

## **Placement Empowerment Program**

### ***Cloud Computing and DevOps Centre***

#### **Use Cloud Storage**

*Create a storage bucket on your cloud platform and upload/download files. Configure access permissions for the bucket.*

Name: Priyanka Mary A

Department : CSE

# Introduction and Overview

In this (PoC), we will explore AWS S3 (Simple Storage Service) to understand its functionality as a reliable cloud storage solution. The task involves creating an S3 bucket, uploading and downloading files, and configuring access permissions to manage who can access the stored data. This PoC demonstrates S3's versatility in securely storing and retrieving files, both publicly and privately. We will also set bucket policies to control access and test public URLs for hosted files. By completing this task, we gain hands-on experience with S3 and its key features, such as scalability, security, and cost-efficiency.

## Objective

The goal of this project is to:

1. **Understand AWS S3 Basics:** Learn how to create, configure, and manage an S3 bucket for cloud storage.
2. **File Operations:** Gain hands-on experience in uploading, downloading, and managing files within the S3 bucket.
3. **Access Control:** Configure bucket policies and permissions to manage secure and public access to stored data.

## Importance of Storage Bucket(S3)

**Foundation for Advanced Use Cases:** Learning how to handle S3 storage is a stepping stone for mastering cloud computing and deploying large-scale applications.

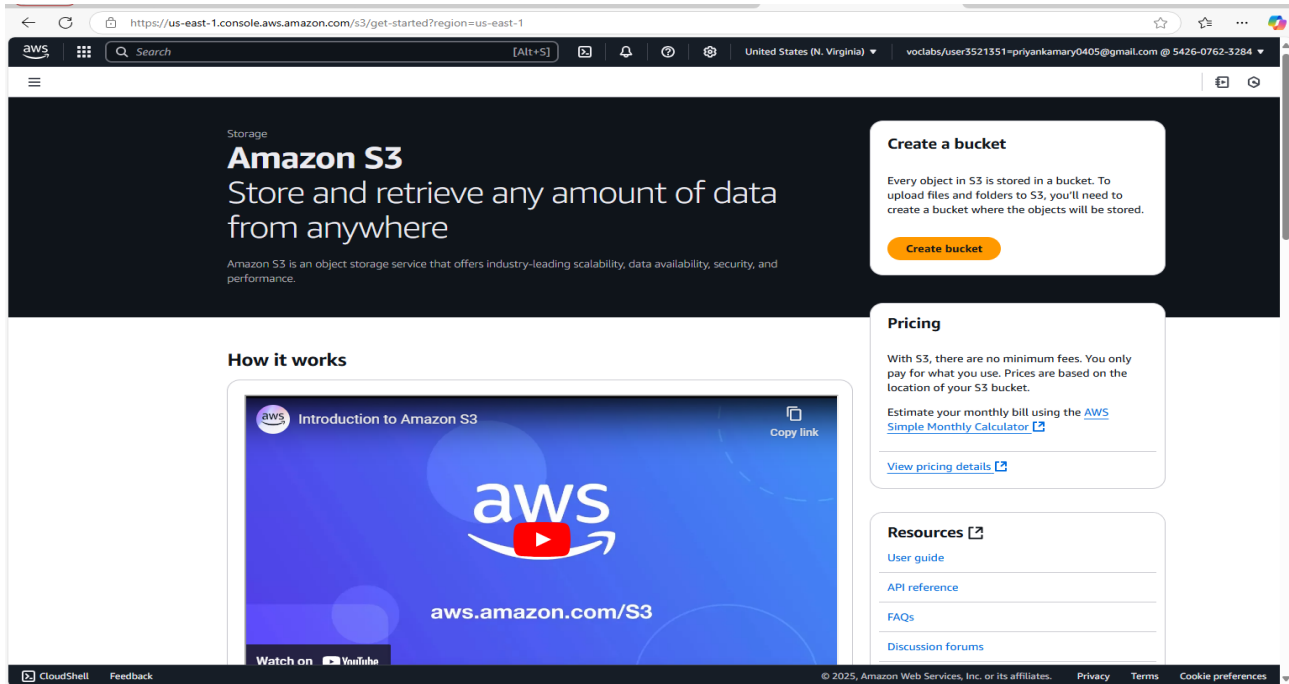
**Hands-On Learning of Cloud Storage:** AWS S3 provides a practical platform to learn cloud storage concepts, enabling users to create buckets, upload/download files, and manage data at scale.

