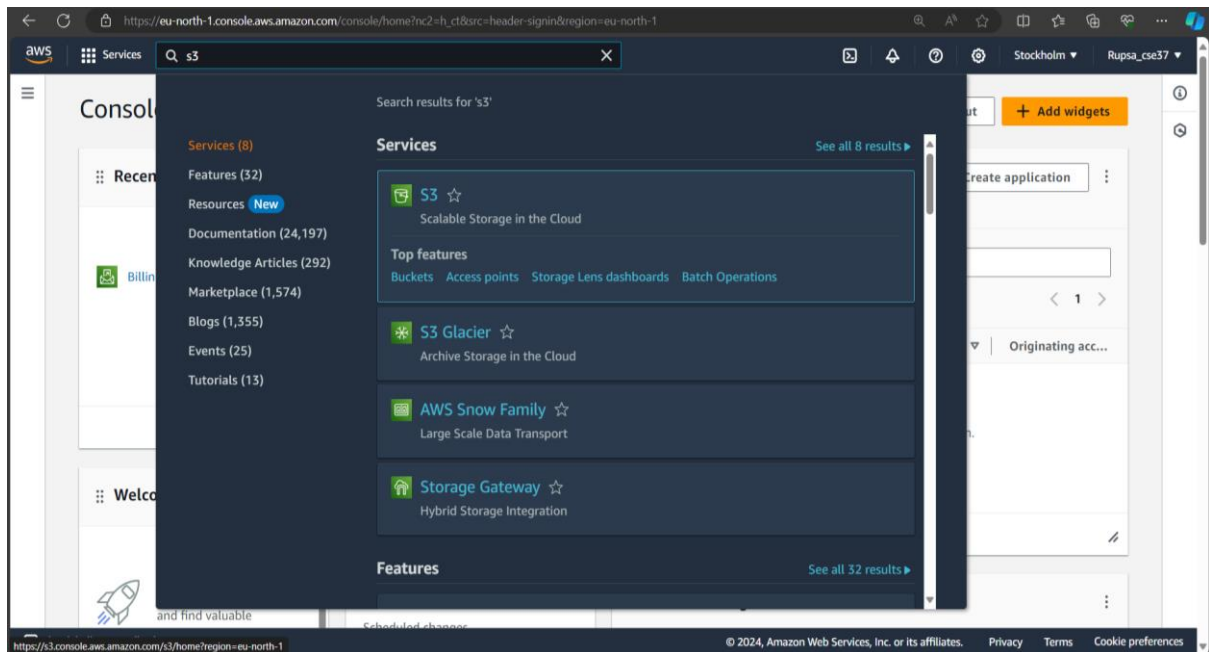


## **PROBLEM STATEMENT :**

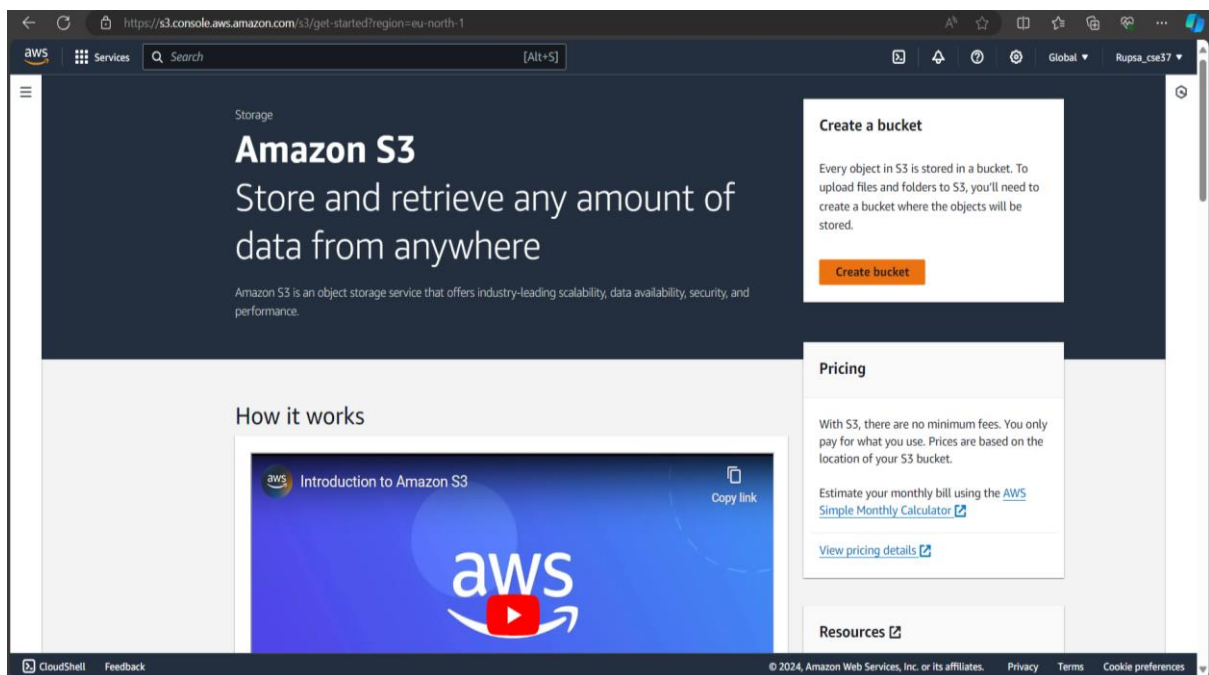
4) Create a private bucket in AWS. Upload a file and check by reassigned URL whether you can access the file or not.

