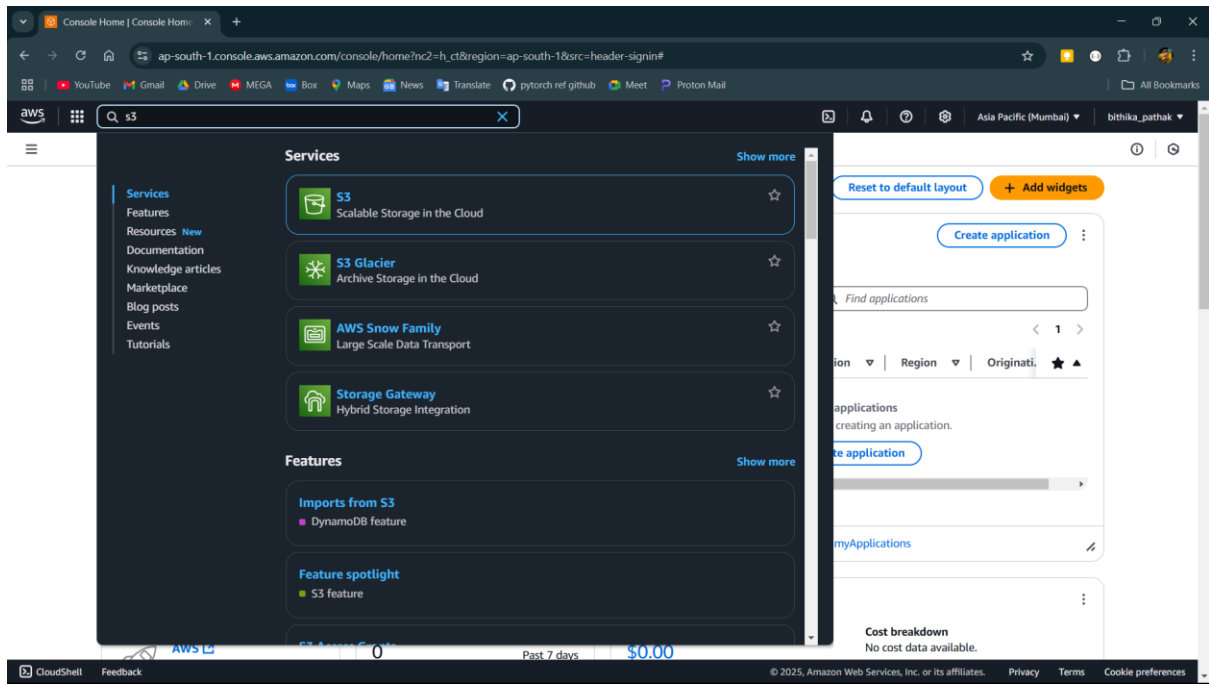


Assignment No:05

Title: Create a public bucket in in AWS. Upload a file and give the necessary permissions to check whether the file url is working.

