SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V12I5P101

Volume 12 Issue 5, 1-9, May 2025
© 2025 Seventh Sense Research Group®

Original Article

Enhancing Banking Disaster Recovery with AWS Cloud Services

Sivakumar Ponnusamy

Independent Researcher, Richmond, VA, USA.

[1]*Corresponding Author : psivakumarmca@gmail.com*

Received: 08 March 2025 Revised: 13 April 2025 Accepted: 01 May 2025 Published: 17 May 2025

Abstract *- In the rapidly evolving banking landscape, Disaster Recovery (DR) has emerged as a critical component of business continuity and regulatory compliance. Traditional DR methods, though reliable, often fall short in scalability, cost-efficiency, and speed. This article explores how Amazon Web Services (AWS) cloud services are revolutionizing disaster recovery strategies in the banking sector. It provides an in-depth analysis of core AWS services such as EC2, S3, RDS, and AWS Elastic Disaster Recovery (DRS). It examines various DR models, including backup and restore, pilot light, warm standby, and multi-site active/active configurations. Through real-world case studies and hypothetical scenarios, the paper highlights the measurable benefits of adopting cloud-based DR—such as reduced downtime, improved recovery metrics, and enhanced regulatory compliance. It also addresses key implementation challenges, including data sovereignty, security, and skills gaps, and outlines how AWS mitigates these risks. Looking ahead, the article discusses emerging trends like AI-driven DR automation and serverless resilience, positioning AWS as a strong and future-ready partner for banking institutions seeking robust disaster recovery solutions.*

Keywords - *Disaster Recovery, Banking sector, AWS Cloud, Business Continuity, Amazon Web Services.*

1. Introduction

The banking sector is currently experiencing a substantial transformation in the rapidly evolving digital economy of the present day [1]. Due to the rise of digital platforms, real-time data processing, and online banking services, uninterrupted availability is crucial. Customers today want their money, digital transactions to be quick and convenient, and 24/7 customer support. Any interruption-hardware failure, cyberattack, natural disaster, or human error can cause significant financial losses, reputational damage, and regulatory penalties. Due to the complexity and susceptibility of current banking systems, Disaster Recovery (DR) is vital to every bank's operational resilience plan.

Disaster recovery aims to restore IT systems and operations after a disruption quickly. This is achieved through the implementation of comprehensive policies, instruments, and procedures. Financial organizations must recover data (DR) lawfully and profitably. Financial institutions process huge amounts of sensitive consumer data and facilitate frequent, high-value transactions [2]. Outages can cause millions in transaction losses, financial regulatory violations, and unauthorized access to confidential data. Well-structured DR plans provide organizational continuity by decreasing unscheduled downtime, ensuring data integrity, and retaining customer trust. Due to the evolving financial services sector and digital risks, banks must promptly review, test, and upgrade their DR capabilities.

1.1. The Crucial Role of Disaster Recovery in Financial Institutions

Disaster Recovery (DR) is essential to regulatory compliance, customer trust, and the bank's continued business operations [3]. System failure or data loss has become increasingly severe as financial institutions and service providers digitalize their products and services and move to real-time data environments. A comprehensive DR plan is necessary. The FFIEC in the US, the GDPR in Europe, and Basel III worldwide all impose strict data security, system backup, and continuity of operations regulations on financial institutions [4]. These guidelines necessitate strict Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), determining the minimum time systems must be restored and the maximum data loss without serious issues. Under unmet criteria, regulators may punish, restrict operations, or cancel banking licenses.

Beyond compliance, consumer trust is crucial. Because they manage sensitive personal and financial data, people expect financial institutions to operate smoothly even during crises. A single outage can destroy a customer's trust in a company, and they may switch to a more reliable competitor. Financial and operational stability also need to be competitive. Even short interruptions might disrupt trading and payments. Therefore, financial institutions should invest in strong, scalable, cost-effective DR solutions. These solutions should incorporate automated failovers, redundant systems, and cloud backups. Disaster

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

recovery is now a strategic imperative for financial institutions in the digital age.

1.2. The Role of Cloud Computing in Modern Disaster Recovery

Traditional disaster recovery systems include secondary data centres, physical backups, and manual failover procedures, which are expensive, rigid, and time-consuming. These antiquated systems sometimes struggle to meet modern Internet banking's automation, speed, and scalability needs. With cloud computing, the game changes. Financial organizations benefit from cloud-based disaster recovery, including cost savings, system flexibility, and faster recovery times. With cloud-based DR, standby hardware is no longer needed, and pay-as-you-go models can match expenses to consumption. Amazon Web Services (AWS) leads cloud service providers in reliable, scalable, and secure DR solutions [5]. AWS's products can aid disaster recovery lifecycle stages such as data backup, replication, automated failover, and system monitoring.