**Data Security and Access Control:** By configuring bucket policies and permissions, users can secure their data and manage who can access it.

# Step-by-Step Overview

## Step1:

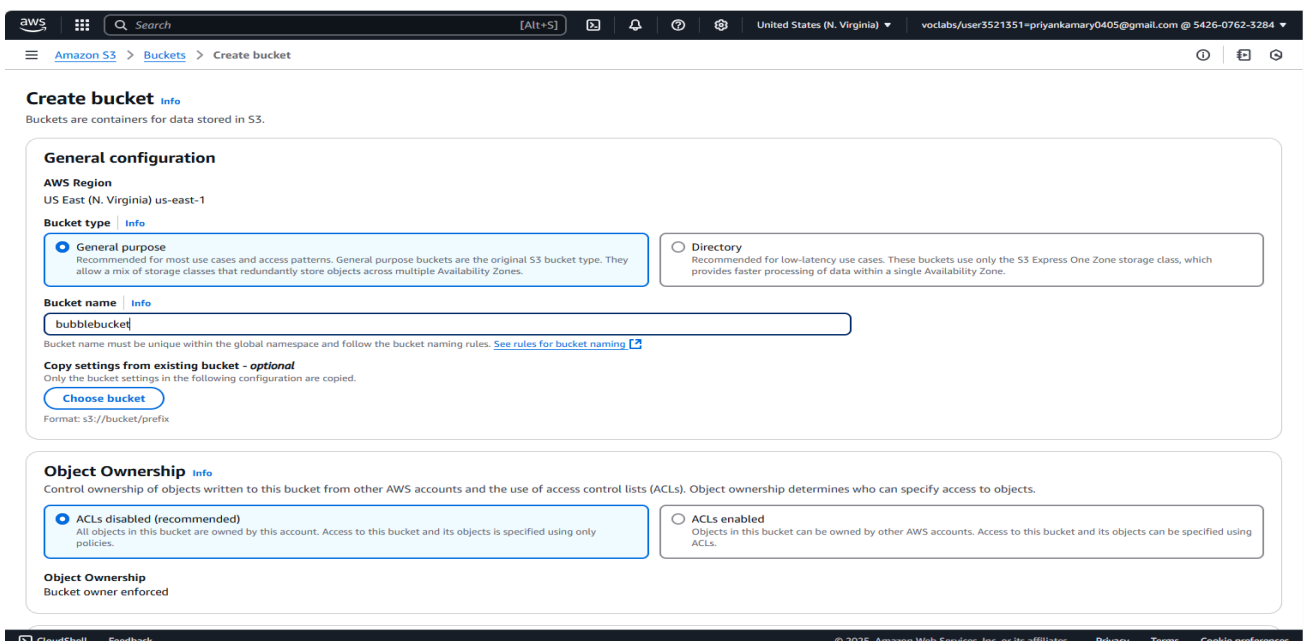
Go to the AWS Management Console, Search for and click on S3



## Step 2 :

Click the "Create bucket" button.

Enter a unique bucket name (e.g., my-storage-bucket-123).



## Step 3 :

Leave "Block all public access" enabled for now (you can modify it later).

**Object Ownership** [Info](#)  
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**Object Ownership**  
Bucket owner enforced

**Block Public Access settings for this bucket**  
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 this bucket and its 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 this bucket 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.

**Bucket Versioning**  
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

**Bucket Versioning**

## Step 4 :

Click "Create bucket".

**Successfully created bucket "ricebucket"**  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

► **Account snapshot - updated every 24 hours** [All AWS Regions](#) [View Storage Lens dashboard](#)  
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

