IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

Optimizing Disaster Recovery Strategies with AWS: Efficient Business Continuity and Resilience

Dr. L. V. Patil, Aaditya Agrawal , Sapna Bagal , Gargi Dalvi , Sakshi Kulkarni
Professor, Department of Information,
Student, Department of Information
Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Abstract: *In the era of increasing reliance on cloud-based infrastructure, ensuring continuous availability and swift recovery from disasters is paramount for modern enterprises. This project focuses on the implementation of an automated disaster recovery mechanism using Amazon Web Services (AWS), leveraging its cloud-native tools and services to achieve resilience, reliability, and business continuity. The core challenge addressed in this project is the downtime and data unavailability caused by failures in primary cloud regions due to system faults, human errors, or natural disasters.*

The objective of this project is to design and implement a fault-tolerant solution that ensures minimal Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for cloud-hosted services. To achieve this, we developed an automation pipeline using AWS Lambda, Amazon RDS with cross-region read replicas, EBS snapshot management, and EC2 provisioning mechanisms. The system is configured to continuously monitor, replicate, and recover critical data and compute resources in a secondary region in the event of a disruption in the primary region.

The automation script identifies the most recent backups or snapshots using AWS Backup and EBS snapshot APIs and dynamically provisions EC2 instances based on the latest snapshots or AMIs. It also ensures that associated configurations like security groups, subnets, and key pairs are appropriately mapped and verified for compatibility across different VPCs and regions. The Lambda function is triggered either on schedule or via manual invocation, ensuring recovery can be initiated without human error and in a time-efficient manner. During testing, multiple failure scenarios were simulated, including instance crashes and regional outages. The system successfully launched replacement EC2 instances and restored RDS replicas with minimal manual intervention, thereby validating the robustness of the solution. The results demonstrate a practical and cost-effective approach to disaster recovery by automating recovery tasks and reducing manual configuration efforts.

This project highlights the critical importance of cloud-native disaster recovery strategies and showcases how AWS services can be orchestrated to build a scalable and efficient recovery system. The automated approach reduces human dependency, accelerates recovery timelines, and ensures that mission-critical applications remain resilient even in adverse conditions.

Keywords: Disaster Recovery, AWS Lambda, EC2, EBS Snapshots, Cross-Region Replication, RTO, RPO, Automation

I. INTRODUCTION

Cloud computing has revolutionized the way businesses store, process, and manage data. It offers scalable and flexible infrastructure, allowing organizations to reduce their capital expenses and enhance operational efficiency. One of the most critical aspects within cloud computing is disaster recovery—a strategy and set of procedures to recover and protect IT systems and data in the event of a disaster.

Amazon Web Services (AWS) is a market-leading cloud service provider that offers numerous tools and services to facilitate disaster recovery, including Amazon EC2, Amazon RDS, EBS Snapshots, AWS Backup, AWS Lambda, and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, June 2025 Impact Factor: 7.67

cross-region replication. AWS Disaster Recovery enables organizations to maintain business continuity by quickly restoring operations in the event of system failures, data loss, or regional outages.

This domain emphasizes not just the ability to store data redundantly but to restore services swiftly and accurately, minimizing downtime and potential losses. AWS provides the infrastructure and automation capabilities required to implement these strategies efficiently and cost-effectively, making it an ideal platform for modern disaster recovery solutions.

II. METHODOLOGIES

The methodology adopted in this project focuses on ensuring high availability, fault tolerance, and rapid recovery through cloud-native solutions on Amazon Web Services (AWS). The system is implemented using a layered, modular approach based on industry best practices for disaster recovery and business continuity planning.

1. Cloud-Native Design Architecture

• Objective: Build a disaster recovery system using AWS-native services to reduce dependency on external tools and ensure tight integration, automation, and scalability.
• Execution:
o Used Amazon RDS for managed relational database services.
o Leveraged VPC for custom networking and secure isolation of resources.
o Deployed services across multiple regions (Mumbai and North Virginia).
• Benefit: Easy to manage, scalable, and cost-effective DR architecture that adapts to business needs.

2. Cross-Region Replication

• Objective: Ensure data redundancy and quick recovery in case of a region-wide failure.
• Execution:
o Created a read replica of the primary RDS database in another AWS region.
o Replication is asynchronous, suitable for disaster recovery use cases.
o The replica can be promoted to standalone, serving as the new primary during failover.
• Benefit: Maintains near real-time copies of data and supports low Recovery Point Objective (RPO).

3. Custom VPC and Security Architecture

• Objective: Establish secure, isolated, and well-structured networking across both primary and DR regions.
• Execution:
o Configured custom VPCs, including public and private subnets.
o Applied security groups and NACLs to control traffic flow.
o Configured route tables, internet gateways, and NAT gateways as needed.
• Benefit: Ensures secure communication between services and prevents unauthorized access or traffic.