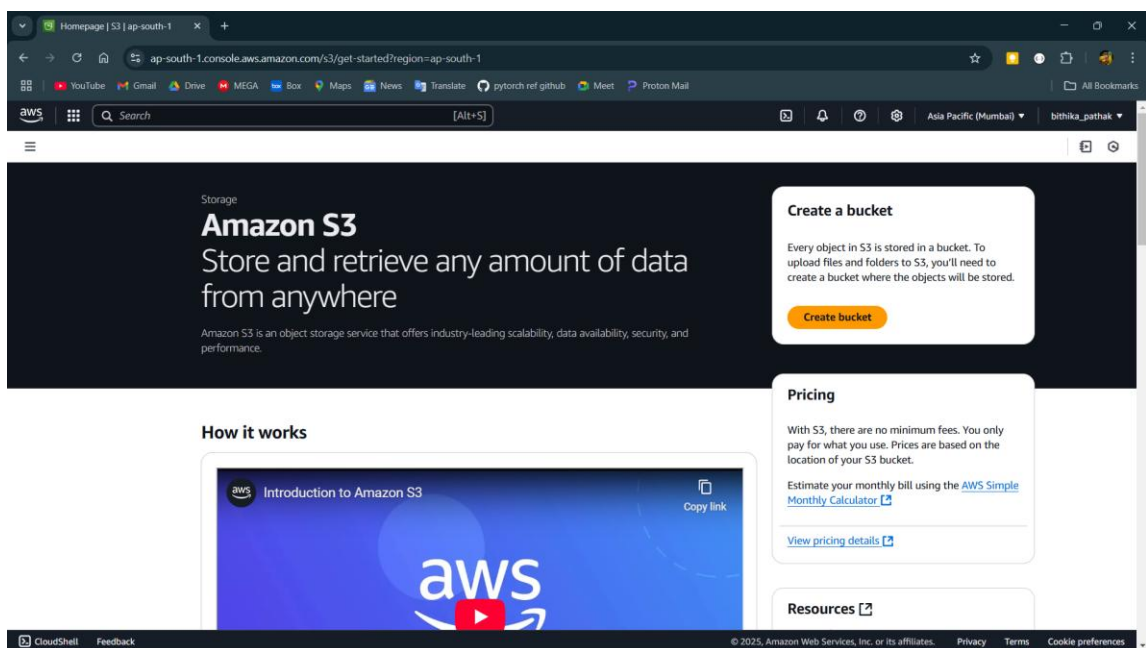
Step-1:

Search S3 in the AWS management console



Step-2:

Click on the S3 and click on create bucket.



Name:Bithika Pathak
Class:CSE(DS)/22/027

Step-3:

Name the bucket the select all the necessary settings uncheck “block all public access” and enable bucket versioning.

The screenshot shows the AWS console 'Create S3 bucket' page. The browser address bar shows the URL: `ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general`. The page title is 'Create S3 bucket | S3 | ap-south-1'. The breadcrumb navigation shows 'Amazon S3 > Buckets > Create bucket'. The 'General configuration' section is active, showing the 'AWS Region' as 'Asia Pacific (Mumbai) ap-south-1'. Under 'Bucket type', 'General purpose' is selected. The 'Bucket name' is 'bithikapubbuck'. The 'Copy settings from existing bucket - optional' section has a 'Choose bucket' button. The 'Object Ownership' section has 'ACLs enabled' selected. The 'Block Public Access settings for this bucket' section is partially visible at the bottom.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-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](#)
bithikapubbuck
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.

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 is independent of one another.

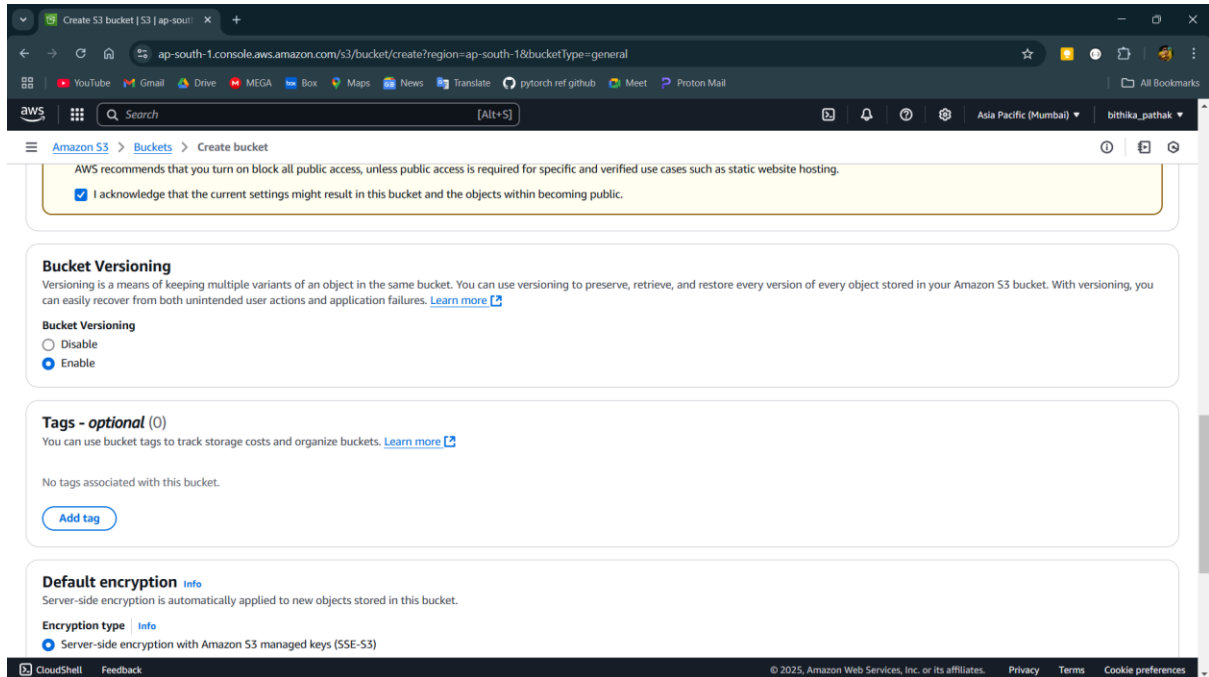
☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing 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.