**General purpose buckets** | Directory buckets

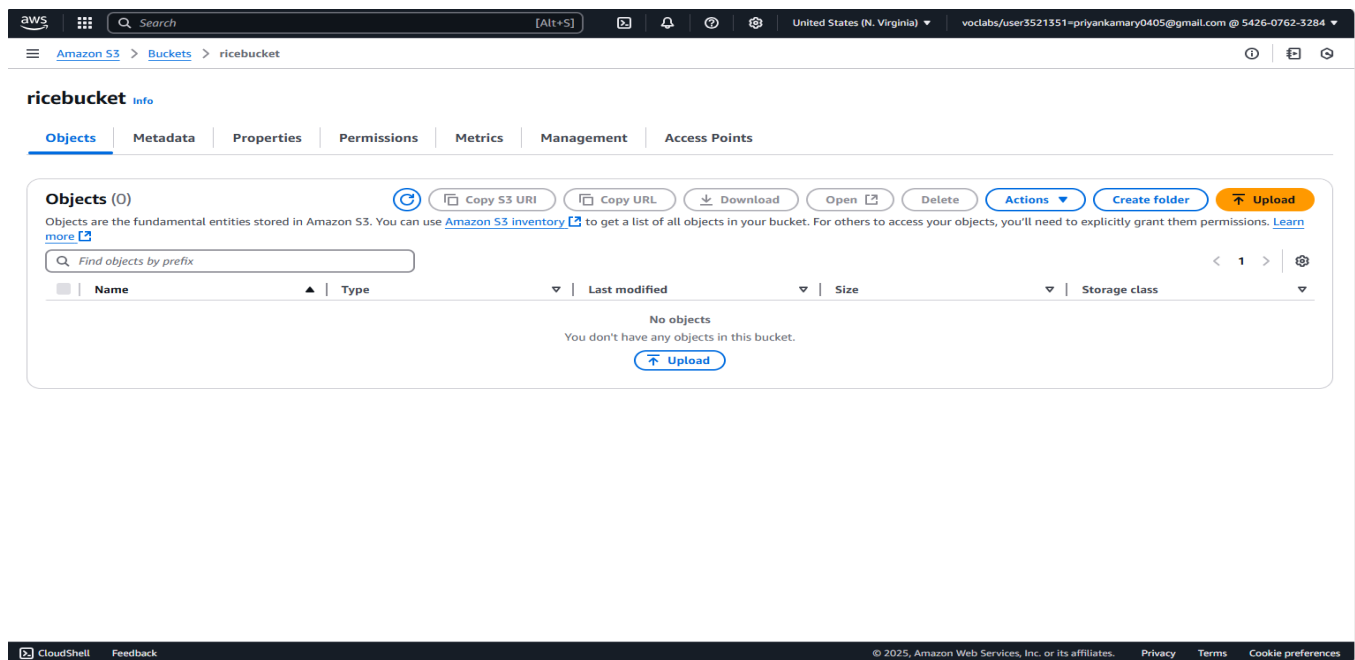
**General purpose buckets (1)** [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	<a href="#">ricebucket</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	January 31, 2025, 10:58:03 (UTC+05:30)