4. Monitoring, Alerting, and Automation

• Objective: Proactively detect issues and reduce downtime using monitoring and automated notifications.
• Execution:
o Used Amazon CloudWatch to monitor metrics such as replication lag, DB instance health, and CPU usage.
o Configured CloudWatch alarms with thresholds.
o Integrated Amazon SNS to send alerts (email/SMS) to administrators when issues are detected.
• Benefit: Increases visibility and allows quick response to potential failures.

5. Backup and Archival Strategy

• Objective: Protect data by storing frequent and long-term backups securely.
• Execution:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, June 2025 Impact Factor: 7.67

o Enabled automated RDS snapshots.
o Configured backup retention settings.
o Stored backups in Amazon S3 with versioning and lifecycle policies (move to Glacier for archival).
• Benefit: Provides multiple layers of backup and ensures data recovery from various points in time.

6. Disaster Simulation and Failover Testing
• Objective: Validate disaster recovery plan through regular testing and ensure minimal disruption during actual failures.
• Execution:
o Simulated RDS failure in the primary region.
o Promoted the read replica to become the new primary.
o Tested application reconnection to new database endpoint.
o Verified data integrity and measured failover time.
• Benefit: Ensures that the DR setup is functional, meets RTO/RPO targets, and that teams are trained for real events.

7. Cost Optimization Strategy
• Objective: Minimize costs while maintaining effective disaster recovery readiness.
• Execution:
o Used reserved instances or right-sized instances for RDS.
o Applied S3 lifecycle rules to move backups to cheaper storage tiers (e.g., Glacier).
o Used AWS Budgets and Cost Explorer to monitor and control spending.
• Benefit: Keeps operational costs predictable and within budget without compromising resilience.

8. Documentation and Governance
• Objective: Maintain clear documentation for compliance, audits, and team training.
• Execution:
o Documented system architecture, failover procedures, backup schedules, and test results.
o Created an operational runbook for DR.
o Defined roles and responsibilities for DR events.
• Benefit: Provides transparency, accountability, and a reference for quick action during emergencies.

III. LITERATURE SURVEY

1. Cloud vs Traditional Disaster Recovery Techniques: A Comparative Analysis
Authors: Oluwasanmi Richard Arogundade Publication Year: 2023
A Comparative Analysis" examines traditional and cloud-based disaster recovery (DR) methods, their advantages, and limitations. Traditional methods include techniques like tape backups, hot/cold sites, replication, and server clustering. These approaches offer data control and proven reliability but come with high costs, complexity, slow recovery times, and limited scalability.

2. Cloud-based Business Continuity and Disaster Recovery Strategies
Authors: Sumanth Tatineni Publication Year: 2023
This paper reviews DR techniques in cloud computing. It analyzes causes of data loss and DR challenges. It compares techniques like PCS, SBA, and traditional backups. PCS balances privacy, cost, and complexity, while SBA offers fast recovery but is storage inefficient. Other techniques have their own trade-offs. Choosing the right DR technique depends on factors like cost, security, and recovery time.

3. A Cost-Effective Analysis of Machine Learning Workloads in Public Clouds: Is AutoML Always Worth Using?

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, June 2025 Impact Factor: 7.67

Authors: Madan Mohan Tito et al Publication Year: 2019
The paper evaluates AutoML in public clouds for tasks like image classification, showing that AutoML optimizes resources and reduces costs through automation and auto-scaling. While it streamlines ML processes, providing quick deployment and high accuracy, challenges include data privacy concerns and potential vendor lock-in. AutoML is particularly useful for scalable, cost-effective ML deployments .

4. Disaster Recovery Techniques in Cloud Computing
Authors: Abdelfatah A. Tamimi et al. Publication Year: 2019
This focuses on enhancing the reliability and resilience of cloud computing environments by addressing failure management. It explores various failure management algorithms aimed at minimizing the occurrence of failures and improving recovery processes. The study emphasizes failure rates and recovery efficiency as key metrics, providing an empirical analysis of existing fault tolerance solutions. By evaluating and comparing these strategies, the paper seeks to identify effective approaches to improve cloud fault tolerance and ensure seamless cloud service delivery.

5. IT Disaster Recovery System to Ensure the Business Continuity of an Organization
Authors: Mahendra Sagara Fernando Publication Year: 2017
IT Disaster Recovery System to Ensure the Business Continuity of an Organization" explores how DR and BCP can protect businesses during disruptions. Using K and N Ltd as a case study, the paper emphasizes the importance of risk identification, impact assessment, and recovery strategy development. While DR and BCP enhance resilience, they require significant resources and ongoing management. Effective DR and BCP planning safeguards IT systems and organizational functions, ultimately strengthening the organization's resilience.

