**aws**

# Placement Empowerment Program
## *Cloud Computing and DevOps Centre*

Task:

Use Cloud StorageCreate a storage bucket on your cloud platform and upload/download files. Configure access permissions for the bucket.

Name: Venkata Sai M          Department:CSE

# Introduction

Cloud storage provides a scalable, secure, and cost-effective solution for storing and managing data in the cloud. This Proof of Concept (POC) focuses on creating a cloud storage bucket, uploading and downloading files, and configuring access permissions to ensure data security and controlled accessibility.

In this POC, we will:

- Set up a cloud storage bucket on a cloud platform (AWS S3, Google Cloud Storage, or Azure Blob Storage).
- Upload and download files to and from the storage bucket.
- Configure access control policies to restrict or grant permissions based on security requirements.

This implementation demonstrates how cloud storage can be utilized for various

applications, including backups, media hosting, and distributed data access.

# Overview

This Proof of Concept (POC) explores the implementation of cloud storage services to efficiently manage and control file storage, access, and retrieval. The objective is to demonstrate the capabilities of cloud storage solutions for handling data in a scalable and secure manner.

**Key Steps Involved:**

1. **Create a Cloud Storage Bucket**
   - Choose a cloud provider (AWS S3, Google Cloud Storage, or Azure Blob Storage).
   - Set up a new storage bucket with appropriate configurations.
2. **Upload and Download Files**
   - Use cloud CLI or SDKs to upload files to the bucket.
   - Retrieve or download files from the cloud storage for verification.
3. **Configure Access Permissions**
   - Define bucket-level access policies.
   - Set up public or private access controls as per security requirements.
   - Implement IAM roles or ACLs to manage user permissions

# Objectives

1. Create a Cloud Storage Bucket
2. Enable File Upload and Download
3. Implement Access Control Mechanisms
4. Ensure Data Security and Integrity
5. Evaluate Performance and Scalability
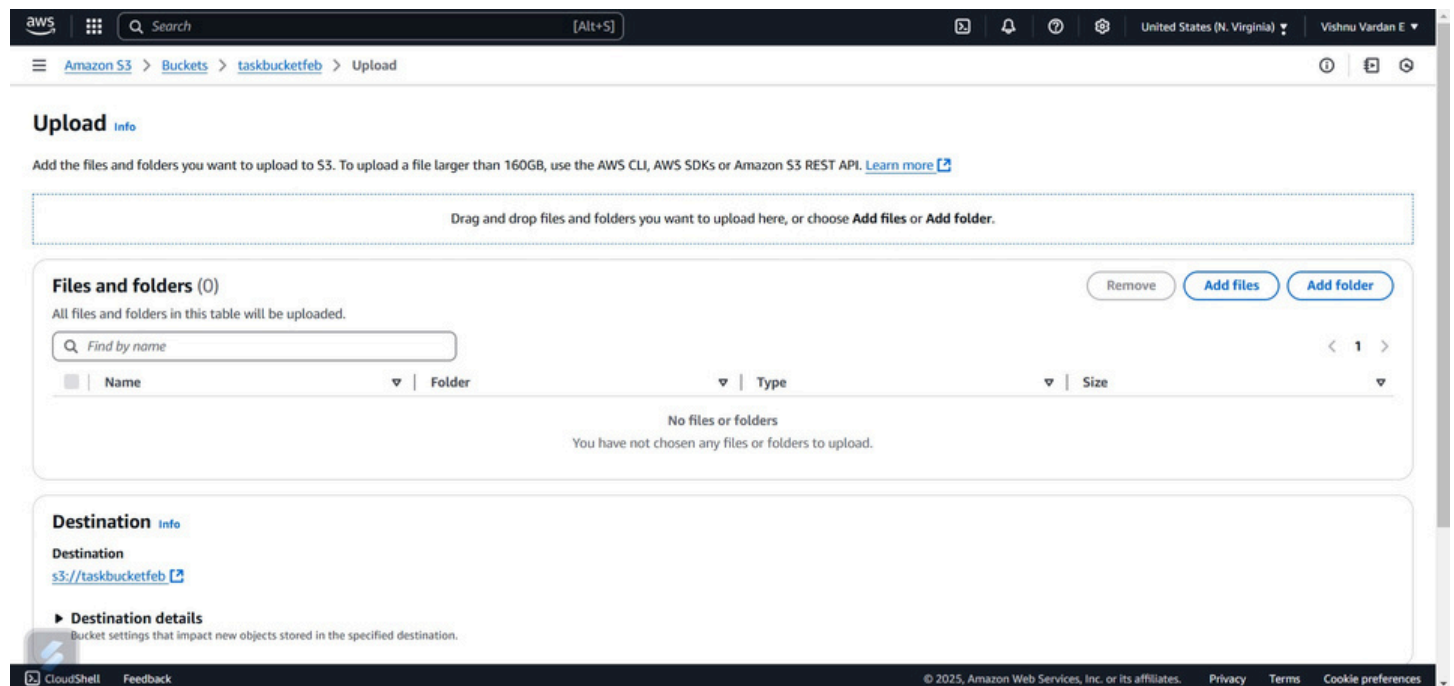6. Document and Analyze Findings

# Step-by-Step Overview

# Step 1:

### Navigate to the AWS Managment Console

In a Managment Console go to S3 and create a new bucket

# Step 2:

Now Upload a file in the S3 bucket



# Step 3:

Touch the bucket and navigate to the permission in top and enable the public access to the bucket then enter the given bucket policy in a edit bucket policy

# taskbucketfeb Info

Objects | Metadata | Properties | **Permissions** | Metrics | Management | Access Points

## Permissions overview

**Access finding**

Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work ☐

View analyzer for us-east-1

## Block public access (bucket settings) [ Edit ]

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more ☐

**Block *all* public access**

⊘ On

▶ **Individual Block Public Access settings for this bucket**

## Bucket policy [ Edit ] [ Delete ]

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more ☐

---

# Edit Block public access (bucket settings) Info

## Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more ☐

☐ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

[ Cancel ]  [ **Save changes** ]

```
{
  "Version": "2012-10-17",
 "Statement": [
   {
     "Effect": "Allow",
     "Principal": "*",
     "Action": "s3:GetObject",
     "Resource": "arn:aws:s3:::your-bucket-name/*"
   }
```

]
}

# Step 4:

Then click on the save changes to the bucket policy

## Step 5:

Then finally navigate to the bucket and click on the copy url and then enter that address to the chrome

+ 7 8 9 - 4 5 6 * 1 2 3 / 0 . = C

# Expected Outcomes:

- Successful creation of a cloud storage bucket.
- Smooth file upload and retrieval process.
- Properly configured access control policies ensuring secure storage.

This POC provides a foundational understanding of cloud storage, making it easier to integrate into applications for large-scale data handling, backups, and media hosting.