## Step 5 :

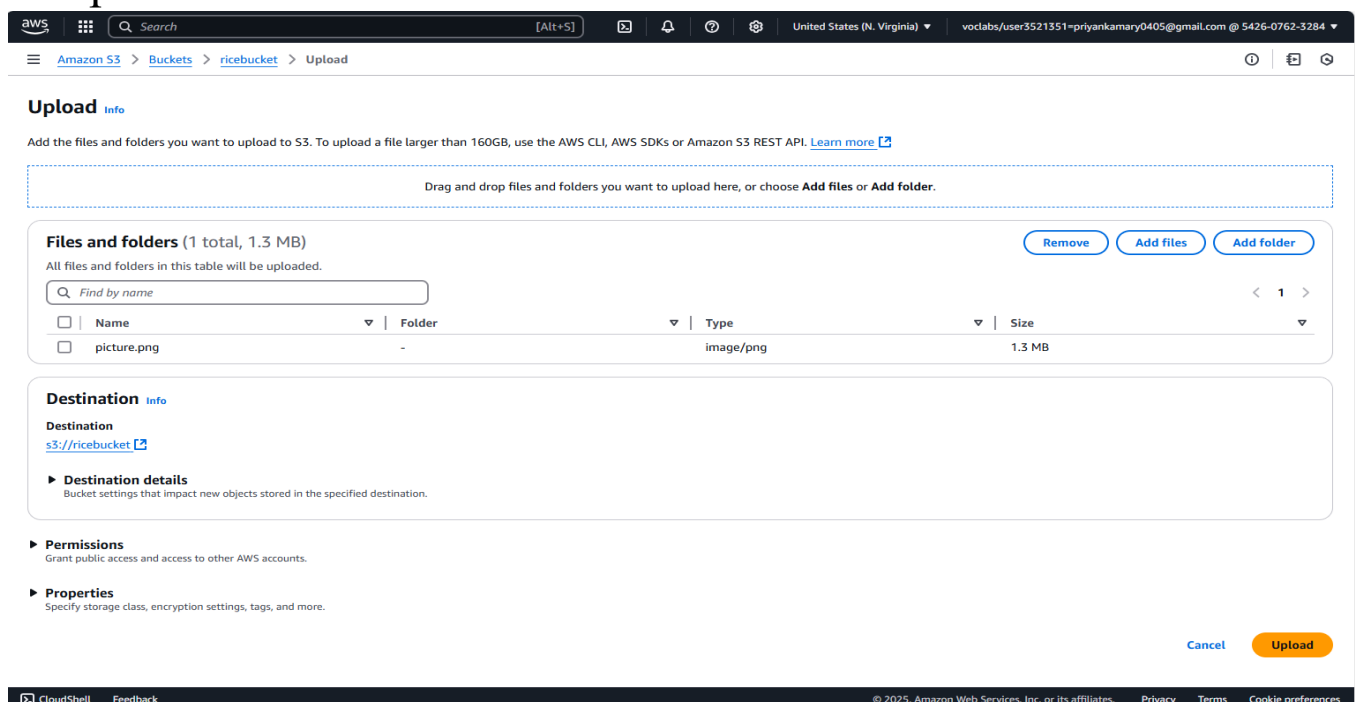
Open your newly created bucket from the S3 console.



## Step 6 :

Click "Upload" and then,

Drag and drop your file(s) or use the Add files button. Click Upload to complete.



Upload succeeded  
For more information, see the [Files and folders](#) table.

### Upload: status

After you navigate away from this page, the following information is no longer available.

**Summary**

<b>Destination</b> s3://ricebucket	<b>Succeeded</b> ✔ 1 file, 1.3 MB (100.00%)	<b>Failed</b> ✘ 0 files, 0 B (0%)
---------------------------------------	--	--------------------------------------

**Files and folders** | Configuration

**Files and folders** (1 total, 1.3 MB)

Find by name

Name	Folder	Type	Size	Status	Error
<a href="#">picture.png</a>	-	image/png	1.3 MB	✔ Succeeded	-

Step 7 :

Go to the uploaded file in your bucket. Click the file name to open its details. Select Download to save the file locally.