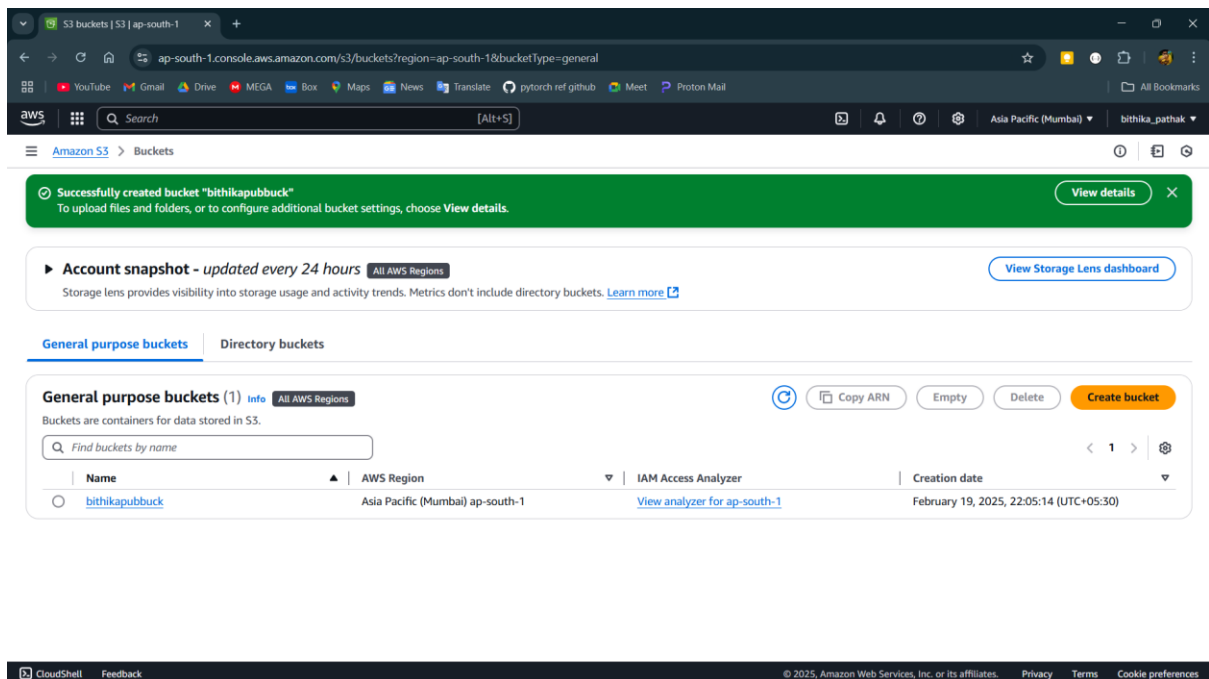
☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**

Name:Bithika Pathak
Class:CSE(DS)/22/027



Step-4:

