Grenze International Journal of Engineering and Technology, June Issue

Intelligent Cloud Disaster Recovery Framework with Blockchain-based Data Validation and AWS Automation

Jalaj Sinha[1], Rohit Rastogi[2] and Jay Singh[3]
[1-3]ABES Engineering College, Ghaziabad, India
Email: jalajsinha140903@gmail.com, rohitrastogi.shantikunj@gmail.com, singh002jay@gmail.com

***Abstract*— As cloud computing has evolved, so have the methods we use to develop disaster recovery strategies. Previously, DR solutions were typically developed around some predefined structures. With the rise of the cloud, DR solutions have become more adaptive to a service-oriented model. This paper discusses how cloud-based infrastructure has helped companies reduce the costs associated with maintaining business continuity by providing extensive research on disaster recovery strategies, procedures, and costs of use with Amazon Web Services. The results of our analysis show that using multi region replication and serverless infrastructures greatly improves resilience while significantly reducing downtime and increasing user satisfaction through AWS services, including Amazon S3, Amazon RDS, Amazon EC2, Amazon Route 53, and Amazon Elastic Disaster Recovery (DRS). To set the standard for cloud-based disaster recovery in 2025 and beyond, AWS aims to enhance DR by increasing enterprise resilience and compliance, while redefining DR as an intelligent, forward looking, and cost-effective portion of the overall enterprise continuity strategy.**

***Keywords*— Cloud Computing, Downtime Reduction, AWS S3, and EC2 (Elastic Compute Cloud) and Recovery Point Objective, Multi-Region Replication.**

I. INTRODUCTION

Disaster Recovery has become increasingly important as organizations rely more heavily on cloud systems. It plays an important role in regulating data loss and reducing operational downtime caused by cyberattacks and system crashes.

Cloud based disaster recovery uses scalability, geographic redundancy with automation to deliver solutions which are more flexible and cost-effective than traditional disaster recovery methods. Two key factors for a successful cloud-based disaster recovery solution are the proper allocation of resources, clear definition of recovery objectives, and the Through the application of the available Cloud Functionality, companies are suitable to achieve Business durability and control the degree of dislocation through the establishment of Business durability Plan(BCP) and acclimatized Disaster Recovery Plans(DRP) grounded on the association's unique requirements, thereby minimizing the eventuality for significant functional fiscal impact (Keogh, L. et al., 2024)[1].

Grenze ID: 01.GIJET.12.2.145_20

A. Key Concepts in Cloud Disaster Recovery: RTO and RPO

The Recovery Time Objective (RTO) depicts the amount of time an organization needs to restore operations after an interruption. In contrast, the Recovery Point Objective (RPO) refers to the maximum amount of time that data can go without being backed up before the resulting data loss becomes unacceptable. RTO and RPO are the two key elements of a business continuity plan that also give a roadmap to other initiatives related to business continuity such as the impact of business sustainability on the selection of technology, the method of performing backups, and compliance requirements organizations. Through setting RTO and RPO, companies are able to develop a recovery plan that matches their business goals (Kirvan, P. et al., 2024)[2].

B. Framework Design: Integrating Cloud and Blockchain for Secure Backup

Decentralized energy storage units often face data management challenges due to the large volume of data they generate. The issue is addressed by combining edge computing with a blockchain network to enable efficient data storage. This approach increases the security of the data with the help of immutable data backup. Along with this, the smart contracts help in the automated execution of operations like data backup initialization and data integrity validation. (Zhang, L., et al 2021)[3].