Amazon S3 > Buckets > ricebucket > picture.png

**picture.png** Info

Copy S3 URI | Download | Open | Object actions

**Properties** | Permissions | Versions

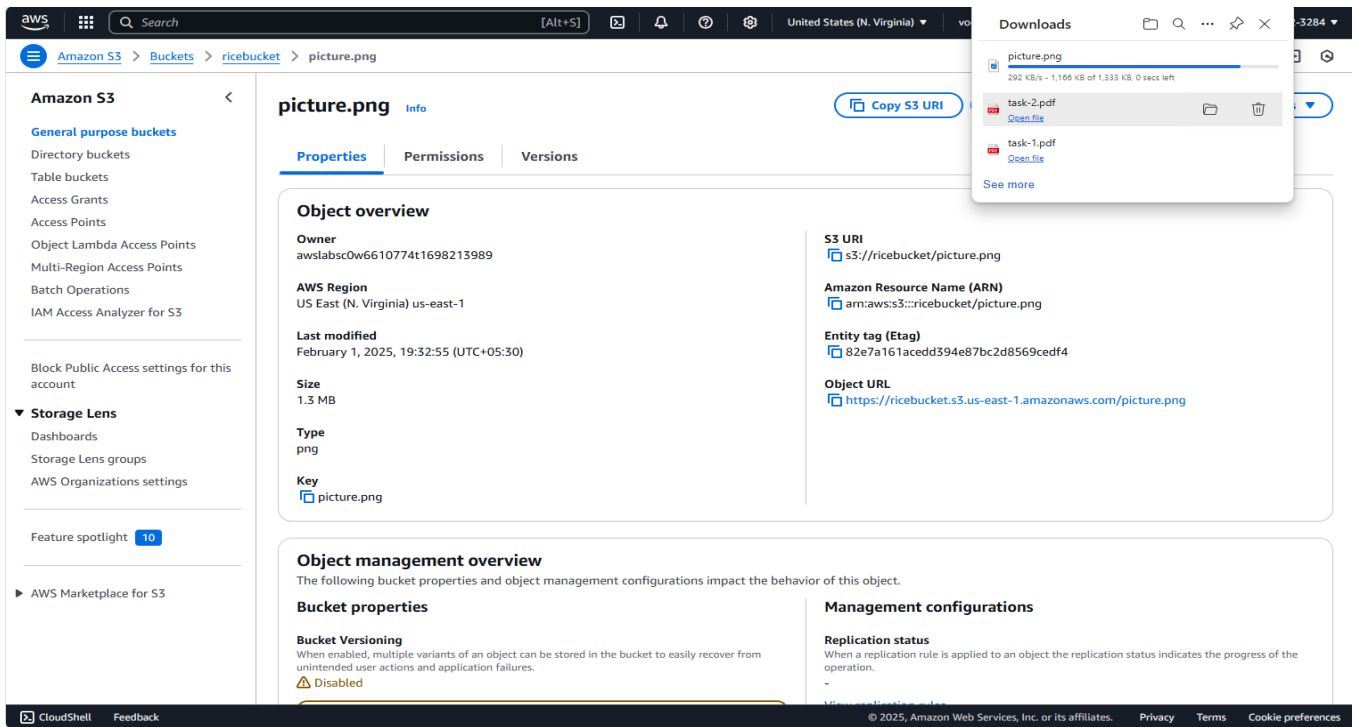
**Object overview**

<b>Owner</b> awslabsc0w6610774t1698213989	<b>S3 URI</b> s3://ricebucket/picture.png
<b>AWS Region</b> US East (N. Virginia) us-east-1	<b>Amazon Resource Name (ARN)</b> arn:aws:s3:::ricebucket/picture.png
<b>Last modified</b> February 1, 2025, 19:32:55 (UTC+05:30)	<b>Entity tag (Etag)</b> 82e7a161acedd394e87bc2d8569cedf4
<b>Size</b> 1.3 MB	<b>Object URL</b> <a href="https://ricebucket.s3.us-east-1.amazonaws.com/picture.png">https://ricebucket.s3.us-east-1.amazonaws.com/picture.png</a>
<b>Type</b> png	
<b>Key</b> picture.png	

**Object management overview**

The following bucket properties and object management configurations impact the behavior of this object.