1.3. AWS Cloud Services: A Strategic Partner in Banking DR

AWS provides scalable and dependable DR solutions for service delivery and data integrity in the financial ecosystem. Due to its vast service portfolio, AWS can meet any financial institution's recovery needs, timescales, and budgets. Banks can automate backup management across all AWS services and Amazon S3 for persistent object storage with AWS Backup, making catastrophe recovery quick and economical [6]. AWS supports complicated designs for mission-critical environments, including pilot light, warm standby, and multi-site active-active deployments. Amazon Elastic Disaster Recovery (AWS DRS), Amazon Relational Database Service (RDS), and Amazon Elastic Compute Cloud (EC2) give processing capability to recover on-premises and cloud workloads quickly, reliably, and cost-effectively.

Beyond infrastructure, AWS improves operational resilience through automation and orchestration. AWS Lambda and AWS CloudFormation allow financial organizations to automate and script DR processes, improving recovery speed and reducing human error [7]. These traits ensure a faster and more reliable response to interruptions. AWS improves DR preparation and deployment with analytics and machine learning. Detecting vulnerabilities, predicting system malfunctions, and automatically correcting them can make disaster preparedness proactive. AWS Cloud Services allows banks to build and implement a flexible disaster recovery plan for the digital banking industry.

1.4. Purpose and Scope of the Article

This article examines how AWS cloud services assist financial companies' disaster recovery. This article will examine the challenges banks have when utilizing conventional DR models, how AWS solves them, and the different DR techniques available on the AWS platform. This article analyses, illustrates and predicts how AWS improves financial firms' catastrophe recovery and resilience. As the digital and regulatory world becomes more complex, banks must embrace cloud-based disaster recovery solutions like AWS.

2. Understanding Disaster Recovery in Banking

2.1. Disaster Recovery in the Context of Banking

Disaster recovery DR methods, policies, and technologies can restore critical IT systems and data. Every banking organization needs a disaster recovery strategy since systems must be highly available and exact. Financial institutions use complex IT infrastructures for digital banking, customer transactions, internal operations, and compliance reporting [8]. Service failures, data corruption, and malfunctions can be devastating. Thus, banking DR involves restoring operations quickly and safely with minimal data loss and service interruption. Unlike IT DR plans with flexible timeframes, Bank DR has strict RTOs and RPOs. These options establish minimal data loss and service restoration time. Loss or delay is strictly prohibited in a field where seconds cost millions.

2.2. Types of Disasters That Banks Must Prepare For

Banks operate in a high-risk environment with numerous potential threats. Threats might be natural, technical, or manmade, requiring different levels of preparedness. Cyberattacks are major threats. Digitization of financial services has led to ransomware, data breaches, and DoS assaults [9]. These events can turn off networks, compromise customer data, and interrupt banking services. Server breakdowns and data centre power outages are common hardware issues. Even with redundant gear, a single point of failure can disrupt service without proper management.

Hurricanes, earthquakes, and floods can damage homes and other structures, although they occur relatively infrequently. Financial institutions may scramble to maintain continuity after branch closures, data centre damage, or connectivity loss. Human error, which includes data loss, misconfigurations, and insider threats, is a substantial but often overlooked risk. Well-developed systems are not immune—one mistake can still cause major data loss or disruptions until it is addressed.

2.3. Challenges in Traditional Banking DR Systems

Many financial institutions deploy outdated or inadequate disaster recovery technologies. Today's fast-paced world makes manual failover, periodic backups, and other data centres risky [10]. Cost is one of the most significant barriers. A dedicated disaster recovery facility with redundant gear, network equipment, and operators is expensive. Underutilized infrastructure makes it harder for smaller and medium-sized banks to justify and sustain costs. Legacy system integration and automation are complex owing to different technologies and suppliers. Recovery procedures can be laborious and error-prone in high-stakes circumstances. Traditional Disaster Recovery (DR)

methods often result in downtime, even when optimized. Manual failover and restoration processes can take hours or even days. During this period, customer service may be unavailable, transactions slow down, and the company's reputation is adversely affected. If regular backups miss recent transactions, data inconsistencies or loss can result. This is a major threat in real-time financial transactions.

2.4. Disaster Recovery Compliance and Regulatory Obligations

Regulators have strong standards to ensure banks are ready for interruptions because financial activities are essential. Compliance is mandatory because violating these regulations might result in significant fines, operational restrictions, or customer distrust. The FFIEC requires American banks to have a disaster recovery-focused Business Continuity Management (BCM) plan [11]. Data availability and resilience are part of Europe's GDPR. Restoring sensitive data quickly and keeping systems working with some downtime is crucial for financial institutions. PCI-DSS and ISO/IEC 27031 recommend methods to ensure financial data and services are reliable and safe. The guidelines require testing, documentation, and practical methods, not abstract strategies. As banks utilize more digital technology and cross-border services, aligning disaster recovery strategies with regulatory criteria becomes more complex and important.