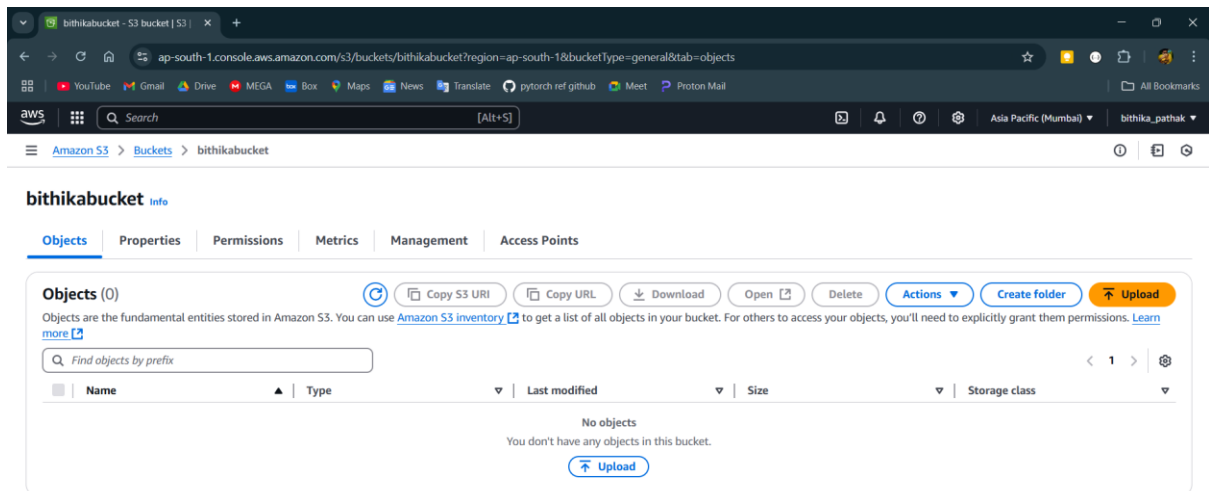
Now click on the name of the created bucket.



Name:Bithika Pathak
Class:CSE(DS)/22/027

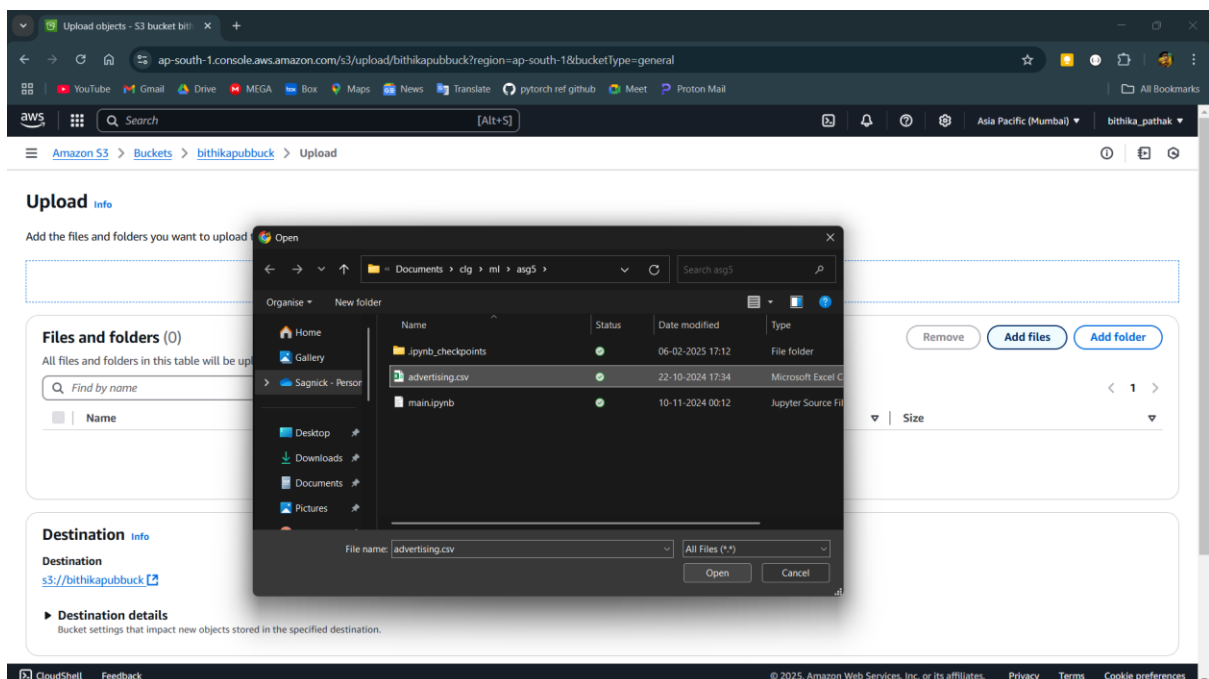
Step-5:

Click on upload to upload file.



