Assignment number: 4
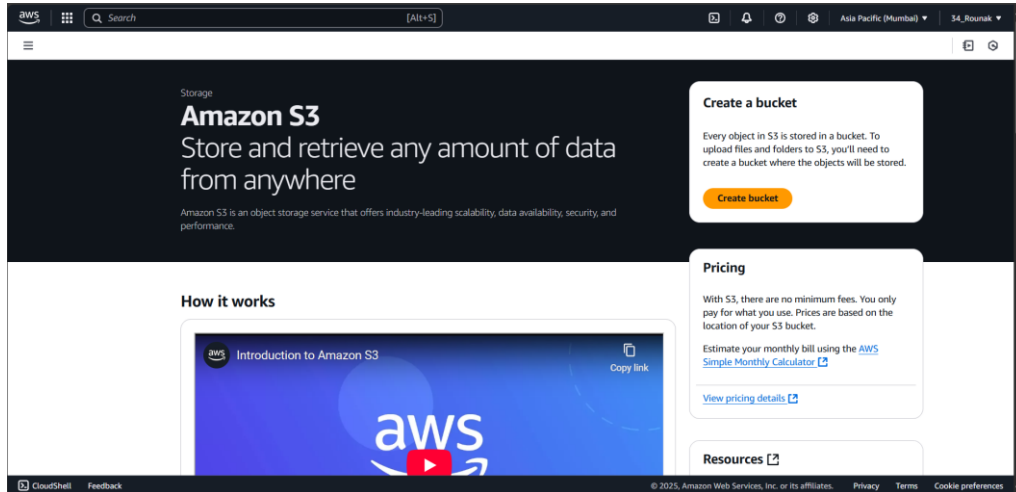
Problem definition: Create a private bucket in AWS. Upload a file and check by presigned URL whether you can access the file or not.
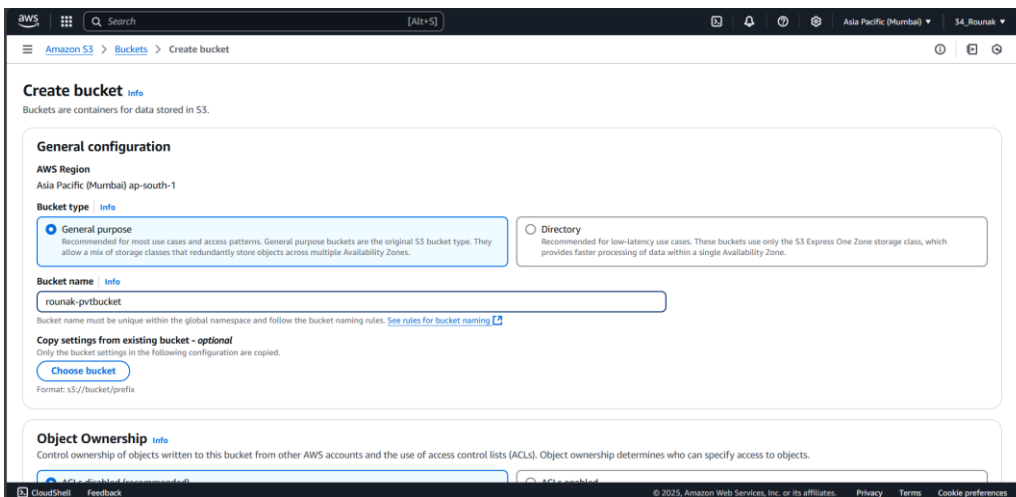
Step 1: Sign in to your AWS account as the root user.

Step 2: In the AWS homepage search box, type "S3" and select the first option to open the Amazon S3 dashboard.

Step 3: Click the "**Create bucket**" button.