### ***Bucket creation and checking for access-***

1. Sign up for an AWS account, search for 'S3' then click on it.



2. Click on 'Create bucket'.



- Fill up the required details->'AWS region', 'Bucket name' then we have to do 'ALC disabled' because we are creating a private bucket and check the other configuration as per the snapshots then click on 'Create bucket'.

The screenshot shows the 'Create bucket' page in the AWS S3 console. The 'General configuration' section is active. The 'AWS Region' is set to 'Asia Pacific (Mumbai) ap-south-1'. The 'Bucket name' is 'myawsbucket'. Below this, there is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button. The 'Object Ownership' section shows 'ACLs disabled (recommended)' selected, with a note that all objects in the bucket are owned by this account. The 'Object Ownership' is set to 'Bucket owner enforced'.

https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general

aws Services Search [Alt+S]

### 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](#)  
myawsbucket  
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.

Object Ownership  
Bucket owner enforced

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the 'Default encryption' section of the 'Create bucket' page. The 'Encryption type' is set to 'Server-side encryption with Amazon S3 managed keys (SSE-S3)'. The 'Bucket Key' is set to 'Enable'. Below this is an 'Advanced settings' section with a note: 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.' At the bottom, there are 'Cancel' and 'Create bucket' buttons.

https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general

aws Services Search [Alt+S]

### 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**

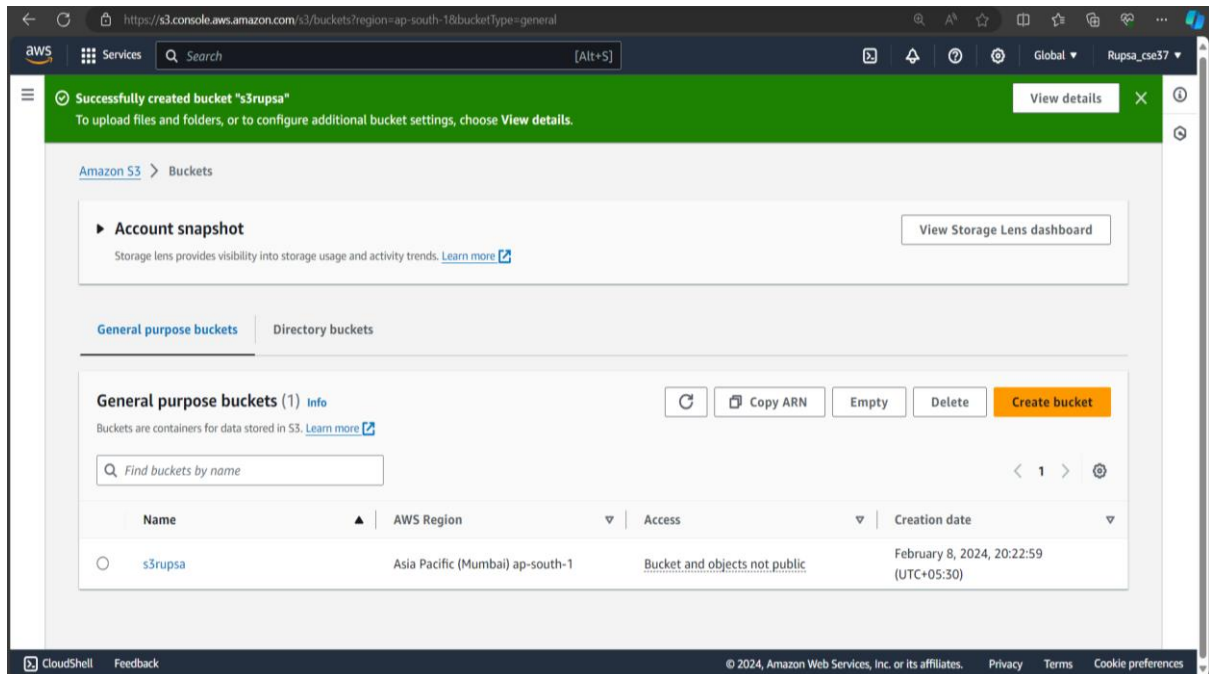
**Advanced settings**

[After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.](#)