3. Cloud-Based Disaster Recovery

3.1. Traditional Disaster Recovery vs. Cloud-Based DR

For years, banks' primary disaster recovery methods were secondary data centres, backup servers, and manual recovery techniques. These configurations usually comprised redundant infrastructure dormant until a disaster, requiring significant initial investment and ongoing maintenance. These technologies made individuals feel safe and in control but could not scale or adapt to new dangers. However, cloud disaster recovery uses third-party suppliers' distributed data centres and virtualized environments like AWS. Cloud services allow banks to automate recovery, store backups, and run failover systems without maintaining physical infrastructure. Cloud DR lets users interact with our existing systems, replicate data continuously, and provision resources on demand [12]. Moving from a hardware-heavy paradigm to a service-driven one simplifies disaster recovery planning and aligns with modern digital banking.

3.2. Key Advantages of Cloud-Based Disaster Recovery

Cloud-based DR solves several conventional DR issues. Financial organizations are increasingly using cloud computing to improve disaster recovery preparations.

3.2.1. Scalability

Scalability is a significant benefit of cloud-based disaster recovery. Scaling up conventionally required new hardware and a long lead time. Cloud services like Amazon Web Services help improve banks' DR capabilities on demand. Cloud platforms can instantly replicate a few critical applications or a core financial system [13]. This versatility will be crucial in emergencies or data processing spikes.

3.2.2. Automation

Automation is a major benefit of cloud-based DR. Banks can automate backup, failover, testing, and compliance checks with AWS Lambda, CloudFormation, and Systems Manager. This ensures consistency, facilitates recovery and reduces human error. Automation allows regular DR plan testing for regulatory compliance and operational readiness.

3.2.3. Cost Efficiency

Many companies use the cloud to save money. Conventional DR requires a huge infrastructure investment that may be rarely used. However, banks only pay for the storage, computing, and networking resources they use with cloud-based DR. AWS's S3 Standard, S3 Glacier, and S3 Glacier Deep Archive tiered storage options let banks choose inexpensive solutions based on data access frequency.

3.2.4. Accessibility and Geographic Redundancy

Due to its global accessibility, cloud-based DR can start recovery operations practically anywhere. This helps in large-scale regional disasters that make backup sites unreachable. AWS offers geographically distributed data centres, allowing banks to store and replicate data in multiple safe locations.

3.3. Transforming RTO and RPO Through the Cloud

RTO and RPO measure disaster recovery plans. The maximum permissible time for service restoration and data loss after RTO and RPO measure a disruption. Traditional systems have difficulty satisfying low RTO and RPO requirements due to the time necessary to activate secondary systems, extricate backups, and reconfigure applications [14]. In banking, transactions happen every second. Thus, downtime causes quick losses, and these metrics can be improved by cloud DR. Banks can achieve RTOs of minutes and RPOs of seconds with instant virtual machine formation, continuous data replication, and automatic failover. AWS DRS can recover and replicate workloads in near real-time without human intervention. These RTO and RPO modifications allow banks to operate during disasters, improving regulatory compliance and customer satisfaction. Cloud-based disaster recovery is more advanced than prior solutions. Banks can build strong infrastructures with cloud technologies like AWS because they solve complexity, cost, and scalability issues and boost recovery metrics.

4. Overview of AWS Cloud Services for Disaster Recovery

Disaster Recovery in the cloud is only as strong as the services that support it. AWS (Amazon Web Services) offers many tools and services designed to build a highly resilient, secure, and automated DR infrastructure. For banks and other financial institutions, leveraging these services means reducing downtime, ensuring data integrity,

and maintaining compliance with regulatory standards while improving operational efficiency and scalability.

4.1. Amazon EC2 (Elastic Compute Cloud)

Amazon Elastic Compute Cloud (EC2), a major AWS service, provides instances of scalable virtual computing environments in the cloud. EC2 can quickly spin up mission-critical applications in a secondary availability zone or region for financial institutions' disaster recovery [15]. In times of crisis, Amazon EC2 enables rapid deployment of computing resources to support critical infrastructure such as databases, APIs, core banking systems, and frontend services. By leveraging custom Amazon Machine Images (AMIs), organizations can launch pre-configured applications and OS instances swiftly to maintain continuity. This capability becomes particularly vital when safeguarding against issues like API drift, which can introduce data inconsistencies or security risks if not monitored and addressed promptly [16]. Banks can also change capacity to maintain performance during failover without spending money on empty infrastructure while the business is good. EC2's strong connection with AWS services like Auto Scaling and Elastic Demand Balancing ensures application availability and resilience under varying demand situations.

4.2. Amazon S3 (Simple Storage Service)

Amazon Simple Storage Service (S3) is safe, scalable, and ideal for storage for archive, backup, log, and static content. Since its design guarantees 99.999999999% endurance, it is a good long-term data archival [17]. S3 can back up databases, apps, and important configurations daily or in real-time, making it ideal for disaster recovery planning. Versioning and lifecycle controls automate backup archival and deletion to reduce expenses. Banks can store data in multiple availability zones or replicate data across regions using S3 Cross-Region Replication (CRR) for speedy access and recovery in any crisis. S3's interaction with AWS Backup and encryption (at rest and in transit) ensures sensitive financial data is protected and recoverable.

