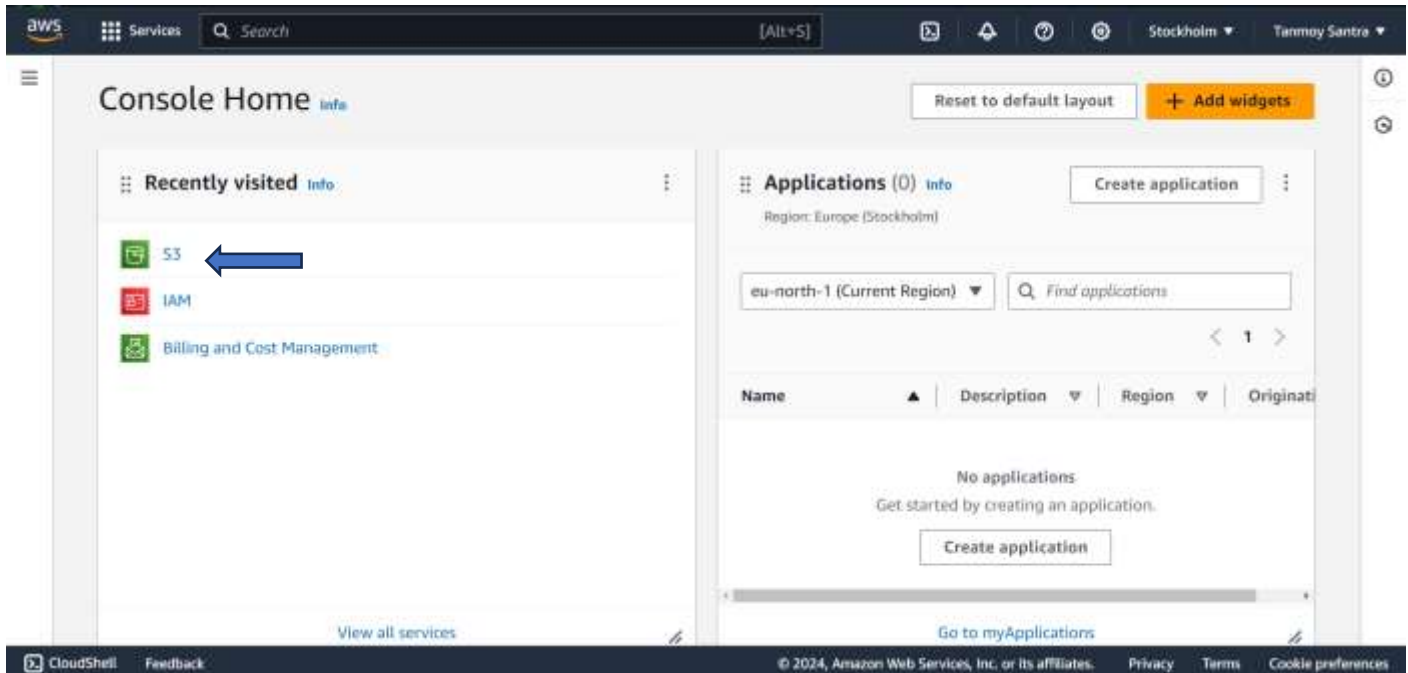


ASSIGNMENT - 4

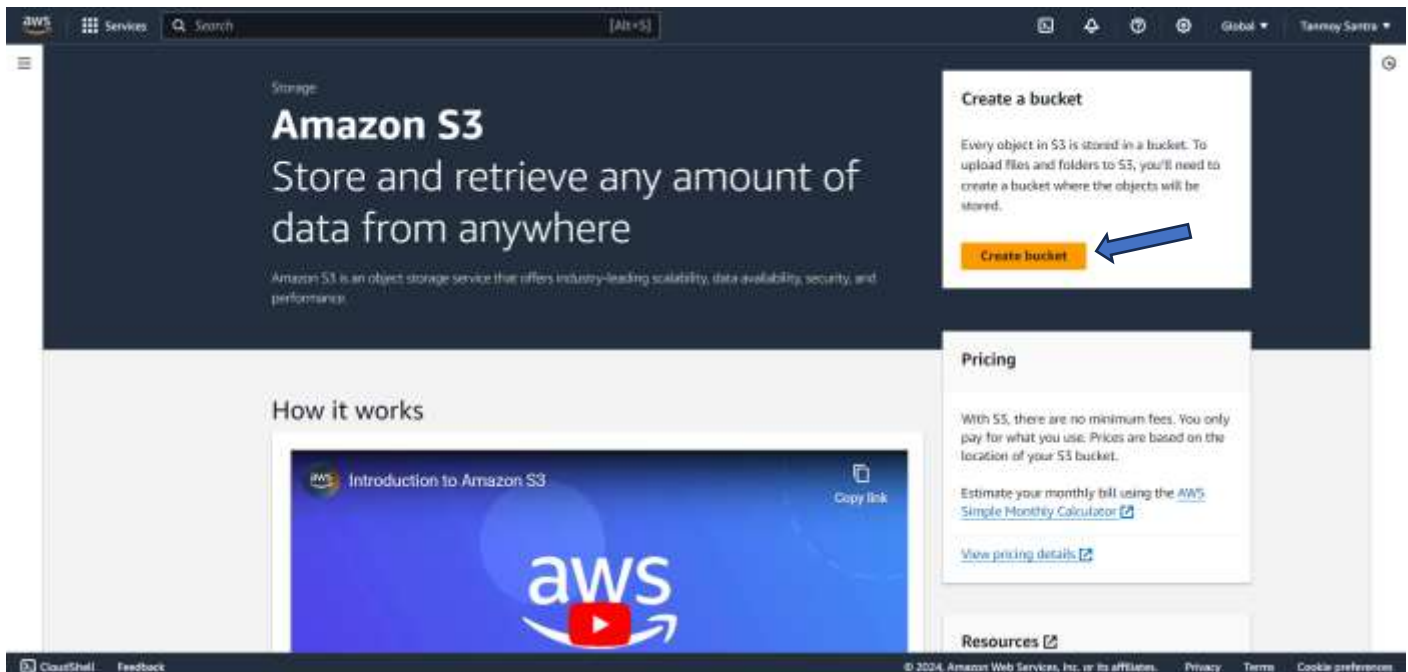
PROBLEM STATEMENT : Create a private Bucket. Upload a file and check by reassigning URL whether you can access the file or not.

To create Private Bucket -

STEP 1- Click on the “S3” button.



STEP 2- Click on “Create Bucket”.



STEP 3- With select AWS Region “Mumbai”, give a Name to the Bucket.

Amazon S3 > Buckets > Create bucket

Create bucket [info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name [info](#)

tanmoybucket1

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/profile

STEP 4- Select “ACLs disabled” & “Block all public access” checkbox. Then Click on “Create Bucket”.

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 ignore 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 object access point policies**

Default encryption [info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [info](#)

- ☒ **Server-side encryption with Amazon S3 managed keys (SSE-S3)**
- ☐ **Server-side encryption with AWS Key Management Service keys (SSE-KMS)**
- ☐ **Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)**
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