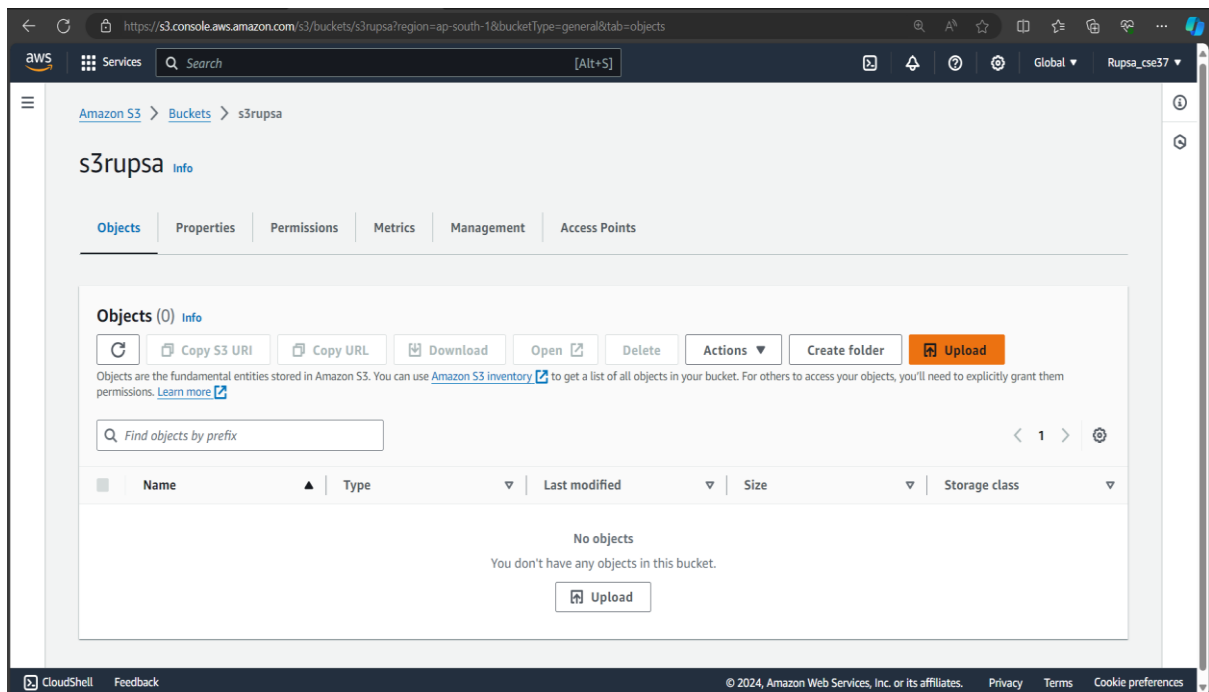
Cancel **Create bucket**

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

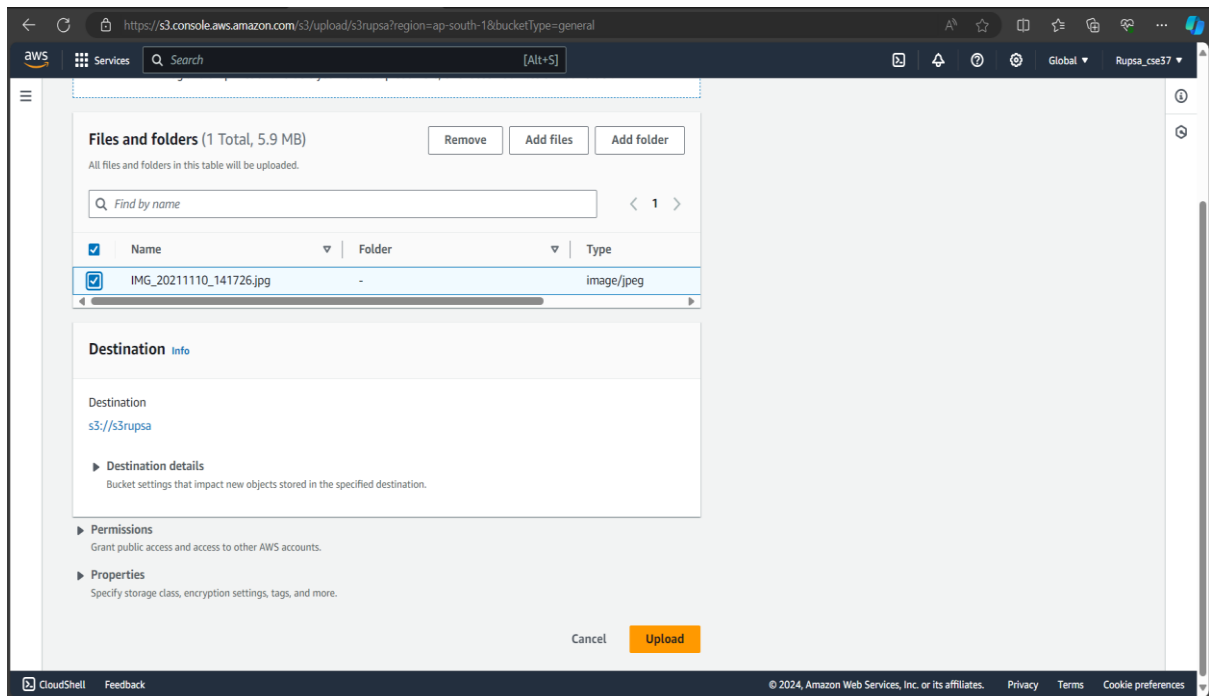
