

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: Bhavyaa.V

Department : IT

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.

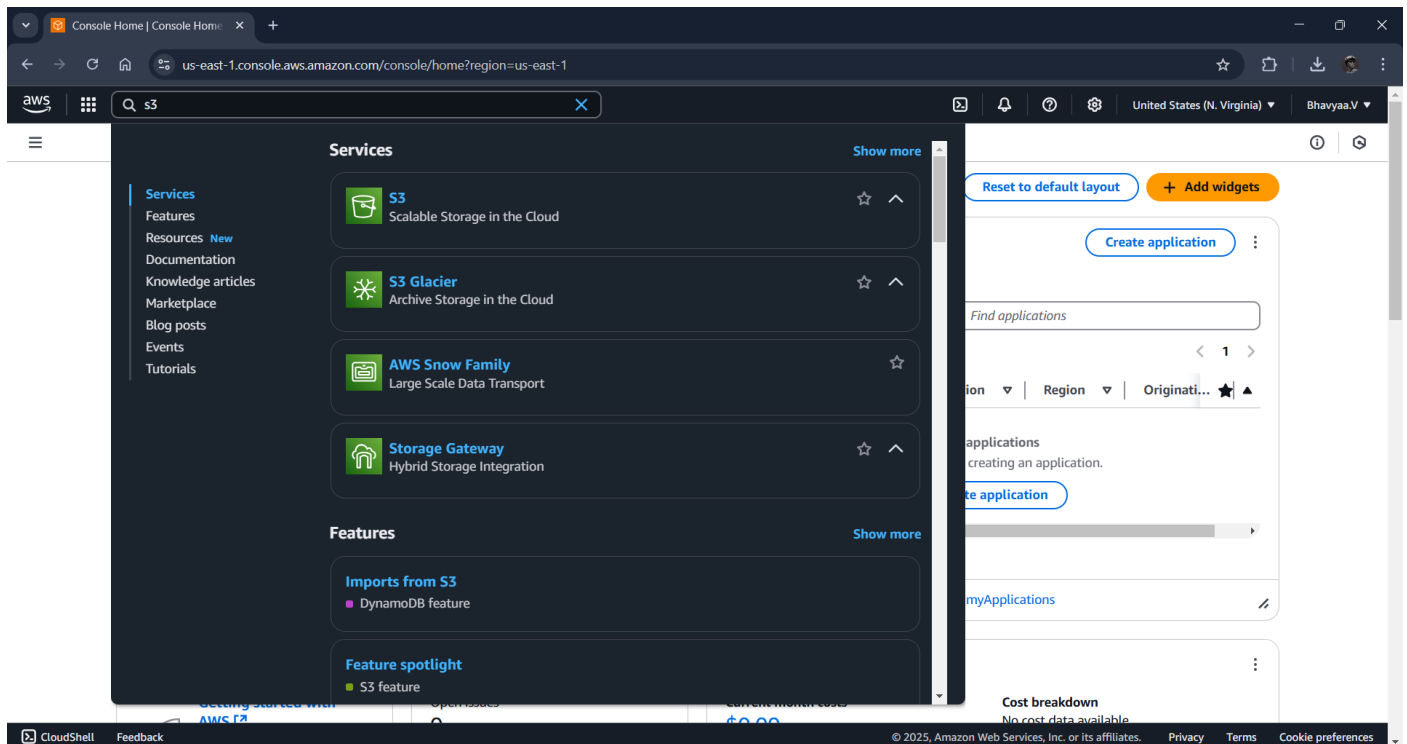
Hands-On Learning of Cloud Storage: AWS S3 provides a practical platform to learn cloud storage concepts, enabling users to create buckets, upload/download files, and manage data at scale.

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.

Create S3 bucket | S3 | us-east-1

us-east-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general

Amazon S3 > Buckets > Create bucket

Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

mynewbucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

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.

CloudShell Feedback

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

Step 3 :

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

Create S3 bucket | S3 | us-east-1

us-east-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general

Amazon S3 > Buckets > Create bucket

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

☒ **Disable**

☐ **Enable**

CloudShell Feedback

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

Step 4 :

Click "Create bucket".