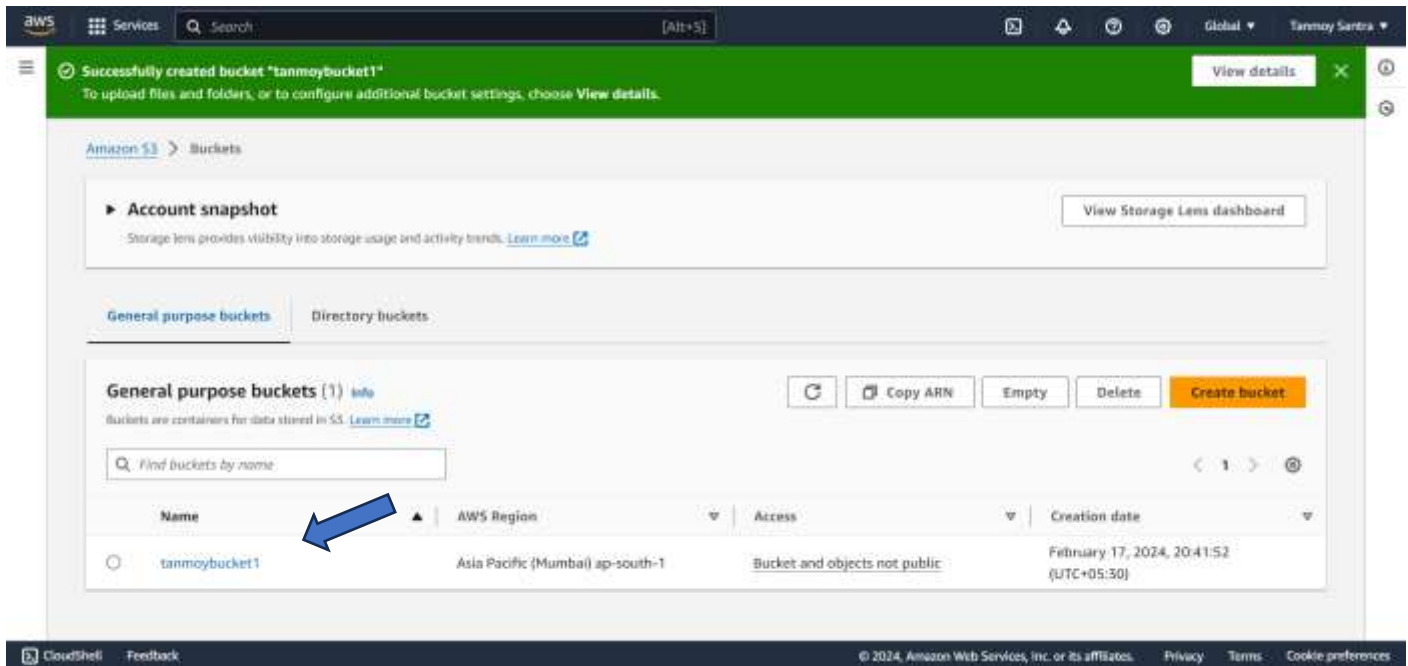
- ☐ **Disable**
- ☒ **Enable**

Advanced settings

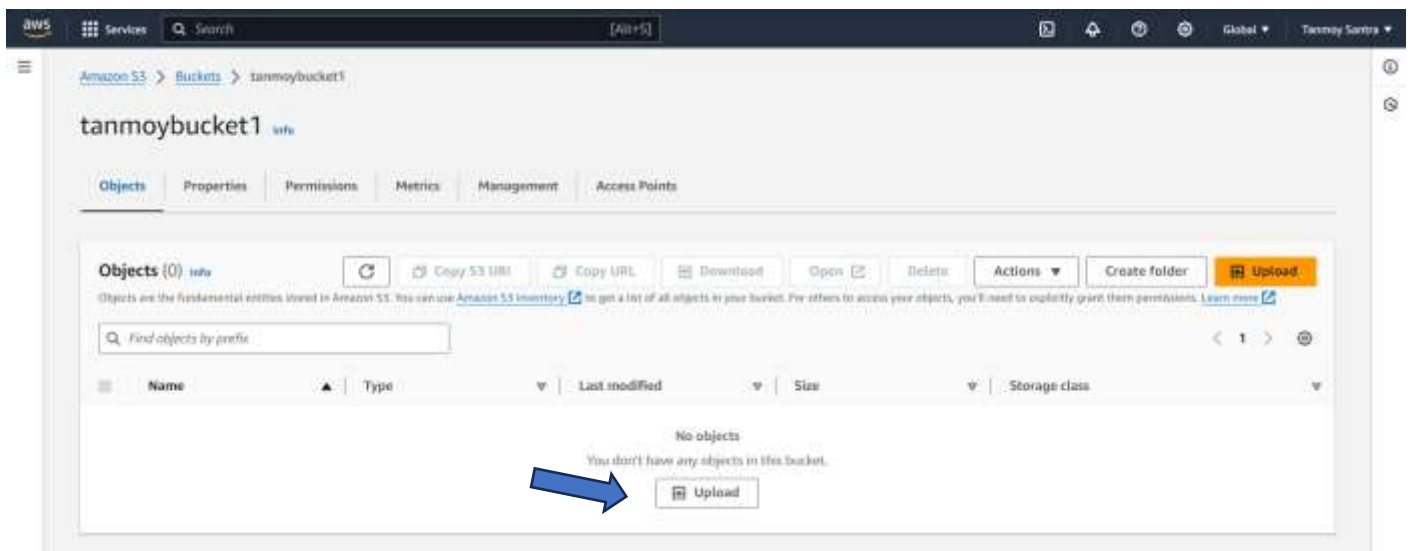
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