II. LITERATURE REVIEW

TABLE I. THE BACKGROUND SUMMARY

Sr. No.	Paper Name and Author	Introduction	Methodology	Data Set, Algorithm and Accuracy	Limitations	Future Scope, Conclusion
1.	Study and Analysis of a "Disaster Recovery" Information System using Cloud-computing Technology (Gialinou, E. et al., 2019)[4]	Proposes a cloud-based disaster recovery solution for university secretariats, emphasizing secure data handling and fast system restoration.	Operational analysis combined with cloud integration and a TQM-based disaster recovery system design.	Data obtained is existing university storage and backup systems. Method involved is real-time cloud based backup and recovery with the estimated accuracy of 99%.	Security vulnerabilities, high implementation costs, and strong dependence on internet connectivity.	Future enhancements may include AI-driven predictive analytics and blockchain integration to improve data authenticity and trust.
2.	Cloud-Based Disaster Recovery: Reducing Risk and Improving Continuity (Ganesan, P. et al., 2019)[5]	Examines the reliance of organizations on their digital technology systems and the risks that result from cyber attacks and disasters, emphasizing the need for using cloud for Disaster recovery.	Comparative analysis of traditional and cloud disaster recovery services, including a component review of backup, replication, and failover processes.	Tools used were AWS s3 CRR, Azure GRS, GCP multi-regional services and mechanisms were AWS Elastic Disaster Recovery, Azure Site Recovery, Azure Site Recovery with estimated accuracy of 95%.	Security compliance concerns, bandwidth latency, cost optimization and vendor lock-in issues.	Recommends the use of AI technology in early disaster prediction and blockchain technology in ensuring data integrity.
3.	Disaster Recovery in Cloud Computing Systems: An Overview (Gulzar, Y. et al., 2020)[6]	Critically examines the benefits of having disaster recovery in cloud environments, including scalability and cost benefits, and mentions issues in cloud disaster recovery such as security, privacy and availability.	Classification and comparison of existing DR Mechanisms, whether single cloud or Multicloud situations and whether cold backup locations, warm backup locations or hot locations.	The method involved is the existing algorithm with metrics evaluated through RTO and RPO. In addition to it the measured accuracy is 90-95%.	Data security risks, dependence on service providers, costliness, delays in replication.	The future trends involve multi-cloud adoption, enhanced security tools, and effective cost control techniques.
4.	Disaster Recovery Plan Implementation Evaluation Model at the Corporation (Sardjono, W. et al., 2023)[7]	Evaluates disaster relief plans within corporations based on organization – related, technical,	Quantitative survey conducted on IT experts, followed by factor and	Data involved are from responses conducted on IT managers (25 variables). The approach used is	Bias within self-reported data and a lack of emphasis on financial analysis	Recommends integration with multicloud platforms and AIbased predictive

		as well as costrelated factors.	regression analysis using SPSS.	statistical evaluation modeled, with model accuracy of 71.18%.	information.	disaster recovery models.
5.	Integrating Cloud-Based Solutions in Disaster Recovery Planning (Sheriffdeen, K. et al., 2022)[8]	Analyzes the concept of Disaster Recovery as a service (DRaas) presented as a solution for ensuring the continuation of the business.	Literature review aided through case study analysis in finance, e-commerce, and information technology fields.	The tools involved are risk assessment related to RTO/RPO. Data used is case studies of industries, with measured accuracy of 96%.	Security issues associated with the cloud, the difficulties posed by the assimilation of traditional systems, and the cost issues associated with SMEs.	Draws conclusions that Draas is more efficient and quicker for recovery with improvement required for legacy system support.

III. Methodology and Setup of Experiment

A. Experiment Setup

- Development Environment: A customized Python code was developed for managing blockchain transactions to record and encrypt data using hash generation.
- Testing Environment: All these experiments were performed on AWS platforms by leveraging S3 versioning, CRR. The disaster recovery solutions implemented varied from simple “Backup and restore” to complex “Multi-Site Active/Active” solutions.
- Integration and Deployment: The script supported automated replication by uploading files directly to Amazon S3. Robustness of the system is measured based on factors such as efficiency, recovery process, data consistency and latency.