The screenshot shows the AWS S3 console interface. At the top, a green notification bar states: "Successfully created bucket 'mynewbucket080205'. To upload files and folders, or to configure additional bucket settings, choose View details." Below this, there's a section for "Account snapshot - updated every 24 hours" with a "View Storage Lens dashboard" link. The main content area is titled "General purpose buckets" and includes a search bar, a table of buckets, and a "Create bucket" button. The table lists one bucket: "mynewbucket080205" in the "US East (N. Virginia) us-east-1" region, created on "February 1, 2025, 17:22:22 (UTC+05:30)".

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

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
mynewbucket080205	US East (N. Virginia) us-east-1	View analyzer for us-east-1	February 1, 2025, 17:22:22 (UTC+05:30)

[CloudShell](#) [Feedback](#) © 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step 5 :

Open your newly created bucket from the S3 console. Click "Upload" and then drag and drop your file(s) or use the Add files button. Click Upload to complete.

The screenshot shows the AWS S3 console interface for the "Upload objects" page. A green notification bar states: "Upload succeeded. For more information, see the Files and folders table." Below this, there's a section for "Upload: status" with a "Close" button. The main content area is titled "Files and folders" and includes a search bar, a table of files, and a "Configuration" tab. The table lists one file: "Untitled document (13).pdf" in the "application/pdf" type, with a size of "145.2 KB" and a status of "Succeeded".

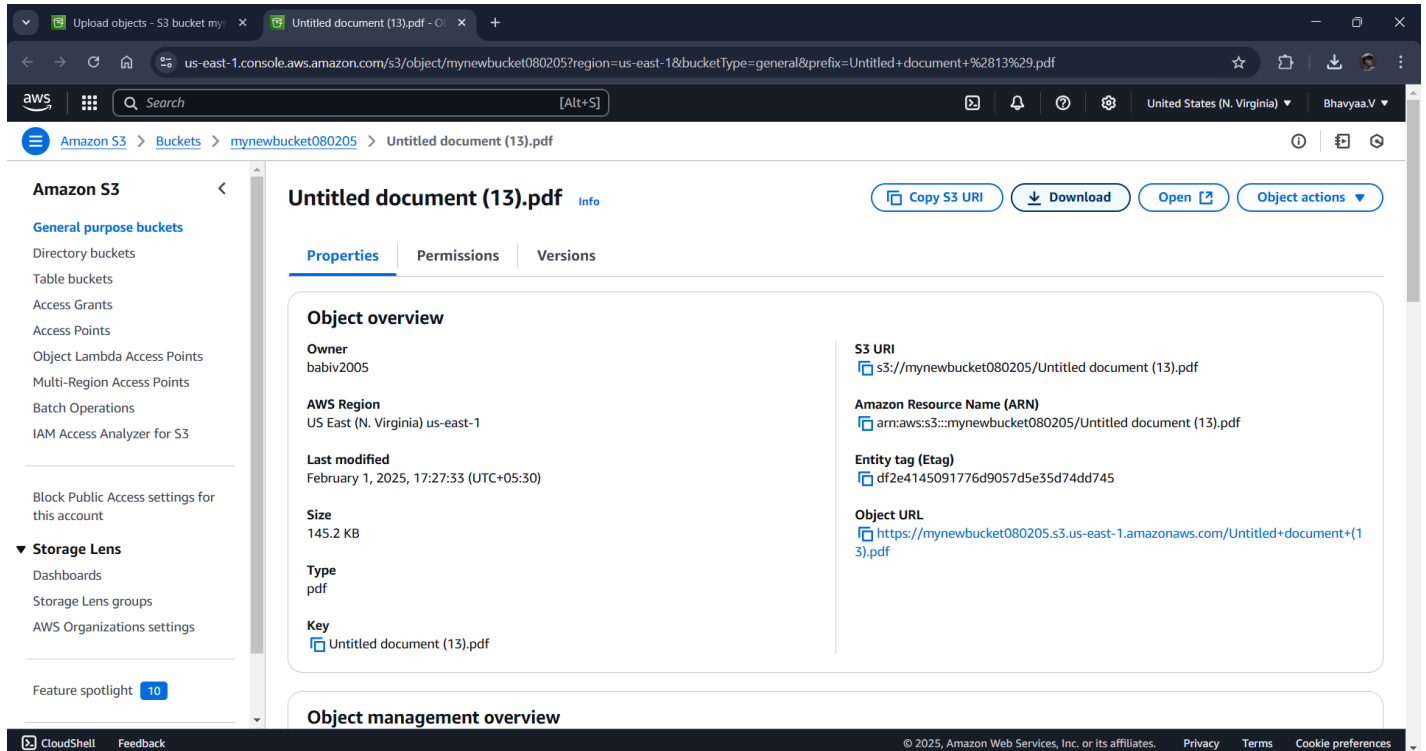
Upload objects - S3 bucket my [x](#)