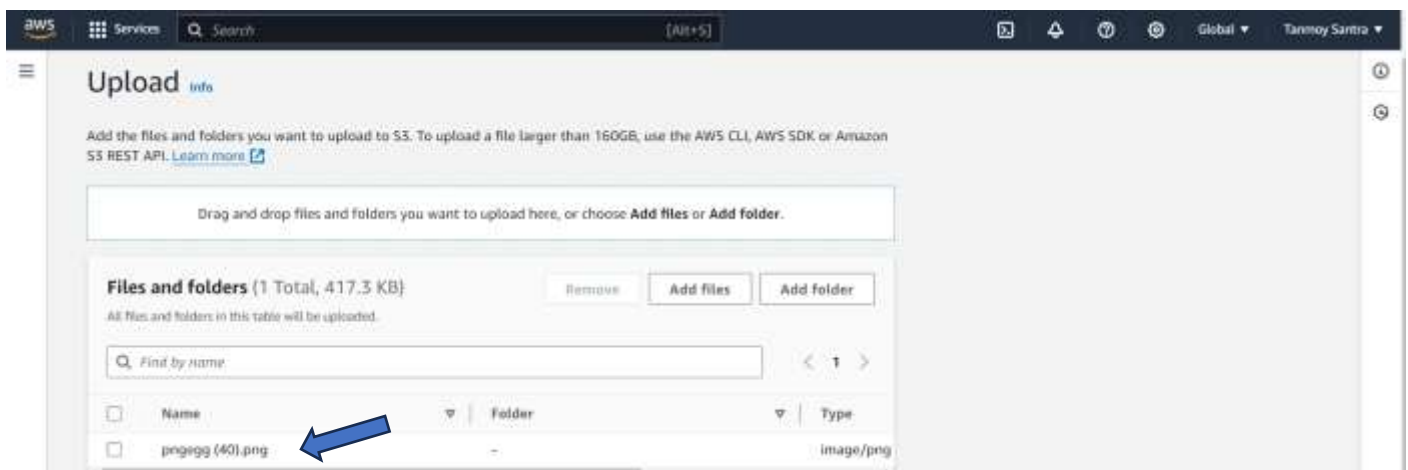
STEP 5- The Bucket is created. Click on the bucket name.