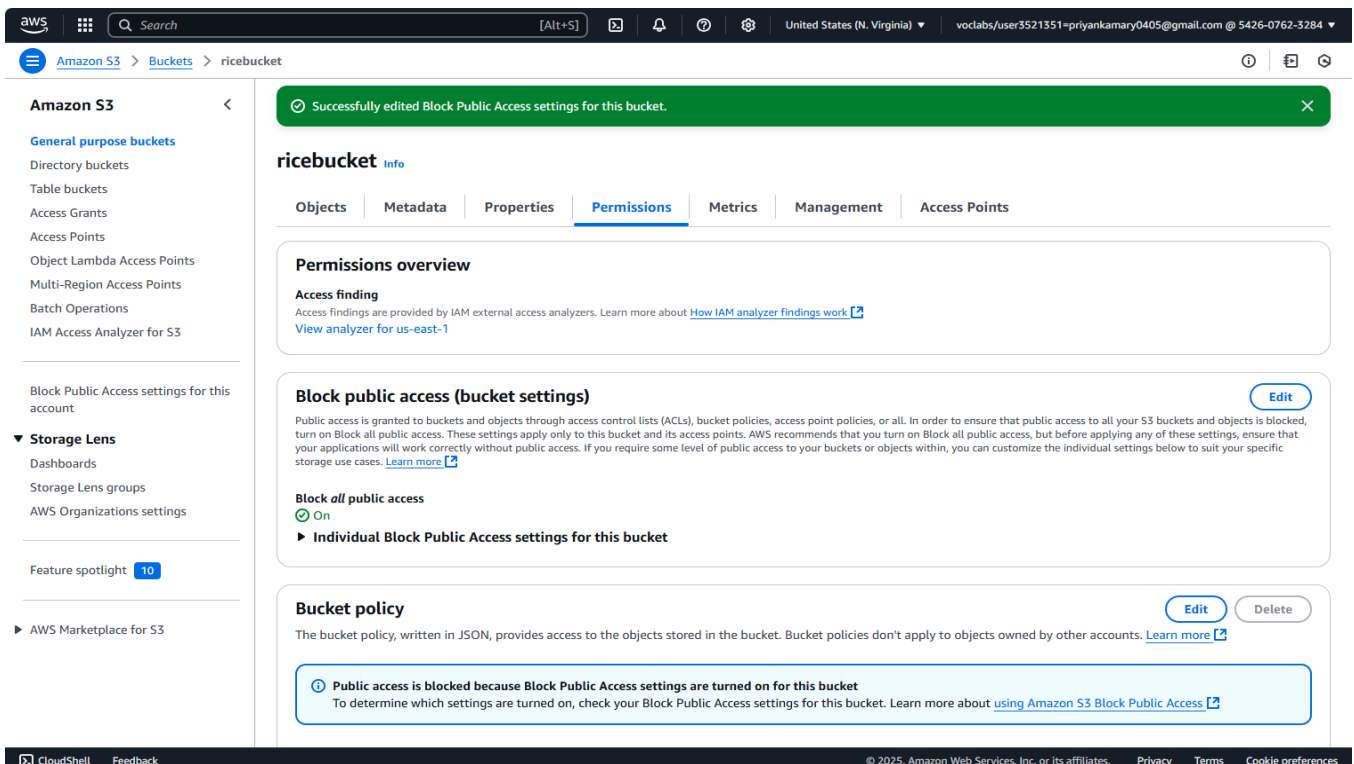
<b>Bucket properties</b> <p><b>Bucket Versioning</b> When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures. ⚠ Disabled</p>	<b>Management configurations</b> <p><b>Replication status</b> When a replication rule is applied to an object the replication status indicates the progress of the operation. -</p>
---	---



## Step 8 :

Open your bucket and navigate to the "Permissions" tab.

Under Block public access, click Edit and uncheck "Block all public access". Confirm by typing "confirm" and save.



Successfully edited Block Public Access settings for this bucket.

### ricebucket

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**  
 Off

► **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](#)

No policy to display. [Copy](#)

## Step 9 :

In the "Permissions" tab, scroll to Bucket Policy and click Edit. Replace your-bucket-name with your actual bucket name. Save changes.

### Edit bucket policy

**Bucket policy** [Policy examples](#) [Policy generator](#)

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](#)

**Bucket ARN**  
 `arn:aws:s3:::ricebucket`

**Policy**

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": "s3:GetObject",
8       "Resource": "arn:aws:s3:::ricebucket/*"
9     }
10  ]
11 }
```

**Edit statement**

Select a statement

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)



aws

Search

[Alt+S]

United States (N. Virginia)

voclabs/user3521351-priyankamary0405@gmail.com @ 5426-0762-3284

Amazon S3

Buckets

ricebucket

Amazon S3

General purpose buckets

Directory buckets

Table buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight 10

AWS Marketplace for S3

Successfully edited bucket policy.

ricebucket

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)

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

Off

Individual Block Public Access settings for this bucket

Bucket policy

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](#)

```
{
  "Version": "2012-10-17",
  "Statement": [

```

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step10:

Use the S3 bucket URL or public file URL to test access permissions.

aws

Search

[Alt+S]

United States (N. Virginia)

voclabs/user3521351-priyankamary0405@gmail.com @ 5426-0762-3284

Amazon S3

Buckets

ricebucket

Amazon S3

General purpose buckets

Directory buckets

Table buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight 10

AWS Marketplace for S3

ricebucket

Info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Object URL Copied

Objects (1)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	<a href="#">picture.png</a>	png	February 1, 2025, 19:32:55 (UTC+05:30)	1.3 MB	Standard

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



## Expected Outcome

By completing this POC, you will:

1. Successfully create an AWS S3 bucket and perform file upload/download operations.
2. Configure and validate access permissions, ensuring secure or public access as needed.
3. Gain a solid understanding of S3's functionality, enabling its use in real-world cloud-based applications.