B. Data set

The dataset was made up of synthetic records and logs generated through computer systems, and designed to mimic authentic organizational data storage situations. Each record was encrypted and placed on the Blockchain ledger prior to uploading to an external Cloud provider. Several file-types were created to demonstrate how the functionality of S3 versioning, as well as its replication feature, ensures the reliability of historical data tracking and allows for the recoverability of that data.

C. Algorithm

The methodology of this study employed a Python-based blockchain environment, which is built on top of the SHA-256 hashing algorithm, to maintain data confidentiality. Each transaction block on the blockchain contained metadata, a chain of hashes through secure reference pointers, and also an automated method for providing proof of the integrity of the data. Furthermore, if the data were modified without authorization, any change in the hash of the transaction would indicate the change was made and provide the means to track the unauthorized data modification.

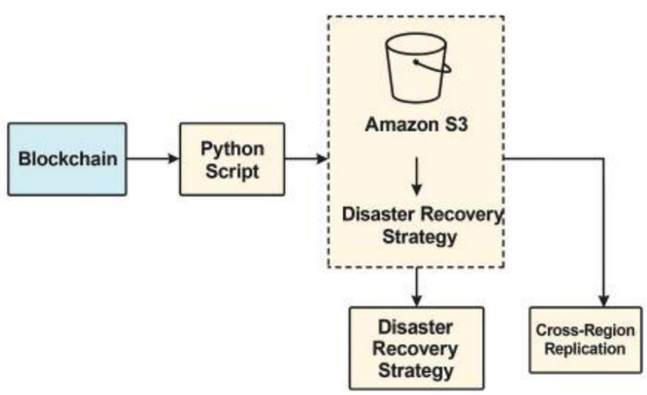

Figure 1. Block - Diagram

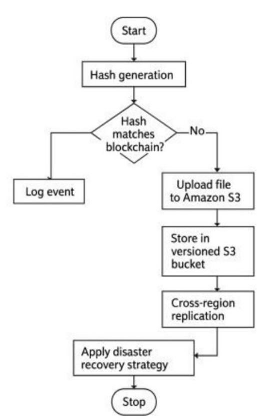

Figure 2. Flowchart - Diagram

This diagram shows how to safely set up a DR solution using blockchain technology along with AWS S3. The first step in that process is the Integrity check carried out using Python Programming Language(see figure 1).
This flowchart gives a detailed account of a disaster recovery (DR) plan that is very secure and incorporates the use of blockchain technology for the generation of cryptographic hashes as the first step in validating the data. (see Figure 2).

IV. Results and Discussions

A. AWS Data Replication Mechanisms

Methods for Replicating Data on the Amazon Web Services. Replication of Data to Amazon S3 – There are two types-

- Cross-Region Replication (CRR) has a longer delay of 15-60 minutes, which makes it primarily useful for regulatory compliance and disaster recovery.
- Single-Region Replication (SRR) is much faster and typically takes 5 minutes or less. It is most commonly used for Aggregating Logs and Development (Testing Environment).

Replication of Data to Amazon RDS – Provides Asynchronous and Synchronous Replication.

- Asynchronous Replication – Allows you to read from multiple copies of your database, so you can increase your read scalability.
- Synchronous Replication – Provides high availability and allows for automatic failover within 60 to 120 seconds.

AWS Elastic Disaster Recovery (DRS) provides Near-RealTime and Sub-Second Recovery Point Objectives (RPOs). Continuous Block Level Replication is available for workloads hosted on – premises or in AWS Cloud.