Step 4: On the Create Bucket page, provide a globally unique bucket name using only lowercase letters and no spaces, and choose the Asia Pacific (Mumbai) ap-south-1 region. In the Object Ownership section, ensure that ACLs are disabled, and in the Public Access settings, keep all public access blocked to ensure your bucket remains private. Click the "**Create bucket**" button to finalize and create your 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.
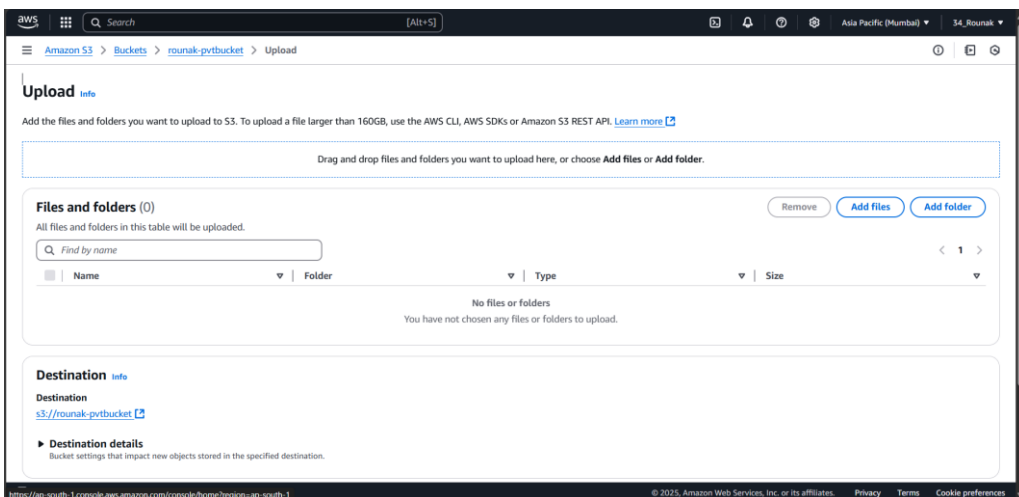
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

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 block public access permissions applied to newly added buckets or objects, and prevent the creation of new public 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.

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

Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more ↗

No tags associated with this bucket.

[Add tag]

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)

[Add tag]

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**]

⊘ **Successfully created bucket "rounak-pvtbucket"**
To upload files and folders, or to configure additional bucket settings, choose **View details**.   [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.   ⟳ [Copy ARN] [Empty] [Delete] [**Create bucket**]

🔍 Find buckets by name   ‹ 1 › ⚙

○	Name	AWS Region ▾	IAM Access Analyzer ▾	Creation date ▾
○	rounak-pvtbucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 5, 2025, 20:36:16 (UTC+05:30)

Name: Rounak Singh   Roll: CSE/22/034   CSE-1 SDITO Lab (PC-CS694)

Step 4: Once the bucket is created, click on its name from the list of buckets to open the bucket details page.

Step 5: Click the "**Upload**" button to begin the process of adding a file to your bucket.