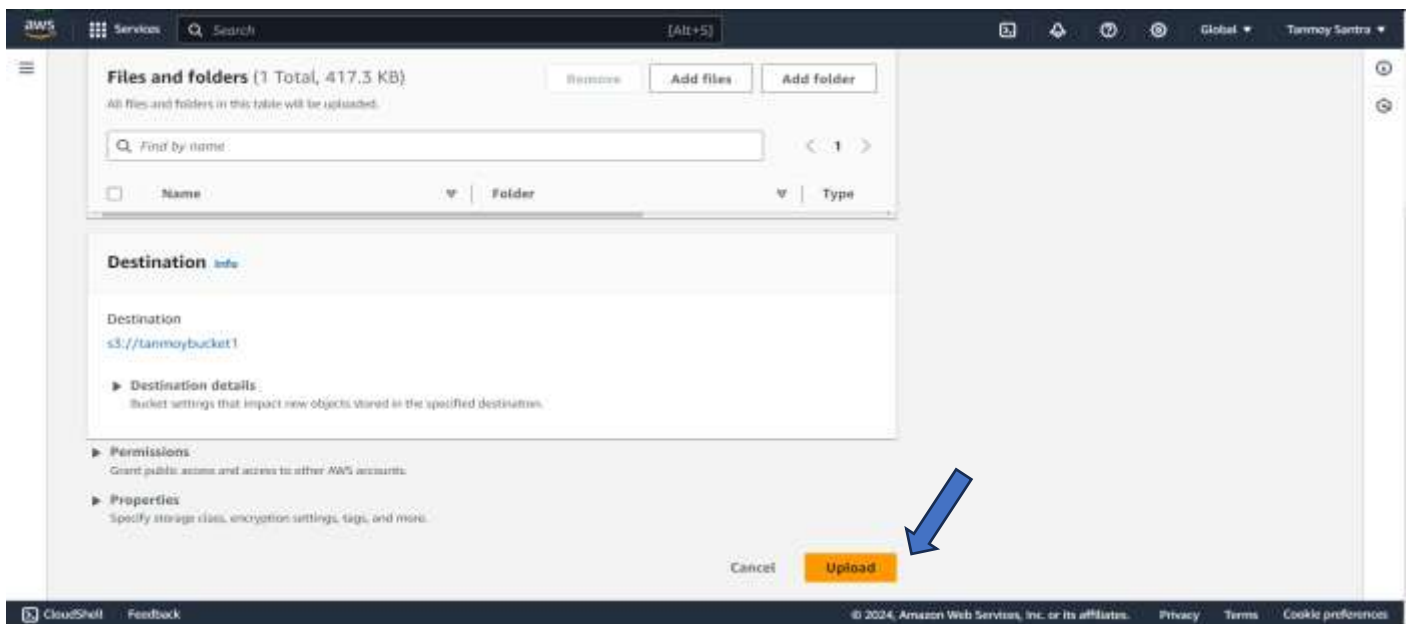


STEP 6- Click on the "Upload".