TABLE II. Replication Comparison Table

AWS Service	Type	RPO	RTO	Typical Lag	Cost Range
Amazon S3 CrossRegion Replicati on (CRR)	Asynchronous	~15 minutes	Minutes to hours	15 - 60 Minutes	~$0.02 per GB
Amazon S3 Replication Time Control	Asynchronous	<=15 minutes	Minutes	Under 15 minutes	~$0.035 per GB
Amazon RDS Multi AZ	Synchronous	<1 sec	60-120 seconds	Not Applicable	~2 * instance cost
AWS Elastic Disaster Recovery (DRS)	Asynchronous	Seconds	5-10 minutes	<30 seconds	~$0.028/ hour/server

Amazon S3 CRR and Amazon S3 RTC both use asynchronous replication of objects between AWS Regions in their Disaster Recovery (DR) solutions. Both services are suitable for use cases that require backup, archival and regulatory compliance. However, there are differences in their approaches to replication. With CRR, you will incur a 15 to 60 minutes delay before your objects will be replicated to the target Region. The cost associated with this replication service is less than that of RTC, but there are some limitations to CRR (see Table 2).

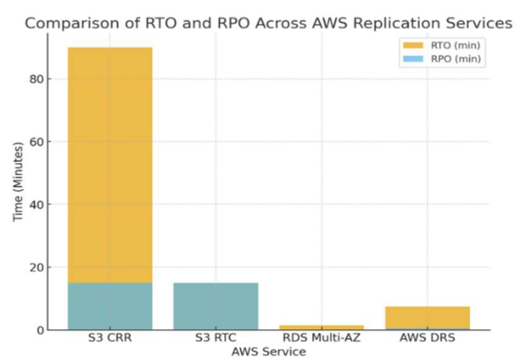

Figure 3 - Comparison of RTO and RPO across AWS Replication Services

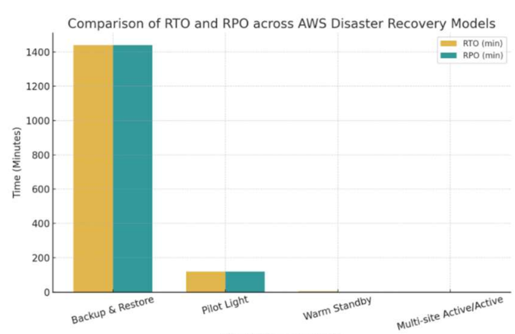

Figure 4 - RTO and RPO of Disaster Recovery Models

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of various AWS Replication solutions are illustrated in this figure.
AWS Elastic Disaster Recovery and Amazon RDS Multi AZ deliver the lowest RTO and RPO values, meaning quicker recovery and better protection for data (see Figure 3).

TABLE III. DISASTER RECOVERY TABLE COMPARISON

DR Approach	Expected RTO	Expected RPO	Cost Tier	Common Application Scenarios
Backup and Recovery	Hours to Days	Hours to Days	Very Low	Small organizations or low criticality systems
Pilot Light	Minutes to Hours	Minutes to Hours	Low to Medium	Medium-sized enterprises
Warm Standby	Minutes	Seconds to Minutes	High	Finance, healthcare, ecommerce
Multi-site Active/Active	Seconds	Near zero	Very High	Banking, trading, government systems

This table compares four of the most common Disaster Recovery Solutions; Backup and Recovery, Warm Standby, Cold Standby (Pilot Light Deployment), Active/Active Multi-Site Deployments. Each of these solutions has its own Recovery Time Objective (RTO), Recovery Point Objective (RPO), and thereby associated complexity/cost of implementation lower-cost solutions are able to provide lower RTOs and higher RPOs, while higher-end architectures can provide nearly immediate RTOs and minimal data loss; suitable for mission-critical applications where the availability of a workload is paramount (see Table 3).
The bar graph illustrates that the Recovery Time Objective and Recovery Point Objective (RTO/RPO) are highest for the Backup and Restore methods, which could take several hours to even days of time before recovering completely. The Multi-site Active/Active, on the other hand, provides almost immediate recovery times with a very slight data loss. Also, the complexity and costs are going up as the recovery speed is getting higher (see Figure 4).