4.3. Amazon RDS (Relational Database Service)

Managed database service Amazon RDS supports several database engines, including SQL Server, Oracle, PostgreSQL, and MySQL. This is crucial for financial institutions that store and analyze client data, financial transactions, and analytical data in relational databases. RDS simplifies catastrophe backup and restoration of critical databases. It offers automated backups, snapshots, and multi-AZ (Availability Zone) deployments with synchronous standby replicas in other AZs. In an outage, RDS can easily transition to this copy. Banks can use cross-region replication and Amazon RDS Read Replicas for sophisticated DR settings to plan for regional failures. This ensures continued data copying to another location.

4.4. AWS Backup

EC2, RDS, DynamoDB, EFS, and other AWS services may be backed up centrally and automatically with AWS Backup. This integrated backup system provides financial organizations with audit records by standardizing backup methods and streamlining compliance reporting [18]. Bank backup plans may include scheduling, retention criteria, and vault specifics.

AWS Backup's cross-region backup and recovery helps meet strict data sovereignty and regional redundancy laws. One-click restores from AWS Backup speed up disaster recovery by reducing manual involvement. Banks value data integrity and availability; therefore, AWS Backup centralizes backup management to reduce lost or inconsistent backups.

4.5. AWS Elastic Disaster Recovery (AWS DRS)

Designed to simplify and speed up disaster recovery, AWS DRS continuously replicates virtual, cloud-based, and physical workloads onto AWS [19]. It minimizes downtime and data loss in a disaster. AWS DRS lets financial organizations transfer workloads from on-premises to AWS without disrupting their infrastructure. Banks can launch EC2 instances in minutes if a workload fails to resume operations. After restoring the environment, rolling back systems will be quick. DRS is ideal for banks with non-cloud native older systems that need modern DR. Automated testing and non-disruptive exercises help achieve compliance without affecting production environments.

4.6. Amazon Route 53

Amazon Route 53, a scalable DNS web service from AWS, is essential for traffic routing during a failover [20]. Route 53 manages DNS failover and routing settings for disaster recovery to deliver users to healthy endpoints. Route 53 can reroute DNS traffic to secondary servers, regions, or availability zones dependent on the application's health if the main systems fail. DNS-based failover is essential for business continuity and downtime reduction since customer access to banking apps and online portals is key. It supports latency-based and geolocation routing to help financial organizations improve user experience and resilience.

4.7. AWS CloudFormation & AWS Lambda for Automation

AWS can automate and improve consistency for a fast and reliable disaster recovery system. AWS CloudFormation lets banks code their infrastructure. CloudFormation templates may install whole DR setups in minutes, including databases, servers, networking configurations, and permissions [21]. This improves recovery uniformity and reduces human error.

AWS Lambda can start backups, migrate to other databases, or notify administrators in a crisis. Event-driven processes that detect mistakes and automate responses are crucial in time-sensitive banking systems. This can be achieved by integrating Lambda with Amazon CloudWatch. Self-healing DR ecosystems built with CloudFormation and Lambda reduce banks' recovery overhead and response times.