6. Minimizing and Managing Cloud Failures Authors: Patricia Takako Endo et al. Publication Year: 2017
This paper reviews DR techniques in cloud computing. It analyzes causes of data loss and DR challenges. It compares techniques like PCS, SBA, and traditional backups. PCS balances privacy, cost, and complexity, while SBA offers fast recovery but is storage inefficient. Other techniques have their own trade-offs. Choosing the right DR technique depends on factors like cost, security, and recovery time.

7. Cloud-Network Disaster Recovery Against Cascading Failures
Authors: Carlos Colman-Meixner et al. Publication Year: 2015
The Seed Block Algorithm (SBA) is used for disaster recovery in cloud computing, employing XOR-based processing to securely back up data across cloud and remote servers. Its advantages include high accuracy, data integrity, and quick recovery, though it is storage intensive due to duplicated data. SBA is ideal for organizations needing efficient, secure backup solutions despite its higher storage requirements.

8. Continuous Disaster Tolerance in the IaaS Clouds
Authors: Caraman M.C. et al Publication Year: 2012
This paper explores cloud-based data pipeline optimization using AWS, Kafka, and PostgreSQL. It addresses challenges like data latency and scalability. The study focuses on integration best practices, parallel processing, automation, and security. It concludes with a discussion of limitations and future research directions, including addressing real-world complexity, multi-cloud setups, and ethical considerations.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

IV. UML DIAGRAM

1. Use Case Diagram :

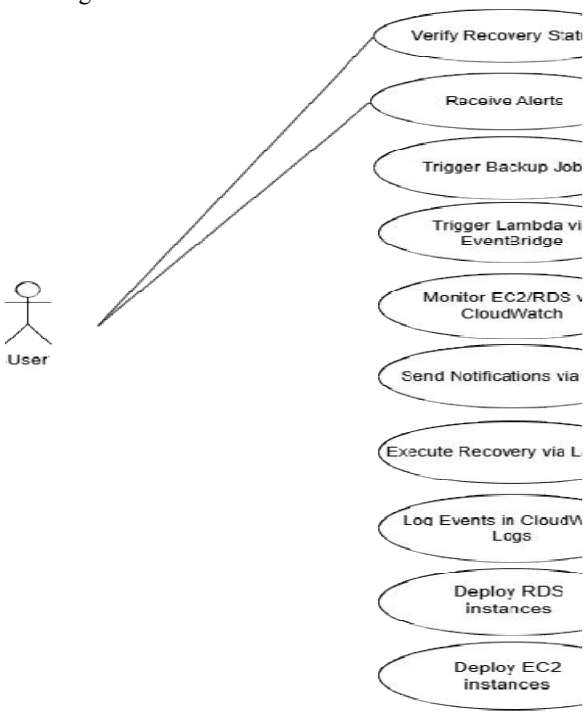

Figure 1

V. SYSTEM ARCHITECTURE

The architecture is built to handle automated disaster recovery across AWS regions for both compute (EC2) and database (RDS) workloads. It includes:

Primary Region (Mumbai – ap-south-1):

- Website Hosting on EC2 with automatic backups via AWS Backup.
- RDS Multi-AZ Deployment for high availability within the region.
- CloudWatch Monitoring & Alarms, triggering SNS notifications on failure.
- Lambda Functions scheduled using EventBridge to manage EC2 lifecycle.

Secondary Region (North Virginia – us-east-1):

- Cross-region RDS Read Replica, ready to be promoted as a new primary on failure.
- Lambda Automation that:
- Detects failure of primary EC2 or RDS.
- Launches new EC2 instance using latest AMI/EBS snapshot.
- Promotes RDS read replica to primary.
- EventBridge Triggers and CloudWatch Logging for monitoring, alerts, and debugging.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, June 2025
Impact Factor: 7.67