Step 6: In the upload interface, click on "**Add files**", select the desired file from your computer, and then click "**Upload**" to start the file transfer.
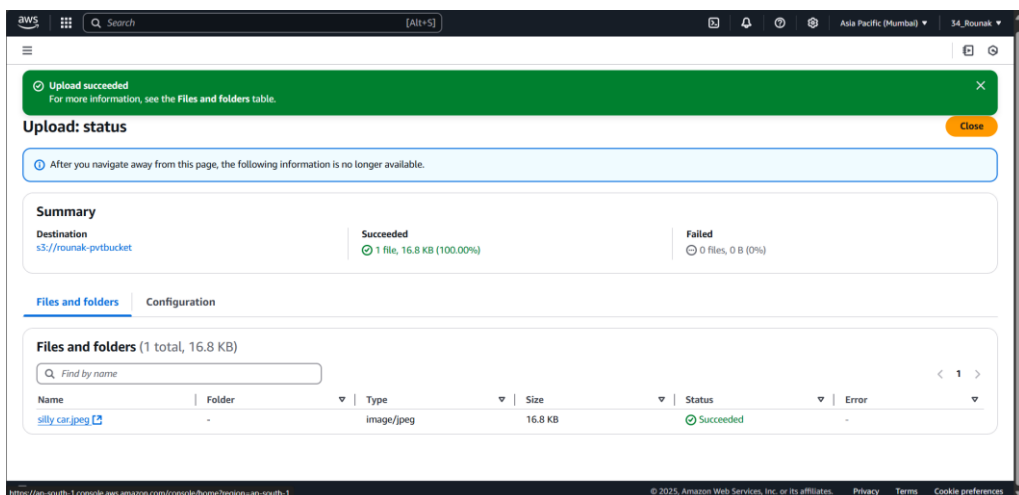
Step 7: After the file is uploaded, locate it in the objects list, click on the file to open its details, and scroll down to copy the Object URL.
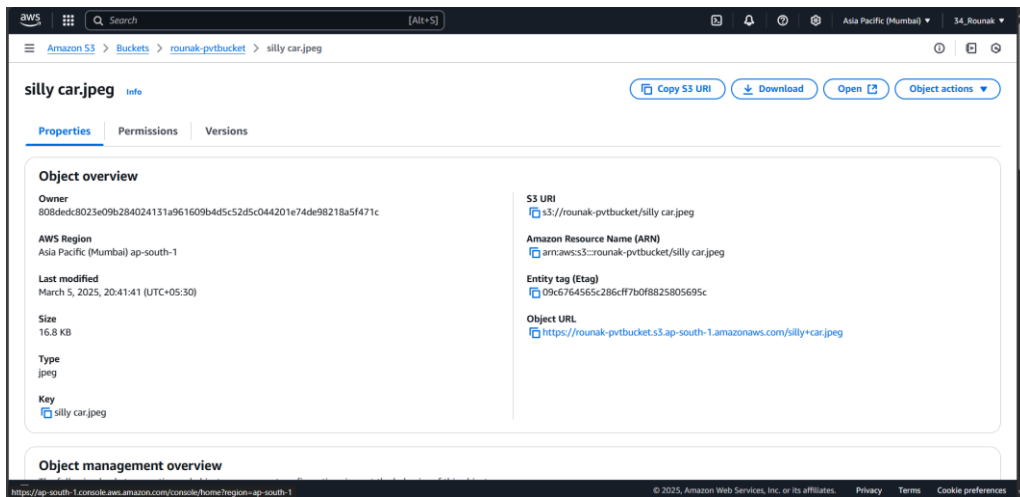
Step 8: Open a new browser tab, paste the Object URL, and press Enter; you should see an error, confirming that the file is in a private bucket.
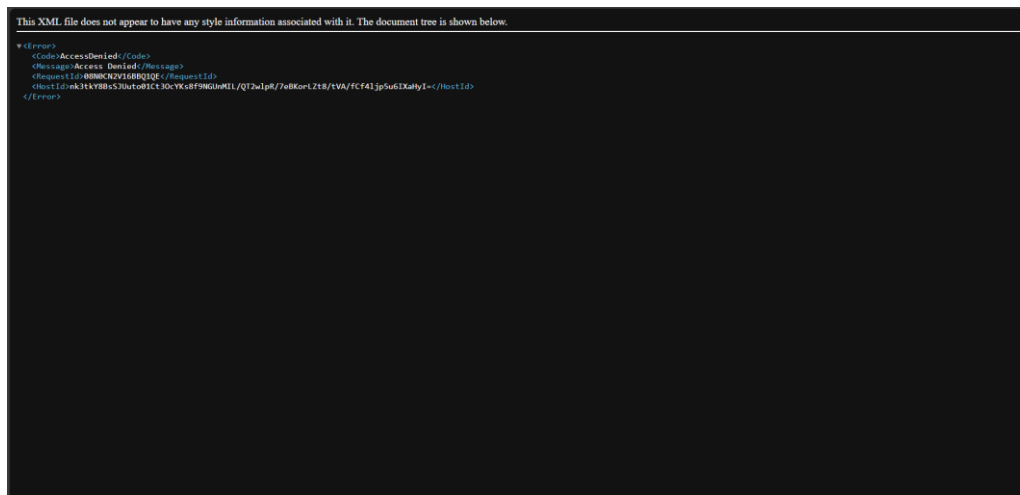