Step-6:

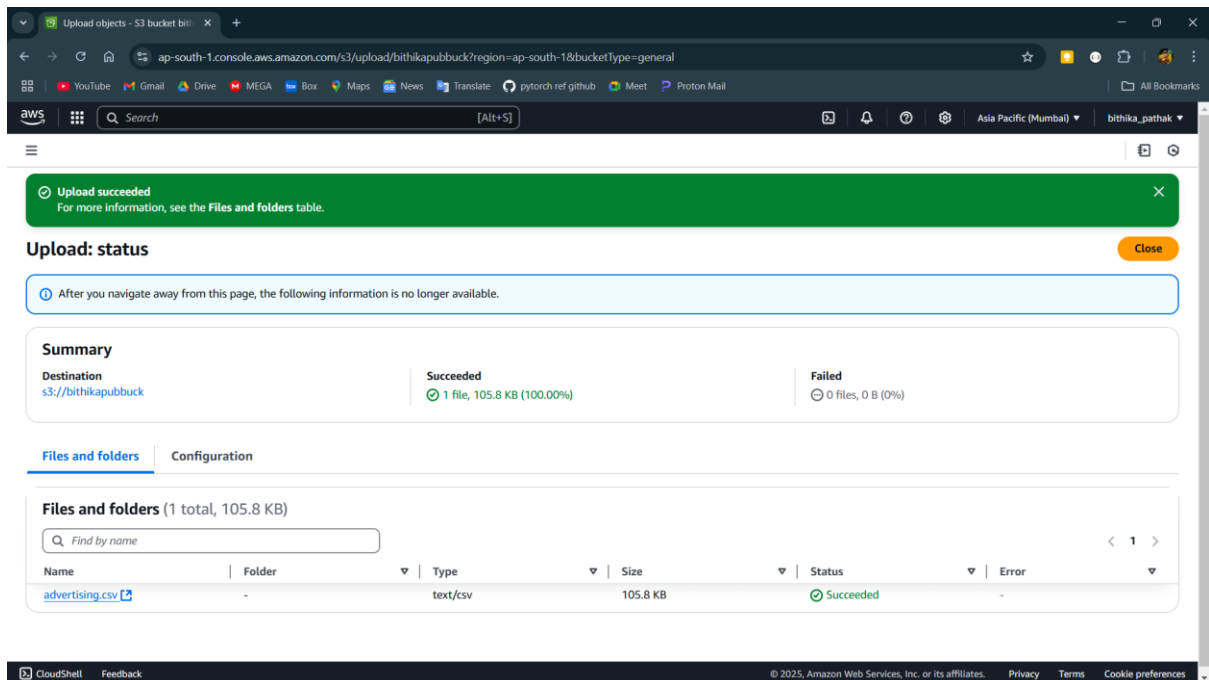
Select the file file to upload and click open. Then press upload