[us-east-1.console.aws.amazon.com/s3/upload/mynewbucket080205?region=us-east-1&bucketType=general](#)

[CloudShell](#) [Feedback](#) © 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step 6 :

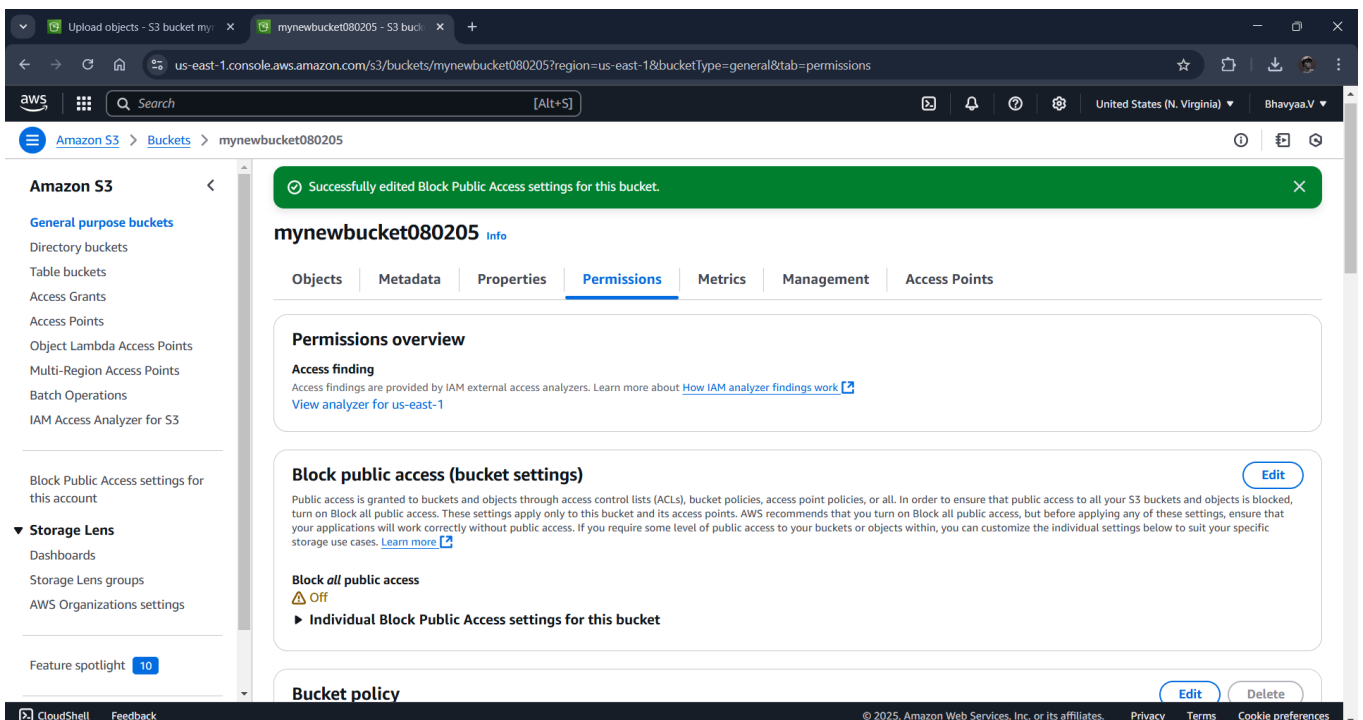
Go to the uploaded file in your bucket. Click the file name to open its details. Select Download to save the file locally.