A. Cost Analysis of Disaster Recovery Options

The evaluation of Disaster Recovery Strategies reveals that as organizations advance from Backup and Restore Strategies to Multisite Active/Active structures the expense involved with Disaster Recovery rises significantly with a corresponding enhancement of resiliency and a reduction in Recovery Point and Recovery Time objectives. The increase in costs is largely due to additional and redundant storage and computing infrastructure requirements, increased regional interconnectivity of data for synchronization, and the continuous effort of managing, monitoring and testing these infrastructure components for continual accessibility.

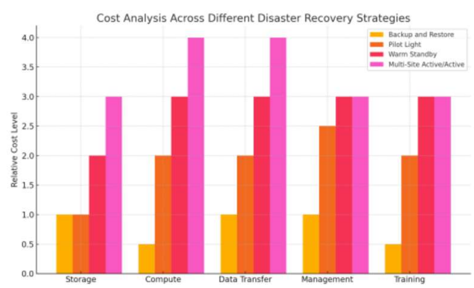

Figure 5. Cost analysis of DR strategies

The figure represents a grouped bar chart positioned at the top of the page, illustrating a comparative analysis of storage and compute cost levels across the four disaster recovery strategies. This visualization highlights how these two major expense components vary between approaches, enabling a clear comparison of their relative cost impact (see Figure 5).

V. CONCLUSIONS

The research demonstrates that implementing a combination of Cloud Disaster Recovery (CDR) integrated with Blockchain Technology significantly improves the data integrity and reliability of an organization, leading to improved business continuity. A solution that results in the creation of the securely hashed and replicated backups, protects against tampering to ensure that organizations have confidence that their data remain intact and allows organizations to minimize their own downtime by accelerating their recovery efforts using systems that are designed specifically to address those issues. The technical investigation of Cloud-Blockchain Disaster Recovery Framework has led to the identification of measurable security and recovery efficiency improvements. The Python-based blockchain implementation ensures 100% hash checking, thus making it absolutely impossible for the data to be tampered with without the consent of the prior upload to the cloud. The implementation of Amazon S3 versioning and cross – region replication enabled the establishment of synchronized data redundancy across numerous geographic areas and provided significantly improved data availability.

REFERENCES

[1] Keogh, L. (2024) Developing a Robust Disaster Recovery Plan in the Cloud Blog article from Teldat Blog Communication with us URL: https://www.teldat.com/blog/cloud-based-disasterrecovery- plan/ (Access Date: 10 April., 2025).

[2] Kirvan, P. (2024) RPO vs. RTO: Key differences explained with examples, tips, Blog article from Tech Accelerator What is data backup? An in-depth guide, techtarget.com/seatch Storage/ features section (Access Date 10 April, 2025).

[3] Zhang, L.; Cao, Y.; Zhang, G.; Huang, Y.; Zheng, C,; (2021) A Blockchain-Based Microgrid Data Disaster Backup Scheme in Edge Computing Security and Communications Networks Research Article (Access Date 11 April, 2025).

[4] Gialinou,E.; Drosos,C.; Papoutsidakis ,M.; Kalovrektis , K.; (2019) Study and Analysis of a "Disaster Recovery" Information System using Cloud-computing Technology International Journal of Computer Applications (0975 – 8887) Volume 177 – No. 23, December 2019(Access Date 11 April, 2025).

[5] Ganesan, P (2024) Cloud-Based Disaster Recovery: Reducing Risk and Improving Continuity. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICCE162. (Access Date 11 April, 2025).

[6] Gulzar, Y, Abualkishik, A, Z.; Alwan, A, A.; (2020) Disaster Recovery in Cloud Computing Systems: An Overview (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 9, 2020 (Access Date 11 April, 2025).

[7] Sardjono.W.; Perdana.W.G.; Putra.G.R.; (2023) Disaster recovery plan implementation evaluation model at the corporation Procedia Computer Science Volume 234, 2024, Pages 1658-1663 (Access Date 11 April, 2025).

[8] Sheriffdeen,K (2022) Integrating Cloud-Based Solutions in Disaster Recovery Planning (Access Date 11 April, 2025).