CLOUD COMPUTING

Next-Gen Cloud Backup:

Ransomware Defense and Multi-Cloud Reliability

Submitted To

Dr. Resham Raj Shivwanshi

Professor at Woxsen University

Submitted By

Palla Chetana Reddy - 23WU0104050

Obulagari Nandini – 23WU0104049

(chetanareddy.palla_2027@woxsen.edu.in)

(nandini.obulagari_2027@woxsen.edu.in)

Introduction

In today's digital economy, data has evolved into more than just information. Organizations rely on the cloud for storing and accessing information because it offers flexibility, scale, and cost efficiency. Yet, with this reliance comes vulnerability. Two persistent threats undermine the reliability of cloud storage: the rise of sophisticated ransomware attacks and the unavoidable reality of cloud service outages.

Ransomware has advanced far beyond simple file encryption; modern variants deliberately target synchronized backups, , leaving no way to recover data. At the same time, the heavy dependence on a single cloud provider creates a dangerous single point of failure. Even the most trusted platforms AWS, Azure, Google Cloud have experienced global outages, leaving millions of users without access to critical data.

This project introduces a **next-generation cloud backup framework** that addresses both problems together. It focuses on protecting backups from ransomware while making sure data remains available even if one cloud provider fails. With features like immutable storage, detection of suspicious uploads, time-delayed verification, and automatic multi-cloud failover, the solution is designed to be both practical and reliable for real-world use.

Problem Statement

1. **Ransomware Exposure** - Conventional backups mirror primary data instantly. If ransomware encrypts files, the backup is also compromised.
2. **Single-Point Dependency** - Outages in one cloud environment cause total inaccessibility of data.
3. **Fragmented Solutions** - Existing solutions often tackle either ransomware or availability, but rarely both together in a unified system.

Objectives

1. Design ransomware-resilient backups using immutability and time-delayed write verification.
2. Develop anomaly detection for spotting mass-encrypted or suspicious uploads.
3. Implement multi-cloud failover to ensure seamless availability when one provider fails.
4. Simulate real-world ransomware & outage scenarios for performance validation.
5. Deliver a functional prototype with clear real-world applicability.

Proposed Tech Stack and Cloud Services

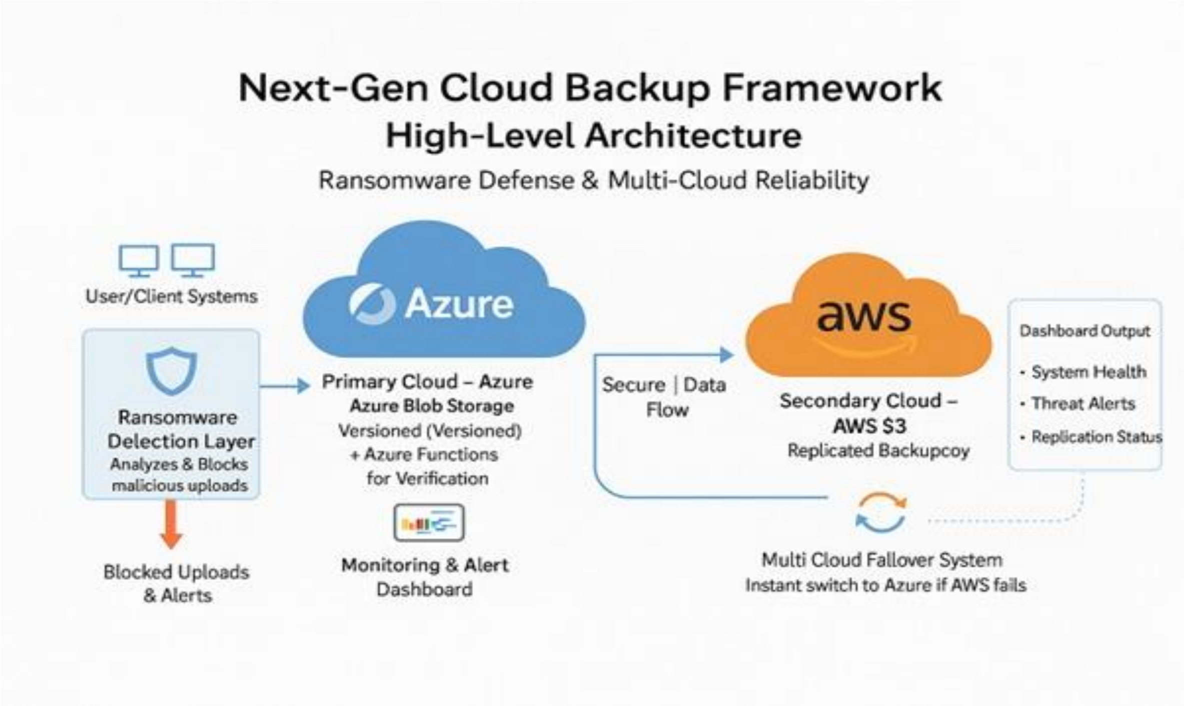
Layer	Tools / Services Used
Programming Language & Framework	Python 3.10 with Flask for backend development and API handling
Primary Cloud Platform	Microsoft Azure using Azure Blob Storage for secure and immutable primary backups, Azure Functions for automated verification and backup triggers, and Azure App Service for hosting the dashboard.
Secondary Cloud Platform	Amazon Web Services (AWS) using S3 Buckets for secondary backup storage and AWS Lambda for synchronization and replication between platforms.
Core Libraries	azure-storage-blob (Azure SDK), boto3 (AWS SDK for Python), pandas, and requests for automation, data handling, and cross-cloud operations.
Version Control & Collaboration	GitHub for code management, documentation, and collaborative development.
Development Tools	Visual Studio Code (IDE) and Git CLI for local development, testing, and deployment management.
Deployment Model	Multi-cloud backup architecture with automatic failover and data verification between AWS and Azure environments