Name:Bithika Pathak
Class:CSE(DS)/22/027

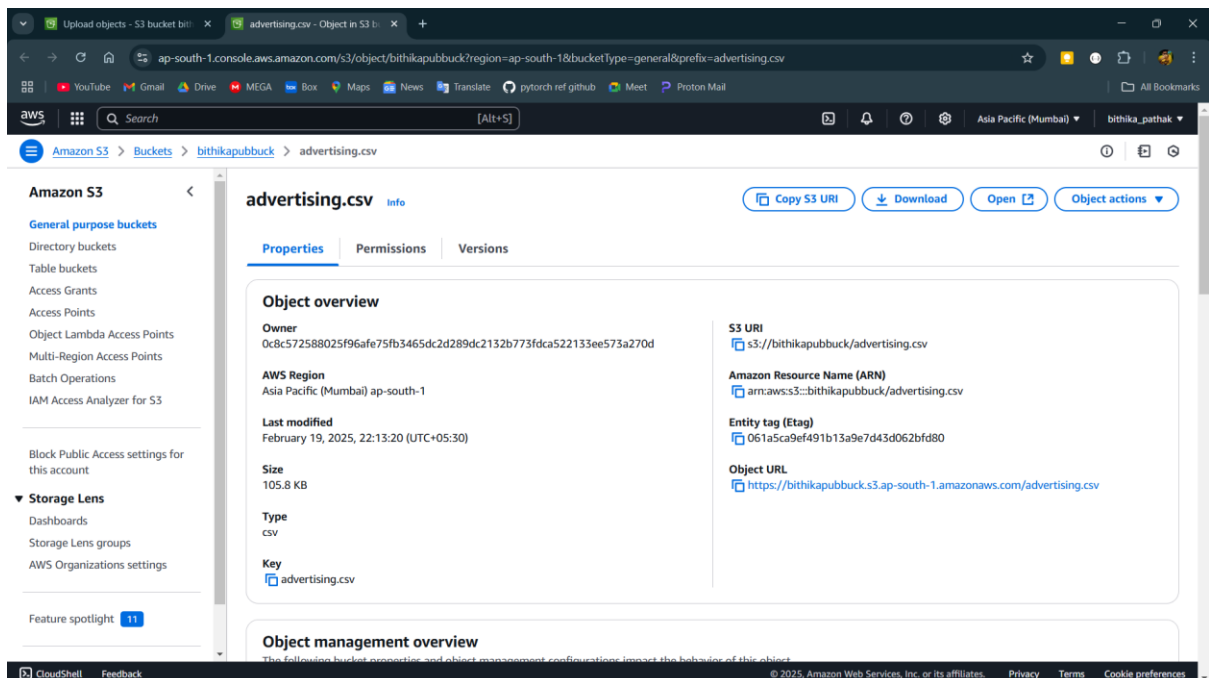
Step-7:

Now click on the name of the file uploaded



Step-8:

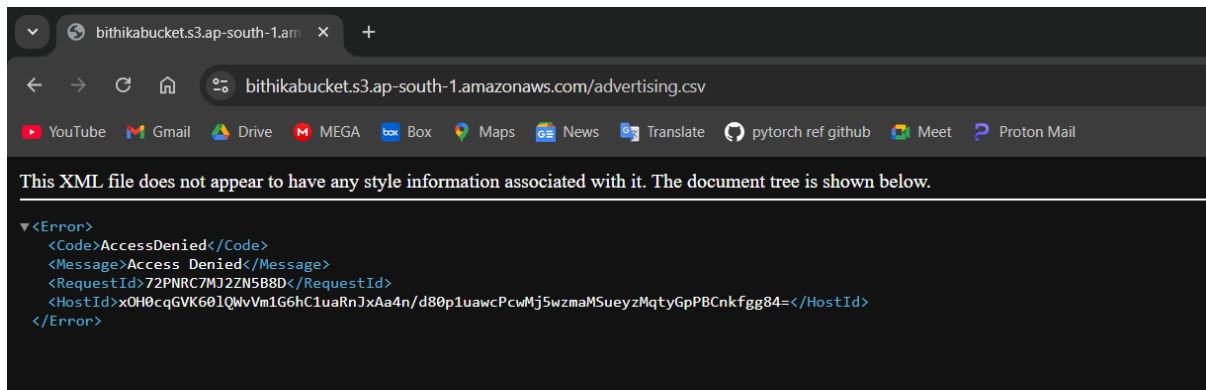
Copy the Object URL and open it in incognito mode.