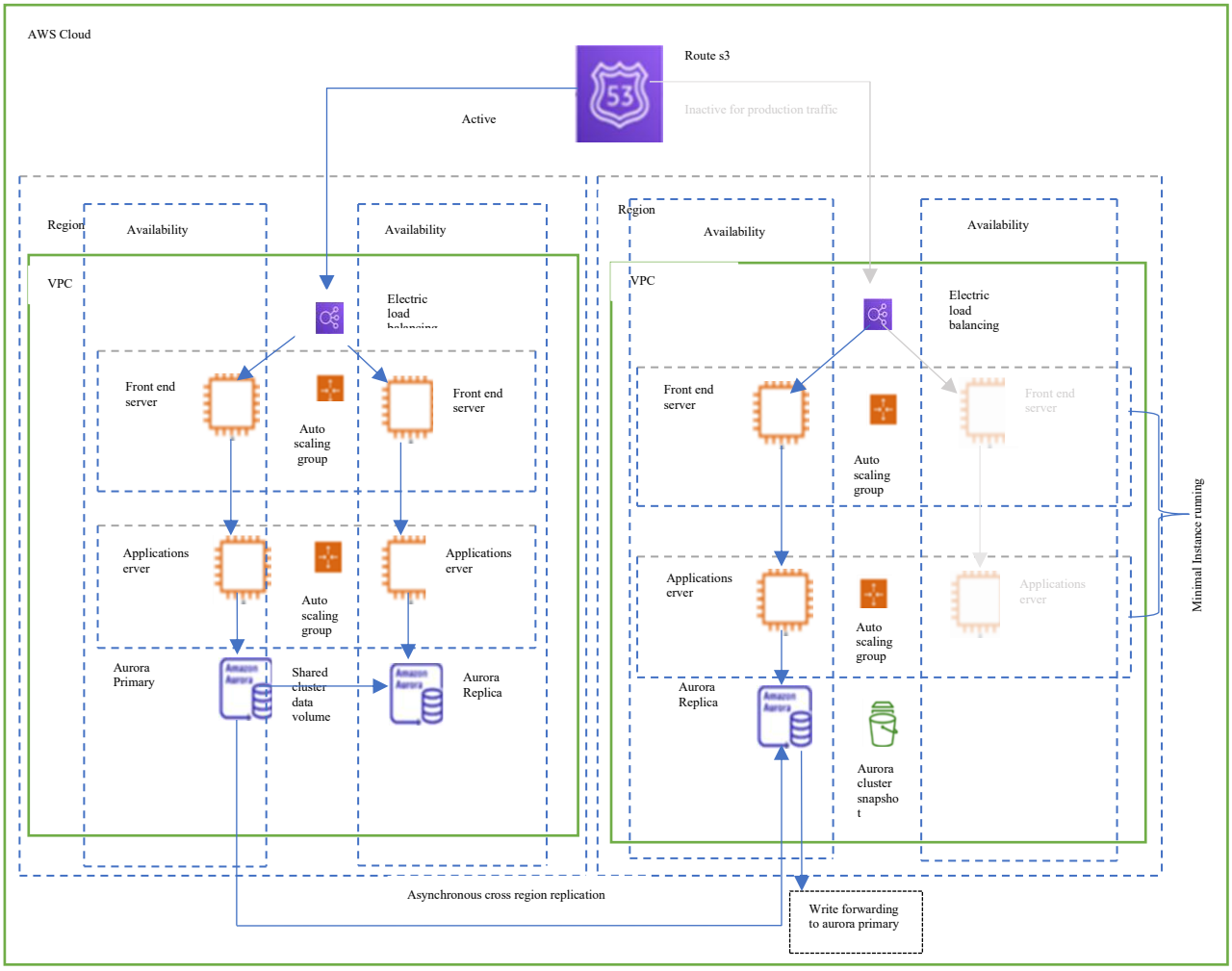

Fig. 1 AWS disaster recovery architecture overview

4.8. Integrated Power of the AWS Ecosystem

Even though each AWS disaster recovery service is unique, its integration is its strength. A disaster recovery strategy could include AWS DRS for workload replication, Amazon S3 with automated rules from Amazon Simple Backup, Amazon Elastic Compute Cloud (EC2) for compute instance spinning, Route 53 for user direction, and CloudFormation and Lambda for orchestration [22].

This seamless connectivity allows financial organizations to create a coherent, scalable, and highly robust disaster recovery architecture to meet modern banking and global regulatory standards.

5. Disaster Recovery Strategies with AWS

The financial business's operational complexity, client demands, and regulatory compliance vary. Hence, there is no common disaster recovery method. AWS's disaster recovery models can meet criticality, budget, and recovery time goals.

Backup and Restore Warm Standby, Multi-site Active/Active, and Pilot Light are disaster recovery options that range from slow and cheap to high availability and some downtime.

5.1. Backup and Restore

Backup and Restore is the cheapest and easiest disaster recovery approach. This technique includes regular Amazon S3 or AWS backups for critical data and settings. These backups restore services in another AWS availability zone or region if a disaster strikes.

The approach has lengthy recovery times but low infrastructure costs [23]. This strategy may work for banks' less important tasks, including back-office systems, archival records, and historical data.

5.2. Pilot Light

Pilot Light extends backup and restore by adding a basic, always-on environment replicating the production system's critical components. Databases, authentication servers, and configuration files remain active, albeit under degraded conditions.

In a disaster, AWS CloudFormation and Amazon EC2 can instantly scale up application servers, frontend services, and other infrastructure [24]. This method balances efficiency and cost. This is an effective alternative for banks that wish to recover key services faster without investing money in a mirrored environment.

5.3. Warm Standby

A reduced production environment version runs continuously in the Warm Standby model. The system works but may not be efficient. AWS auto-scaling or CloudFormation scripts scale the alternative environment to meet production demand during a failover. Banks like this strategy because it balances pricing and availability. It is cheaper than a multi-site configuration and recovers faster than a pilot light.

Warm standby is best for key banking functions, including online client portals, mobile banking platforms, and internal processing systems, which must be restored quickly to maintain service levels and compliance.

5.4. Multi-site Active/Active

The most expensive and reliable disaster recovery method is multi-site active/active. It involves running two or more fully functional production sites simultaneously. Even if one area fails, traffic is dispersed using Amazon Route 53 to ensure request processing. Although operational costs are significant, this strategy yields the lowest RTO and RPO [25]. For low-downtime services, real-time trading platforms, and institutions with high transaction volumes, Active/Active is the norm.