High-Level Architecture

The project follows a multi-cloud backup and recovery framework that prioritizes data security, ransomware protection, and continuous availability. The system primarily uses Microsoft Azure for storage and processing, with AWS as the secondary cloud for redundancy and failover support.

Workflow:

1. The user initiates a backup via the Flask-based web interface.
2. Data is first stored in Azure Blob Storage, where immutability and versioning prevent ransomware tampering.
3. After verification, the data is automatically replicated to AWS S3 for secondary backup.
4. Azure Functions and AWS Lambda handle backup scheduling, verification, and synchronization.
5. If Azure experiences downtime or data issues, the system triggers an automatic failover to AWS, maintaining uninterrupted data access.



Timeline

Day	Task	Deliverable
Day 1	Set up free-tier cloud accounts (Azure + AWS). Create base storage containers in Azure Blob Storage and S3 buckets in AWS.	Multi-cloud environment ready
Day 2	Implement immutable storage in Azure Blob (using immutability policies) and test secure file upload.	Ransomware-resilient storage layer
Day 3	Develop an anomaly detection script in Python to identify suspicious or mass-encrypted uploads.	Functional anomaly detection module
Day 4	Add time-delayed verification before finalizing uploads to strengthen ransomware protection.	Secure and verified backup mechanism
Day 5	Build a Flask-based failover system to automatically switch between Azure (primary) and AWS (secondary) during outages.	Automated failover routing system
Day 6	Integrate all modules (storage + anomaly detection + failover). Simulate ransomware attack and outage scenarios for testing.	End-to-end prototype tested
Day 7	Perform final testing, refine project documentation, and prepare presentation materials.	Submission-ready project

Team

Palla Chetana Reddy – 23WU0104050 (chetanareddy.palla_2027@woxsen.edu.in)
Obulagari Nandini – 23WU0104049 (nandini.obulagari_2027@woxsen.edu.in)

Expected Outcomes

1. **Secure Backups** – Immutable and verified, ensuring ransomware cannot overwrite recovery points.
2. **Resilient Access** – Multi-cloud failover guarantees uninterrupted data availability.
3. **Complete Prototype** – A tested, functional system showcasing defense against both attacks and outages.
4. **Innovative Design** – A rarely attempted integration of security and resilience in academic settings.
5. **Practical Impact** – A framework directly relevant for enterprises seeking reliable disaster recovery solutions.