Name: Bithika Pathak
Class: CSE(DS)/22/027

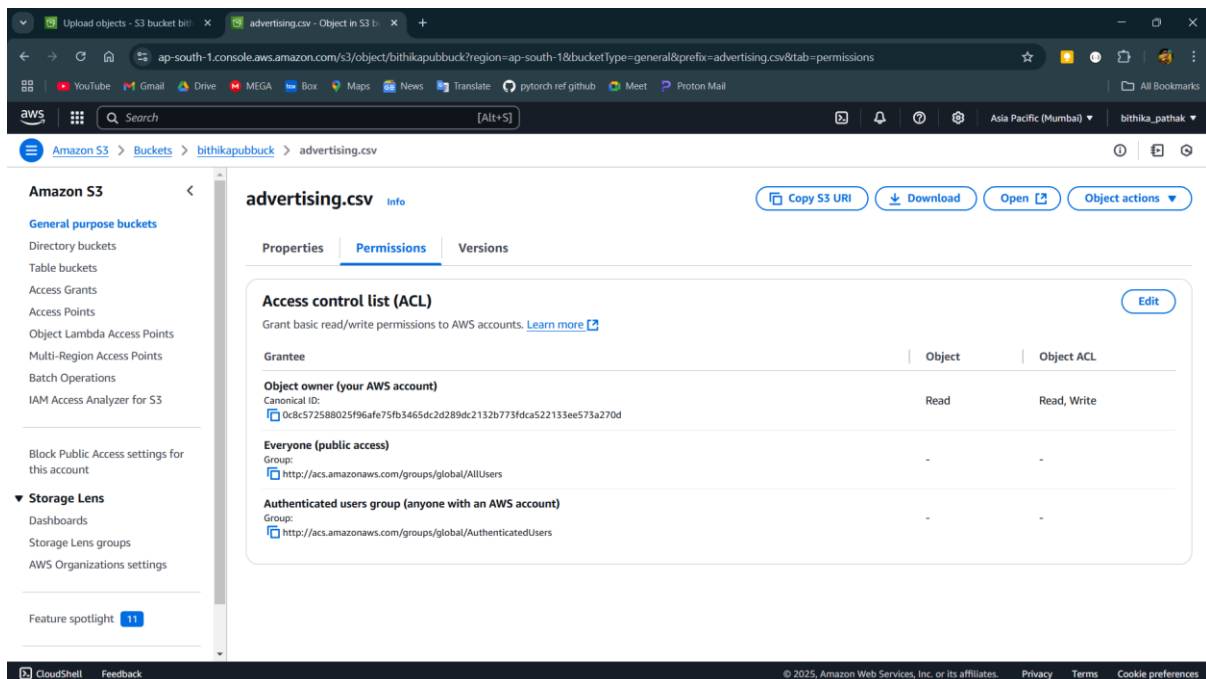
Step-9:

Now the access is denied.



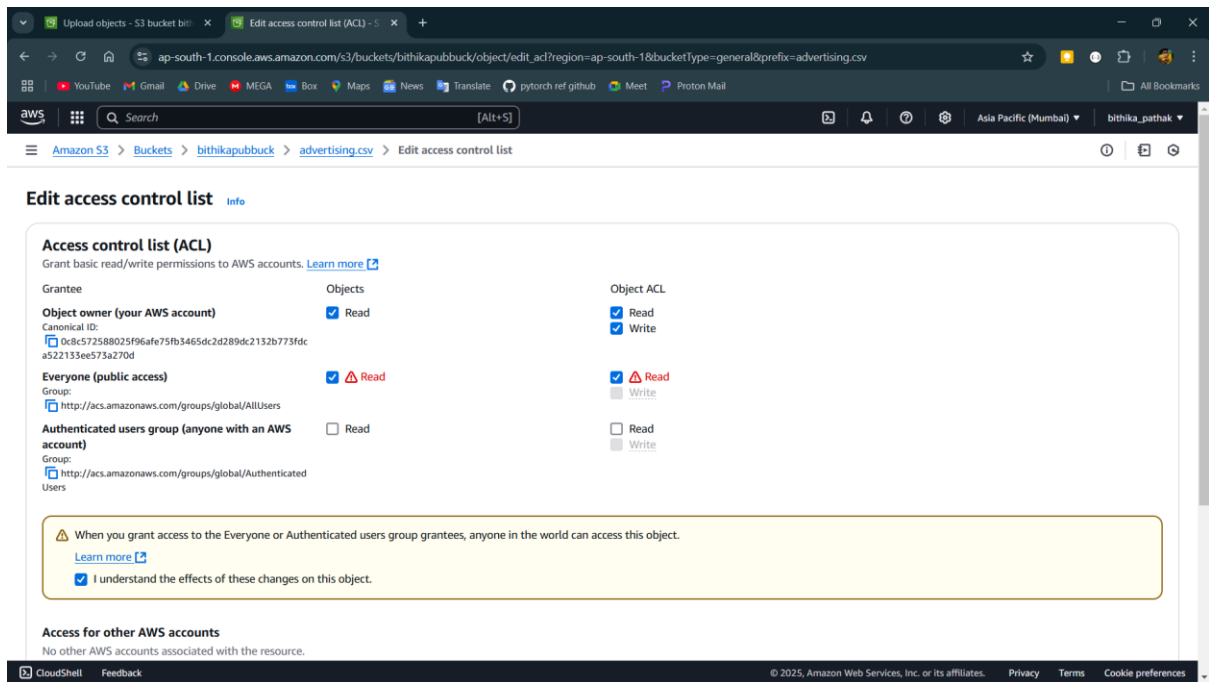
Step-10:

Open the permissions and click on edit.



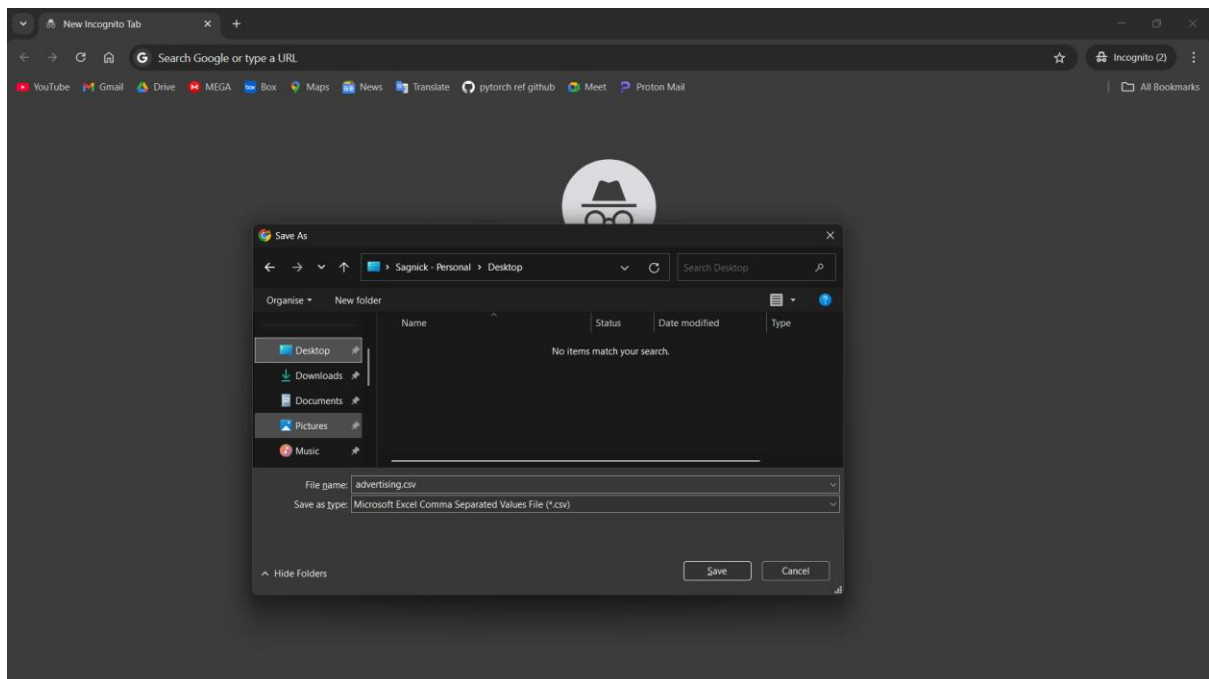
Step-11:

Now check on read of objects and objects acl everyone(public access) and then save changes.



Step-12:

Now copy the object url and the file will download.



Name: Bithika Pathak
Class: CSE(DS)/22/027