Step 8 :

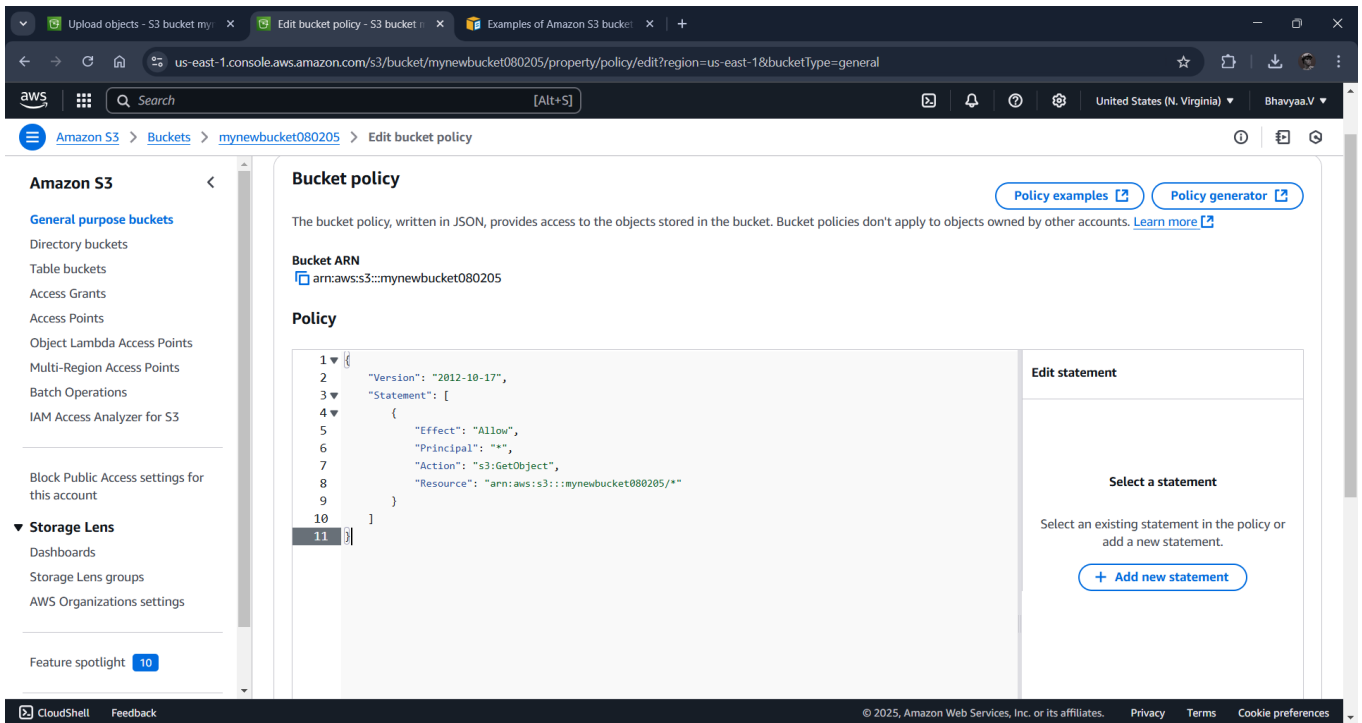
Open your bucket and navigate to the "Permissions" tab.