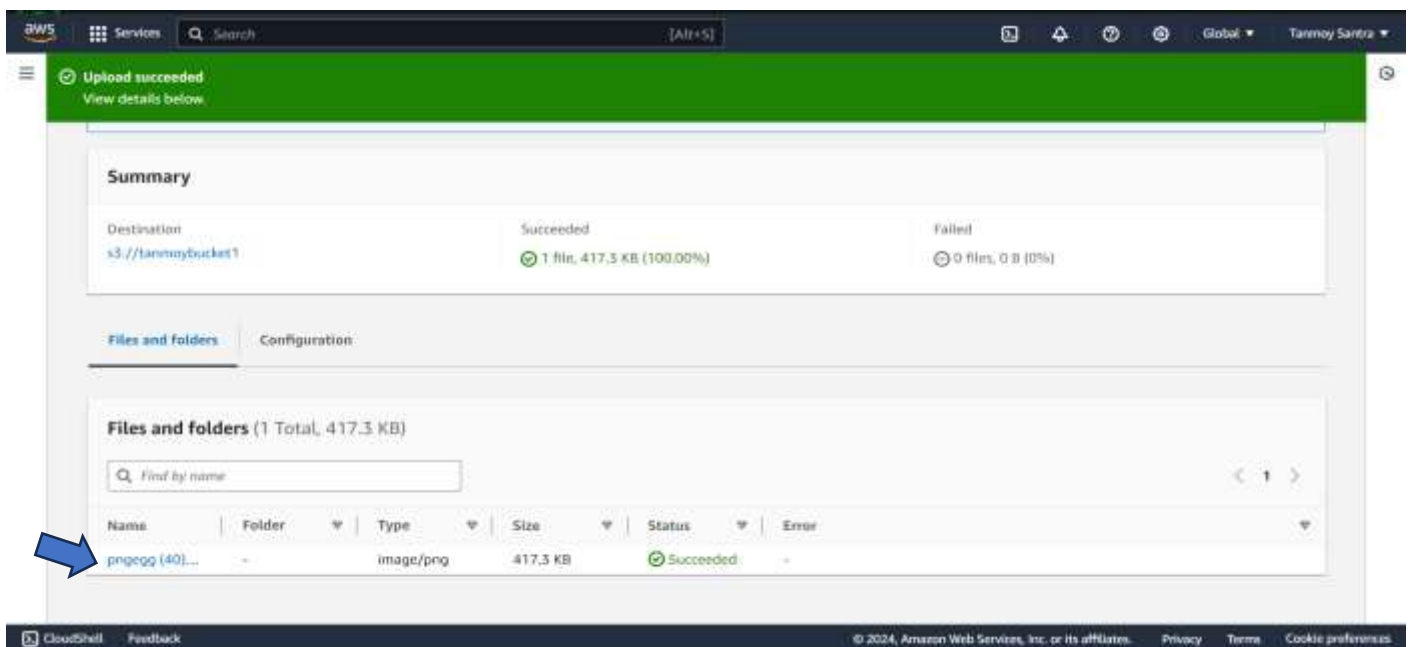


STEP 7- Click on "Add file" and add the files then click upload.