Table 1. DR Models Comparison Table

Strategy	Cost	RTO	RPO	Suitability
Backup & restore	Low	High	Medium	Archival/Non-Critical Apps
Pilot Light	Medium	Medium	Low	Core Systems, Limited Budget
Warm Standby	Medium	Low	Low	Essential Services
Multi-site Active	High	Very Low	Very Low	Real-time Banking/Trading

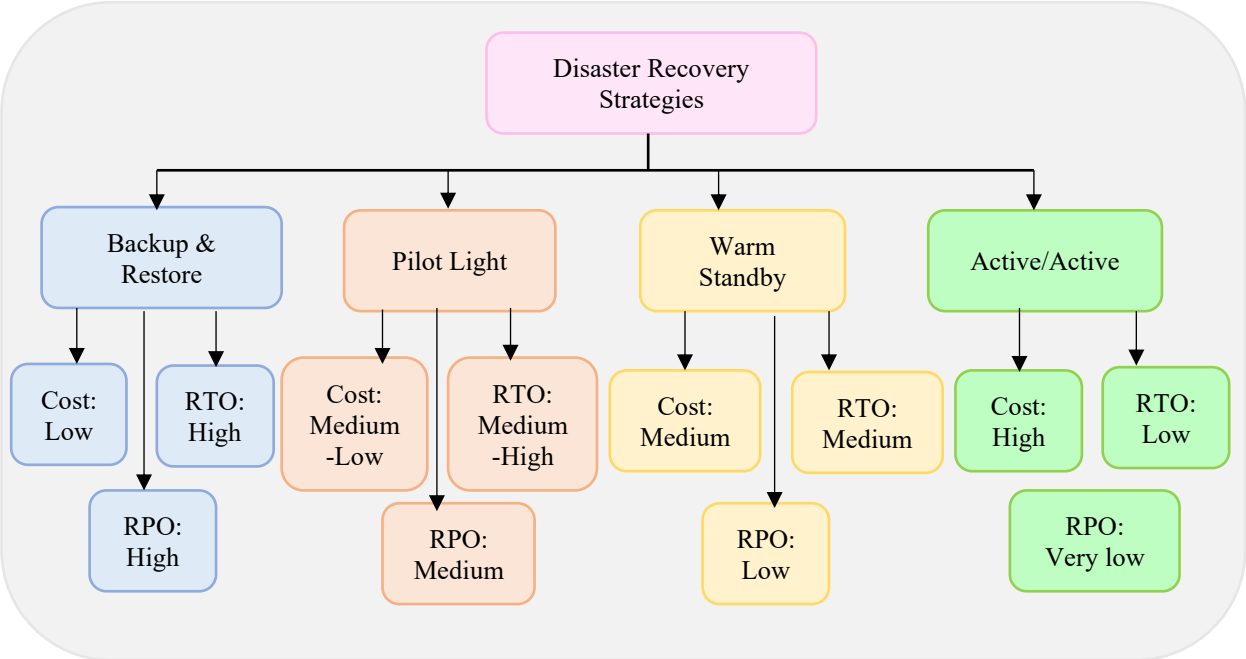

Fig. 2 Disaster Recovery Strategy (Source: Self-Created)

5.5. Choosing the Right Strategy for Banks

Financial institutions choose DR strategies based on risk appetite, regulatory needs, and budgetary constraints. Structured solutions are most efficient, with warm standby or active/active workloads for critical parts and pilot light or backup and restoration models for less critical parts.

Budget-conscious banks with a low tolerance for downtime may prefer Pilot Lite, whereas institutions that provide 24/7 customer care in multiple regions may need active/active settings. AWS's scalability and agility allow banks to create disaster recovery strategies that suit their technological and commercial goals to protect operations and consumer confidence.

6. Case Studies

6.1. Case Study 1: Mid-Sized Bank Transitions to AWS for Disaster Recovery

A mid-sized regional bank in three states used a disaster recovery plan with a secondary data centre co-located with the original one and weekly tape backups. While useful, this technology was expensive to maintain and may take 10 hours of human work to restore functions after a breakdown. Compliance checks also noted testing delays and poor backup coverage. The bank integrated AWS into its disaster recovery strategy to streamline operations and minimize costs. Its pilot light design used Amazon EC2 for critical computing, Amazon RDS for its core databases, and Amazon S3 for daily backups of transactional data [26].

AWS Lambda and CloudFormation automated environment scaling and infrastructure provisioning during failovers. After switching, the bank cut disaster recovery infrastructure costs by 70% by eliminating its secondary physical facility.

The biggest improvement is bringing mission-critical RTO down to 45 minutes from 8-10 hours. Continuous data replication reduced RPO from 24 hours to 5 minutes. Regular automated testing of recovery procedures helped the bank pass its latest compliance examinations.

6.2. Case Study 2: Large Financial Institution Implements Hybrid DR with AWS

A large international bank used on-premises and cloud-native disaster recovery solutions. The bank retained its important systems on-premises and used AWS for offsite backup and secondary failover due to historical infrastructure investments and restrictions. AWS Elastic Disaster Recovery replicated workloads from private data centres to AWS [27]. The bank built warm standby environments for its digital banking services in two AWS regions using Amazon RDS Multi-AZ for core database resilience and Amazon Route 53 for DNS failover. S3 and AWS Backup backed up and restored less critical systems like internal analytics platforms and employee intranet services. A disaster recovery simulation allowed the bank to fail over its online banking platform to AWS in under 20 minutes, compared to two to four hours before. After the drill, important services interacting with consumers had less than 30 minutes of outage and a 50% improvement in RTO. The hybrid model's upfront expenses were 25% more than a cloud-only DR solution but 25% lower than two full-scale data centres. Integrating existing systems with AWS DRS and ensuring compliance across jurisdictions were the biggest challenges, especially for cross-border data replication.