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



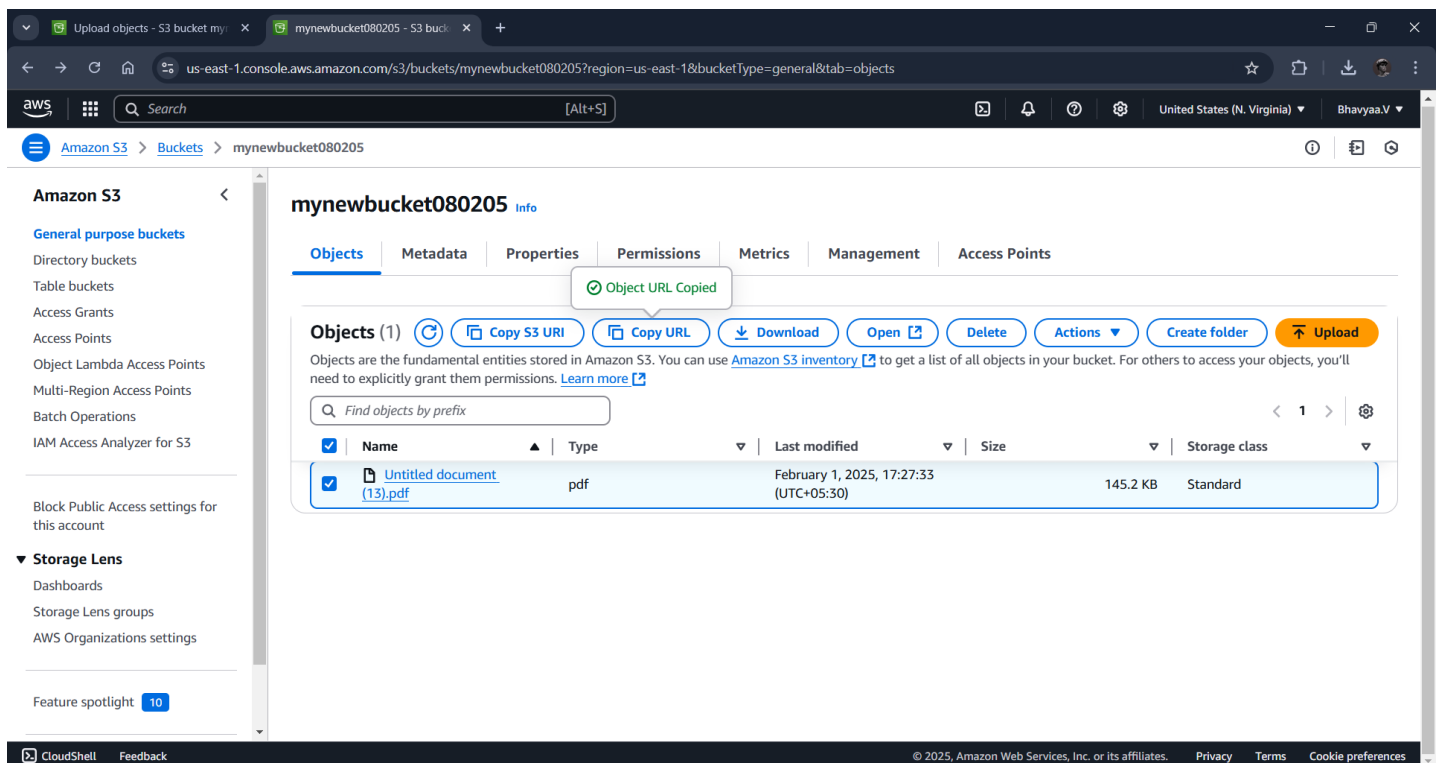
Step 9 :

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



Step10:

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



mynewbucket080205.s3.us-east-1.amazonaws.com/Untitled+document+(13).pdf

Untitled document

1 / 1 100%

Generate OTP Function: This function used to generate the OTP which is a random 6 digit integer with the help of randint module in python.

Send OTP Function: This function is used to send the OTP to your respective recipient mail id

Verify OTP Function: This function is used to verify th OTP that is sent to your mail.

Procedure:

- First create a dynamo db table with streams enabled(give new image).
- Create the generate otp function with necessary permission to access the dynamo db table in order to store the otp and the recipient mail id and expiry time in dynamo db.
- Enable TTL for the expiry time attribute.
- Create SES identities for both sender and recipient mail id and verify it
- Create the send otp function with necessary permissions to access dynamo db and ses so that it can retrieve the data from the dynamo db and send it to the recipient mail.
- Create the verify otp function with necessary permissions to access the dynamo db so

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.