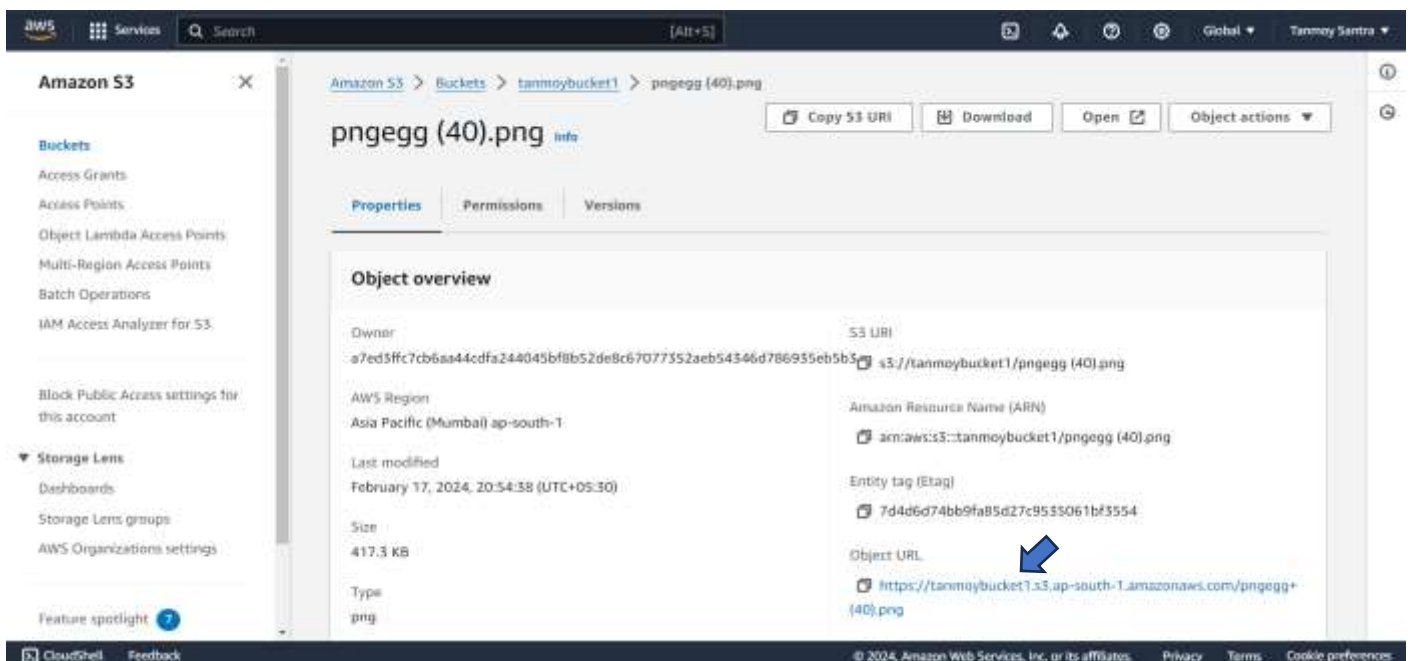




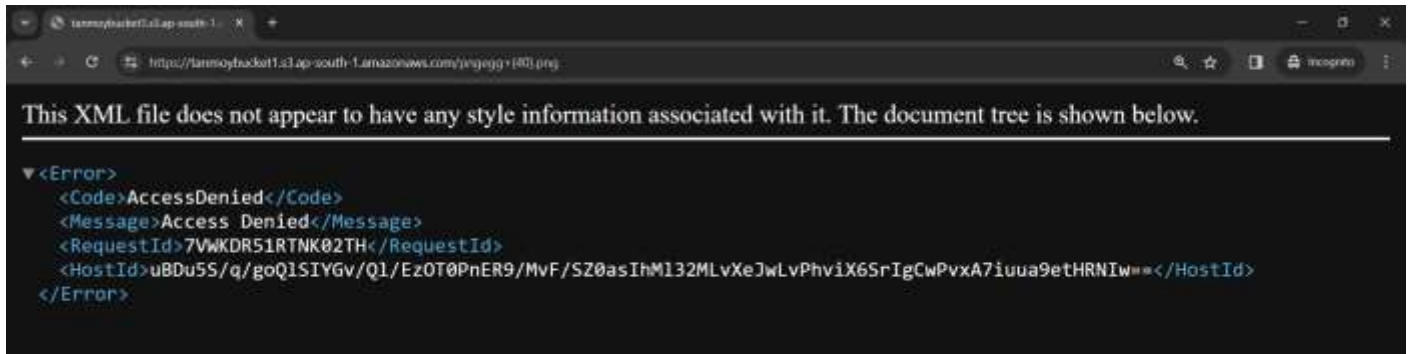
STEP 8- The file has been uploaded successfully. Click on the file name.



