] Andrade, E. and Nogueira, B., 2020. Dependability evaluation of a disaster recovery solution for IoT infrastructures. The Journal of Supercomputing, 76(3), pp.1828-1849.

[23] Sartwell, M.L., 2020. Strategies for the Development of IT Disaster Recovery Plans in the Manufacturing Industry (Doctoral dissertation, Walden University).

[24] Syed, A.A.M. (2024). Disaster Recovery and Data Backup Optimization: Exploring Next-Gen Storage and Backup Strategies in Multi-Cloud Architectures. *International Journal of Emerging Research in Engineering and Technology*, *5*(3), pp.32–42.

[25] Ailamaki, A., Fault Tolerance and Disaster Recovery Techniques for Big Data in Cloud Environments.

[26] Song, Y., Routray, R., & Hou, Y. (2014, May). Scalable data analytics platform for enterprise backup management. In *2014 IEEE Network Operations and Management Symposium (NOMS)* (pp. 1–7). IEEE.

[27] Patel, H.B. and Kansara, N., (2024). Dynamic Orchestration of Multi-Cloud Resources for Scalable and Resilient AI/ML Workloads: Strategies and Frameworks. *Journal*.

[28] Batu, J. (2024). Implementing Infrastructure-as-Code with Cloud Disaster Recovery Strategies. *International Journal of Computer Trends and Technology*, *72*, pp.41–45.

[29] Ajiga, D., Okeleke, P.A., Folorunsho, S.O., and Ezeigweneme, C., 2024. Methodologies for developing scalable software frameworks that support growing business needs. Int. J. Manag. Entrep. Res, 6, pp.2661-2683.

[30] Sicoe, A.F., Botez, R., Ivanciu, I.A., and Dobrota, V., 2022, June. Fully automated testbed of Cisco virtual routers in cloud-based environments. In 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) (pp. 49-53). IEEE.

[31] Elgdamsi, K. and Embarak, M., 2023. Implementing a Disaster Recovery Solution for Datacenters Using VMware Site Recovery Manager. TUJES, 4(01).

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

[33] Lohani, K., Bhardwaj, P., Atrey, A., Kumar, S., & Tomar, R. (2022). Applications of Artificial Intelligence in IT Disaster Recovery. In *Machine Intelligence and Data*

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Science Applications: Proceedings of MIDAS 2021 (pp. 663–677). Singapore: Springer Nature Singapore.

[34] Khan, R.S., Sirazy, M.R.M., Das, R., and Rahman, S., 2022. An AI and ML-enabled framework for proactive risk mitigation and resilience optimization in global supply chains during national emergencies. Sage Science Review of Applied Machine Learning, 5(2), pp.127-144.

[35] Cinque, M., Cotroneo, D., Esposito, C., Fiorentino, M., and Russo, S., 2015, October. A reliable crisis information system to share data after the event of a large-scale disaster. In 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (pp. 941-946). IEEE.

[36] Tsubaki, T., Ishibashi, R., Kuwahara, T., & Okazaki, Y. (2020, January). Effective disaster recovery for edge computing against large-scale natural disasters. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1–2). IEEE.

[37] Chen, J., Li, K., Bilal, K., Li, K., and Yu, P.S., 2018. A bi-layered parallel training architecture for large-scale convolutional neural networks. IEEE Transactions on Parallel and Distributed Systems, 30(5), pp.965-976.

[38] Borukaiev, Z., Ostapchenko, K., Chemerys, O., and Evdokimov, V., 2022. Information Technology Platform for Automation of Decision-Making Processes by the Organizational Management System. In Power Systems Research and Operation: Selected Problems II (pp. 257-279). Cham: Springer International Publishing.

[39] Kirpalani, C., (2024). Technology-Driven Approaches to Enhance Disaster Response and Recovery. Geospatial Technology for Natural Resource Management, pp. 25-81.

[40] Johnson, E. (2021). The Role of Automation in Disaster Recovery Planning.

[41] Aliya, H. & Nicola, H. (2024). Enhancing Corporate Resilience: A Comprehensive Disaster Recovery Plan for Ensuring Business Continuity in the Age of IoT Security.

[42] Tomarchio, O., Calcaterra, D., Di Modica, G., and Mazzaglia, P., 2021. Torch: a TOSCA-based orchestrator of multi-cloud containerized applications. Journal of Grid Computing, 19(1), p. 5.

[43] Sekar, J. (2023). MULTI-CLOUD STRATEGIES FOR DISTRIBUTED AI WORKFLOWS AND APPLICATIONS. *Journal of Emerging Technologies and Innovative Research, 10, pp. P600-P610*.

[44] Zeydan, E., Baranda, J., and Mangues-Bafalluy, J., 2022. Post-quantum blockchain-based secure service orchestration in multi-cloud networks. IEEE Access, 10,p 129520-129530.

[45] Damaševičius, R., Bacanin, N., and Misra, S., 2023. From sensors to safety: Internet of Emergency Services (IoES) for emergency response and disaster management. Journal of Sensor and Actuator Networks, 12(3), p. 41.

Received: August 05, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[46] Wang, Y., (2021). Multiperiod optimal allocation of emergency resources in support of cross-regional disaster sustainable rescue. *International Journal of Disaster Risk Science*, *12*(3),p 394–409.

[47] Qu, C., Sorbelli, F.B., Singh, R., Calyam, P., and Das, S.K., (2023). Environmentally aware and energy-efficient multi-drone coordination and networking for disaster response. IEEE Transactions on Network and Service Management, 20(2), pp. 1093–1109.

Received: August 05, 2025