Table 2. Key metrics from case studies

Bank Type	Pre-AWS RTO	Post-AWS RTO	Pre-AWS Downtime	Post-AWS Downtime	Cost Reduction
Mid-sized Bank	8–10 hours	45 minutes	Up to 12 hours	< 1 hour	70%
Large Institution	2–4 hours	20 minutes	2–3 hours	< 30 minutes	25%

7. Implementation Challenges and Mitigation

Despite the benefits, Many institutions have difficulty integrating AWS-based disaster recovery solutions from on-premises settings. Financial institutions must meet PCI-DSS, FFIEC, and GDPR data protection, auditing, and traceability requirements. The cloud stores confidential customer and financial data, raising security, breach, and third-party liability concerns. Also important are encryption and data sovereignty. Many financial organizations operate in multiple countries. Therefore, local laws need data to be retained within each jurisdiction. AWS KMS and customer-managed keys enforce region-specific data centre rules that strongly encrypt data in transit and at rest. Amazon Macie helps classify and detect threats to improve compliance. The skills gap is another issue. Cloud-native technologies can be difficult for traditional banking IT teams to manage. Certifications, hands-on labs, and AWS Skill Builder help build internal cloud competencies.

AWS Outposts, which put AWS infrastructure on-premises, enable a more flexible hybrid architecture. AWS's global footprint, scalable service model, and full security, compliance, and governance tools help institutions overcome these issues and build a robust DR strategy.

8. Future of Disaster Recovery in Banking with Cloud

New technologies and regulatory demands are redefining banking crisis recovery. Disaster recovery increasingly relies on ML and AI. AWS technologies like AWS Fault Injection Simulator and Amazon SageMaker can help financial organizations anticipate problems, spot abnormalities, and simulate disaster scenarios to eliminate human error. Another trend, serverless architecture, helps financial organizations manage backend activities without infrastructure. With AWS Lambda and Amazon EventBridge, financial institutions may create event-driven, automated disaster recovery protocols that respond to system errors. This ensures availability and greatly reduces recovery time. Predictive analytics can identify and avoid failure patterns using real-time monitoring technologies like AWS X-Ray and Amazon CloudWatch.

9. Conclusion

Disaster recovery has been a major strategic target for the banking industry due to the importance of operational continuity in consumer confidence and regulatory compliance. This article examined how AWS cloud services can be utilized to build powerful, scalable, and cost-effective DR systems. AWS services including EC2, S3, RDS, DRS, Lambda, and CloudFormation, help banks raise RTO and RPO, save money, and reduce downtime. Backup and restore and multi-site active/active DR models and how financial institutions can adjust their DR strategy to their budget and risk tolerance were also discussed. AWS's speedier recovery and higher compliance were shown in real-world circumstances. Although cloud-based DR deployment has challenges, AWS provides the tools, education, and adaptability to overcome them. Due to AI, PA, and serverless computing, banks' disaster recovery prospects are good with AWS. Disaster Recovery in the cloud is a strategic move towards online trust and resilience.

References

[1] Premkumar Ganesan, "Cloud-Based Disaster Recovery: Reducing Risk and Improving Continuity," *Journal of Artificial Intelligence and Cloud Computing*, vol. 3, no. 1, pp. 1-4, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Jordan Nelson, *The Role of Automation and AI in Enhancing Disaster Recovery Processes in Multi-Cloud Environments*, pp. 1-19, 2025. [Google Scholar]

[3] Tomasz Nowak, "Cloud Transformation for Modern Banking Systems," *International Journal of AI, BigData, Computational and Management Studies*, vol. 1, no. 3, pp. 23-30, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Sasikiran Vepanambattu Subramanyam, "Cloud Computing and Business Process Re-engineering in Financial Systems: The Future of Digital Transformation," *International Journal of Information Technology and Management Information Systems (IJITMIS)*, vol. 12, no. 1, pp. 126-143, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ravi Chandra Thota, "Cloud Security in Financial Services: Protecting Sensitive Data with AWS well-Architected Framework," *International Journal of Novel Research and Development*, vol. 6, no. 4, pp. 18-24, 2021. [Google Scholar] [Publisher Link]

[6] Naga Rishyendar Panguluri, "Cloud Computing and Its Impact on the Security of Financial Systems," *Computer Science and Engineering*, vol. 14, no. 6, pp. 121-128, 2024. [Google Scholar] [Publisher Link]