STEP 9- Copy the "Object URL".



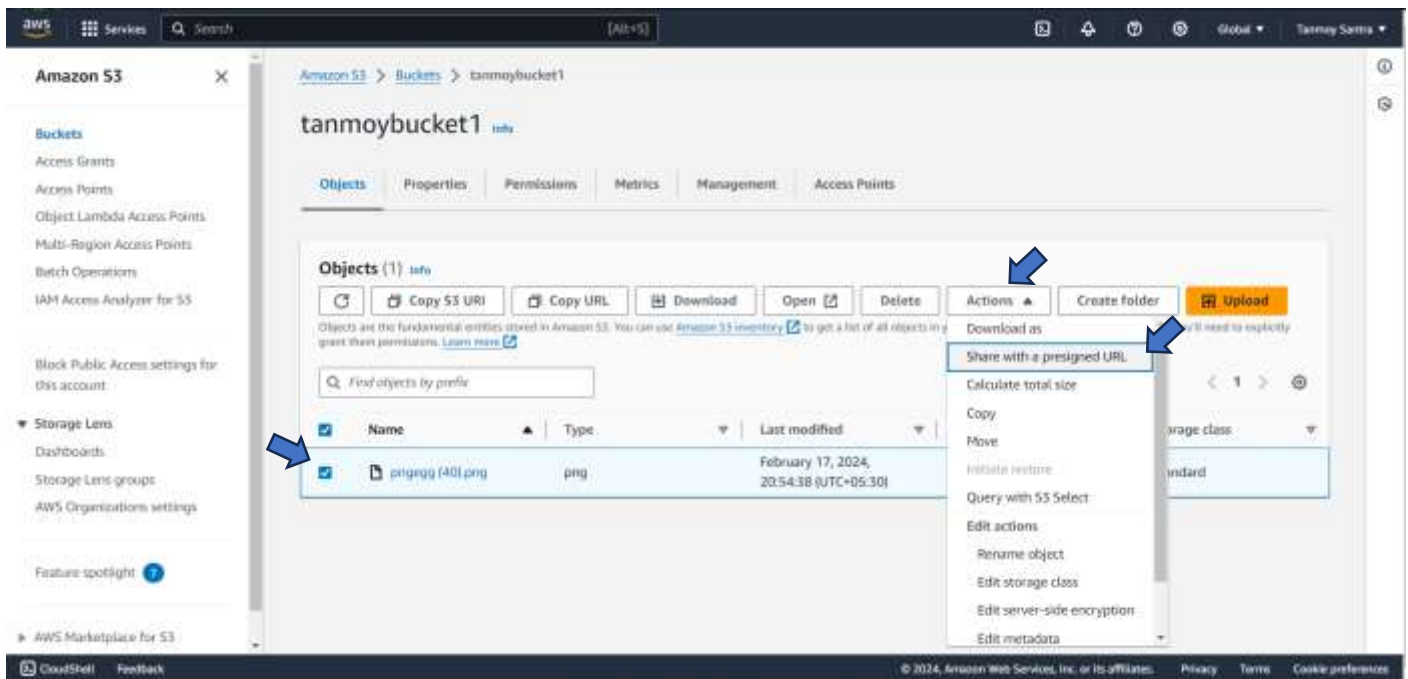
STEP 10- Open a new browser window and paste the URL in the address bar.



