

**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: Keerthana Sri G**

**Department : ECE**

## Introduction

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.

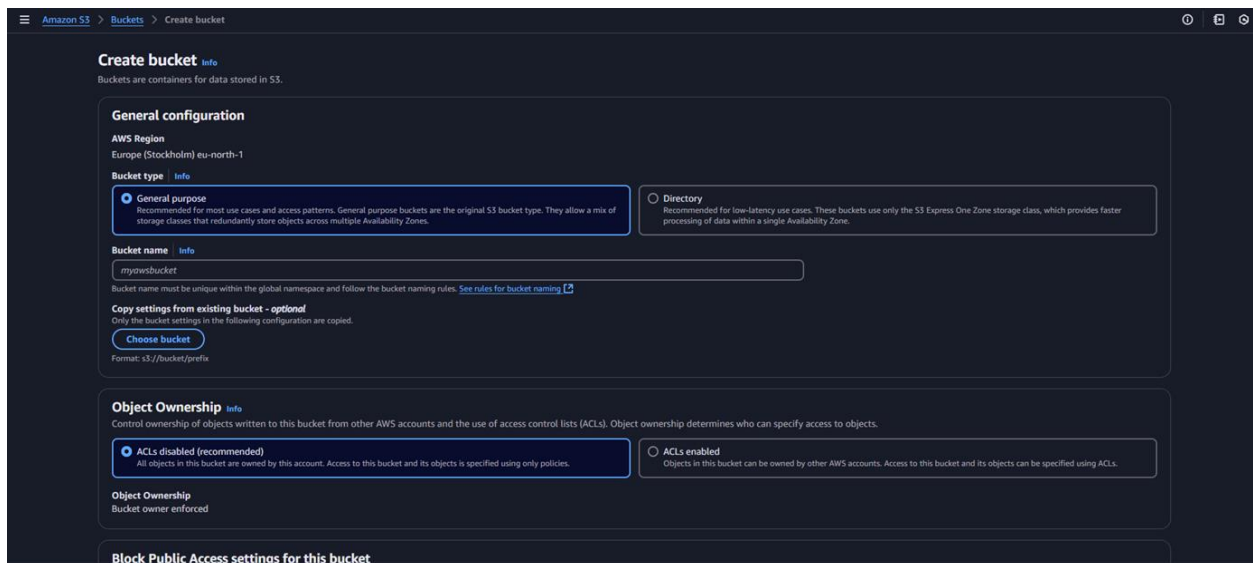
## Objectives

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

## Step by Step Overview

### 1. Create a S3 Bucket

- Log in to your management console.
- Navigate into S3.
- Block public access.



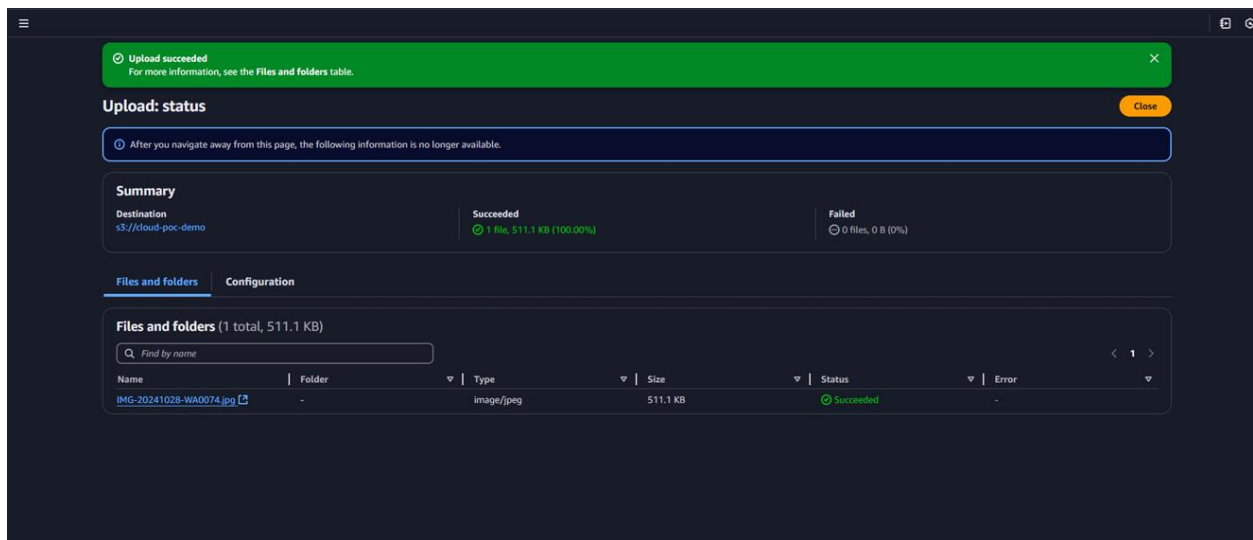
The screenshot shows the 'Create bucket' page in the AWS S3 console. The page is titled 'Create bucket' with an 'Info' link. Below the title, it states 'Buckets are containers for data stored in S3.' The 'General configuration' section includes the 'AWS Region' set to 'Europe (Stockholm) eu-north-1'. Under 'Bucket type', the 'General purpose' option is selected, with a description: '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.' The 'Directory' option is also visible, described as '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.' The 'Bucket name' field contains 'myawsbucket', with a note that the name must be unique within the global namespace and follow naming rules. Below this, there is a section for 'Copy settings from existing bucket - optional', with a 'Choose bucket' button and a format example 's3://bucket/prefix'. The 'Object Ownership' section shows 'ACLs disabled (recommended)' selected, with a note that all objects are owned by the account and access is specified using only policies. The 'Object Ownership' dropdown is set to 'Bucket owner enforced'. At the bottom, there is a section for 'Block Public Access settings for this bucket'.

## 2. Upload into bucket

- Now, after creating the bucket. Open it and Click on Upload option.
- Choose a image into upload.
- Go to the uploaded file in your bucket. Click the file name to open its details. Select Download to save the file locally.

## 3. Permissions

- Open your Bucket and navigate to “Permissions” tab.
- Click on “Block Public Access”.



## 4. Accessing the uploaded image

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

## Outcome:

We have successfully create an AWS S3 bucket and perform file upload/download operations. And configured and validate access permissions, ensuring secure or public access as needed. And gained a solid understanding of S3's functionality, enabling its use in real world cloud-based applications.