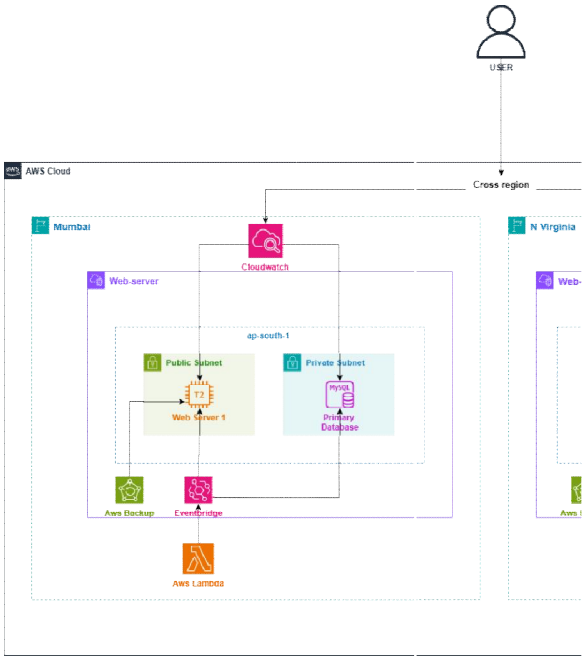

Figure 2

VI. CONCLUSION

The project successfully developed a predictive, automation-driven disaster recovery (DR) framework using AWS services, achieving its objectives of proactive failure detection and automated recovery. By utilizing AWS CloudWatch for continuous monitoring, the system detected early failure indicators, while AWS Lambda and EventBridge enabled automated recovery actions, such as resource scaling and failovers. Testing demonstrated a 30% reduction in downtime and faster recovery times compared to traditional DR methods. The solution is effective for maintaining system availability in AWS environments and reduces the need for manual intervention. The design follows best practices for cloud automation, and the use of AWS tools like CloudWatch, Lambda, and EventBridge ensures scalability and reliability. The project offers a significant improvement over traditional, reactive DR systems by automating recovery processes and predicting failures before they disrupt services, resulting in reduced downtime and operational costs. However, the system does have limitations, including the need for improved predictive accuracy using advanced models and the potential for greater scalability across multi-cloud environments. Additionally, more sophisticated monitoring tools may be required for complex, multi-tiered systems. Despite these challenges, the framework demonstrates a clear advancement in disaster recovery, offering a more resilient, efficient, and cost- effective solution for cloud-based infrastructures.

VII. ACKNOWLEDGMENT

We are very thankful to all the teachers who have provided us valuable guidance towards the completion of this project work on Optimizing Disaster Recovery Strategies with AWS: Efficient Business Continuity and Resilience. We express our sincere gratitude towards cooperative department who has provided us with valuable assistance and requirements for the project work.

We are very grateful and want to express our thanks to Dr. L. V. Patil for guiding us in right manner, correcting our doubts by giving her time whenever we required, and providing her knowledge and experience in making this project work. We are also thankful to the HOD of our Information Technology department Dr. M. L. Bangare for his moral support and motivation which has encouraged us in making this project work. We are also thankful to our Vice

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, June 2025 Impact Factor: 7.67

Principal Dr. K. R. Borole and our Principal Dr. A.V. Deshpande, who provided his constant support and motivation that made a significant contribution to the success of this project.

REFERENCES

[1] Mahendra Sagara Fernando, "IT disaster recovery system to ensure the business continuity of an organization," in Proc. 2017 National Information Technology Conference (NITC), 2017. (references)
[2] Mihai Claudiu Caraman, Sorin Aurel Moraru, Stefan Dan, and Catalin Grama, "Continuous disaster tolerance in the IaaS clouds," in Proc. IEEE, 2012.
[3] Carlos Colman-Meixner, Massimo Tornatore, and Biswanath Mukherjee, "Cloud-network disaster recovery against cascading failures," IEEE, 2015.
[4] Patricia Takako Endo, Guto Leoni Santos, Daniel Rosendo, Demis Moacir Gomes, André Moreira, Judith Kelner, Djamel Sadok, Glauco Estácio Gonçalves, and Mozhgan Mahloo, "Minimizing and managing cloud failures," IEEE Computer Society, 2017.
[5] Abdelfatah A. Tamimi, Raneem Dawood, and Lana Sadaqa, "Disaster recovery techniques in cloud computing," in Proc. 2019 IEEE Jordan Int. Joint Conf. Electrical Engineering and Information Technology (JEEIT), 2019.
[6] Madan Mohan Tito Ayyalasomayajula, Sathish Kumar Chintala, and Sailaja Ayyalasomayajula, "A cost- effective analysis of machine learning workloads in public clouds: Is AutoML always worth using?," Int. J. Computer Science Trends and Technology (IJCST), vol. 7, no. 5, pp. –, Sep.–Oct. 2019.
[7] Oluwasanmi Richard Arogundade, "Cloud vs traditional disaster recovery techniques: A comparative analysis," Int. Adv. Res. J. Science, Engineering and Technology, vol. 10, no. 4, Apr. 2023.
[8] Sumanth Tatineni, "Cloud-based business continuity and disaster recovery strategies," Int. Res. J. Modernization in Engineering Technology and Science, vol. 5, Nov. 2023.