[7] Muhammad Ehsan Rana, Tzung Maw Yik, and Vazeerudeen Abdul Hameed, "Cloud Computing Adoption in the Banking Sector: A Comparative Analysis of Three Major CSPs," *2023 IEEE 6th International Conference on Big Data Artificial Intelligence (BDAI)*, Jiaxing, China, pp. 244-250, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Nissi Joy, "Secure and Scalable Cloud Architecture for Banking Transactions: An AWS-Based Multi-AZ Deployment with Compliance and Monitoring," *International Journal of Emerging Research in Engineering and Technology*, vol. 4, no. 4, pp. 1-14, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Anil Kumar Bayya, "Leveraging Advanced Cloud Computing Paradigms to Revolutionize Enterprise Application Infrastructure," *Asian Journal of Mathematics and Computer Research*, vol. 32, no. 1, pp. 133-154, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] Omoniyi Babatunde Johnson et al., "Designing a Comprehensive Cloud Migration Framework for High-revenue Financial Services: A Case Study on Efficiency and Cost Management," *Open Access Research Journal of Science and Technology*, vol. 12, no. 2, pp. 58-69, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Vijay Kartik Sikha, "Developing a BCDR Solution with Azure for Cloud-Based Applications Across Geographies," *North American Journal of Engineering Research*, vol. 5, no. 2, pp. 1-10, 2024. [Google Scholar] [Publisher Link]

[12] Mahfooz Alam et al., "Cloud Computing: Architecture, Vision, Challenges, Opportunities, and Emerging Trends," *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India, pp. 829-834, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Harikumar Nagarajan et al., "Advanced Database Management and Cloud Solutions for Enhanced Financial Budgeting in the Banking Sector," *International Journal of HRM and Organizational Behavior*, vol. 11, no. 4, pp. 74-96, 2023. [Google Scholar] [Publisher Link]

[14] Abhilash Katari, and Madhu Ankam, "Data Governance in Multi-Cloud Environments for Financial Services: Challenges and Solutions," *International Journal of Multidisciplinary and Current Educational Research (IJMCER)*, vol. 4, no. 1, pp. 339-353, 2022. [Google Scholar] [Publisher Link]

[15] Ava Thompson, "AI-Driven Insights for Risk Management in Banking: Leveraging Cloud-Native Technologies for Scalability," *International Journal of AI, BigData, Computational and Management Studies*, vol. 3, no. 4, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Anoop Gupta, "API Drift Detection Enhancing Data Protection," *International Journal of Computer Applications*, vol. 186, no. 49, pp. 47-50, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Munif Bafana, and Ashraf Abdulaziz, "Hybrid Cloud Harmony: Integrating On-Premises and AWS Infrastructure for Seamless Operations," *Asian American Research Letters Journal*, vol. 1, no. 1, pp. 1-12, 2024. [Google Scholar] [Publisher Link]

[18] Muhammad Ehsan Rana, and Lai Zhen Ji, "The Role and Potential Applications of Cloud Computing in the Banking Industry," *2023 15th International Conference on Development in eSystems Engineering (DeSE)*, Baghdad & Anbar, Iraq, pp. 293-298, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Rajeswaran Ayyadurai, Karthikeyan Parthasarathy, and Muhammad Habib, "The Optimizing Financial Data Transfers in the Cloud: A Comparative Analysis of Encryption and Machine Learning Algorithms," *International Journal of Digital Innovation, Insight, and Information*, vol. 1, no. 1, pp. 1-13, 2025. [Google Scholar] [Publisher Link]

[20] Axel Egon et al., "*Evaluating the Development and Significance of Cloud Computing: Transforming the Digital Society*," Working Paper, University of Pennsylvania, pp. 1-22, 2025. [Google Scholar]

[21] Rajmani Bundela, Namrata Dhanda, and Kapil Kumar Gupta, "Identification and Analysis of Security Issues in Cloud Computing," *2024 2nd International Conference on Disruptive Technology (ICDT)*, Greater Noida, India, pp. 1685-1690, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Sai Chetan Muppalla, Sonali Rana, and Jasneet Chawla, "Cloud-Powered Blood Bank Management-Leveraging AWS Services for Efficiency and Scalability," *2023 3rd Internatioanl Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Bangalore, India, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Manya K. Ravindranathan, D. Sendil Vadivu, and Narendran Rajagopalan, "Cloud-Driven Machine Learning with AWS: A Comprehensive Review of Services," *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, Bangalore, India, pp. 1-8, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Righa Tandon, Ajay Verma, and P.K. Gupta, *Fault Tolerant and Reliable Resource Optimization Model for Cloud*, Reliable and Intelligent Optimization in Multi-Layered Cloud Computing Architectures, 1st ed., Auerbach Publications, pp. 1-35, 2024. [Google Scholar] [Publisher Link]

[25] Ang Ting Xun et al., "Building Trust in Cloud Computing: Strategies for Resilient Security," *Computer Science and Mathematics*, pp. 1-22, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Ravikiran Kandepu, "Leveraging FileNet Technology for Enhanced Efficiency and Security in Banking and Insurance Applications and Its Future with Artificial Intelligence (AI) and Machine Learning," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 12, no. 8, pp. 20-26, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Shin Yee Liew et al., "Navigating the Retail 4.0 Landscape: The Transformative Impact of Cloud Computing," *2023 IEEE 21st Student Conference on Research and Development*, Kuala Lumpur, Malaysia, pp. 499-507, 2023. [CrossRef] [Google Scholar] [Publisher Link]