Step 9: Return to the file's details page in your bucket, click on the **Actions** button, and choose the "Share with presigned URL" option.
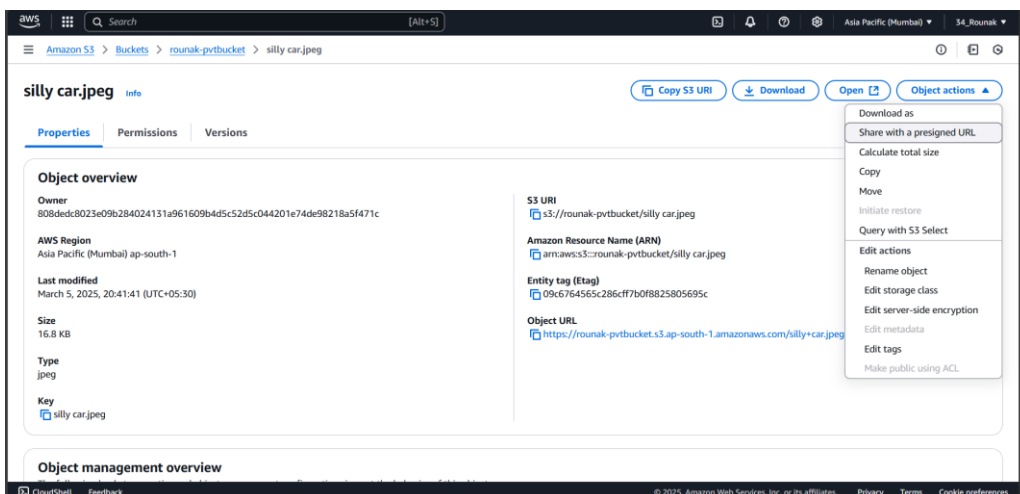
Step 10: In the pop-up dialog, specify the duration for which the pre-signed URL should remain active, then click "**Create presigned URL**" to generate the URL (which is automatically copied to your clipboard).
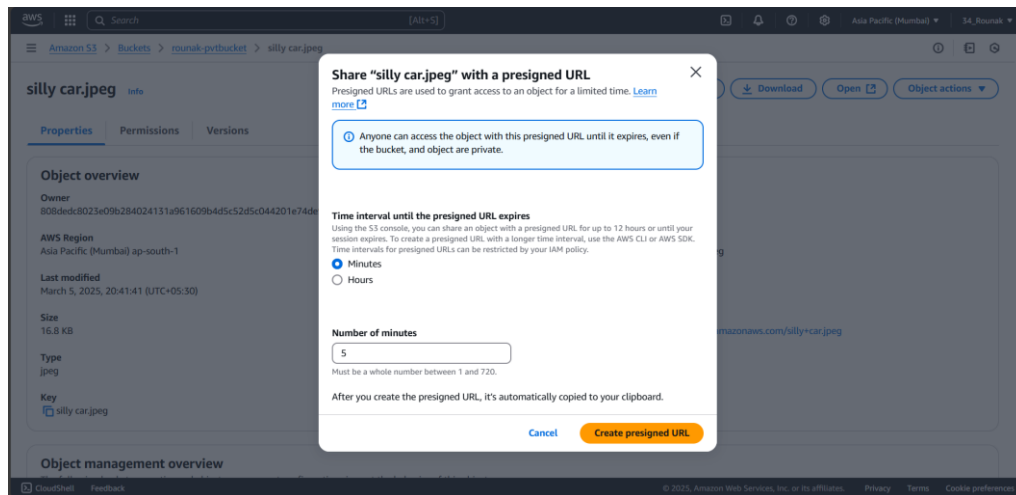
Step 11: Finally, open another browser tab, paste the pre-signed URL, and press Enter to verify that you can access the file using the temporary link.

Name: Rounak Singh   Roll: CSE/22/034   CSE-1 SDITO Lab (PC-CS694)