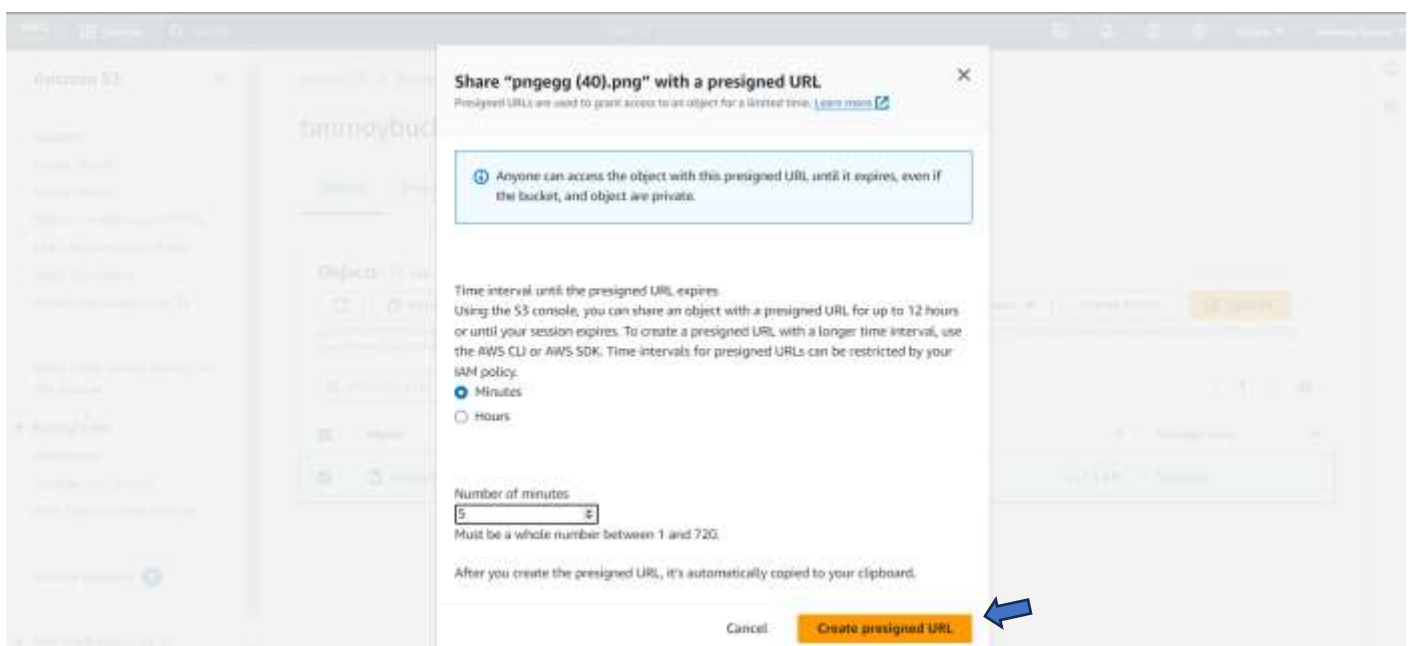
To reassign url -

STEP 1- Open the Bucket.

STEP 2- Select the file and Click on the “Actions” dropdown menu and select the “presigned URL”.



STEP 3- Give a Time limit & then click on the “Create Presigned URL” button.



STEP 4- Copy the URL & Open a new browser window and paste the URL.