4. 's3rupsa' bucket is created successfully then click on name->'s3rupsa'.



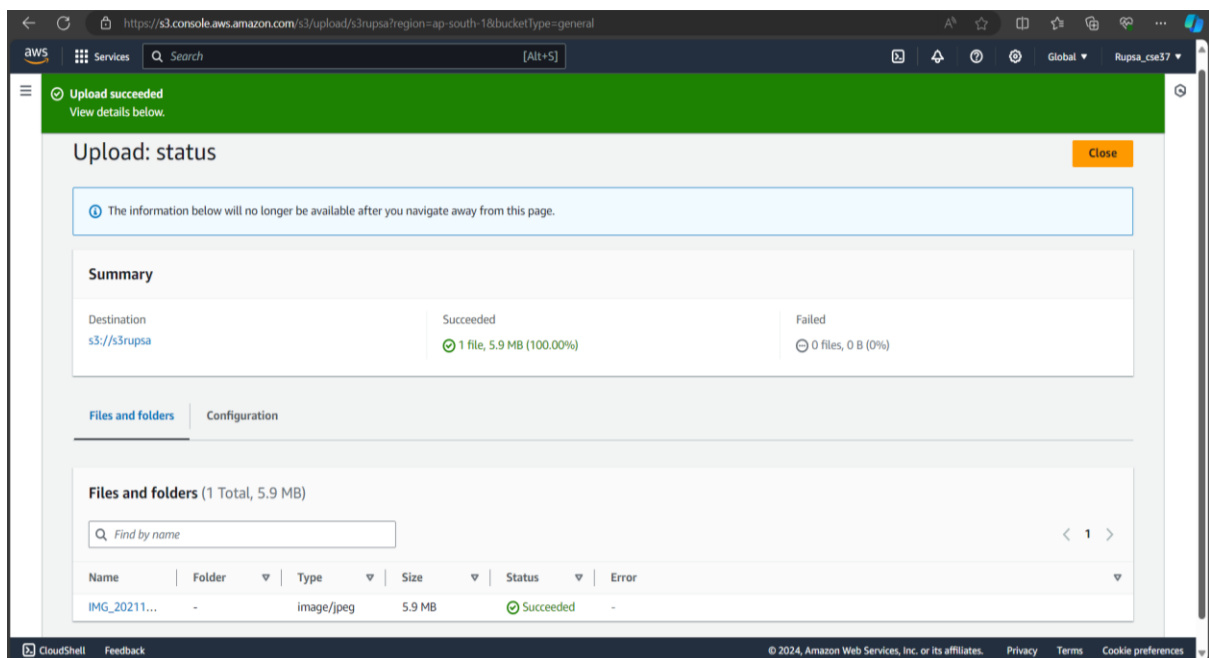
5. Under 's3rupsa', click on 'Upload' then choose a file of your choice .



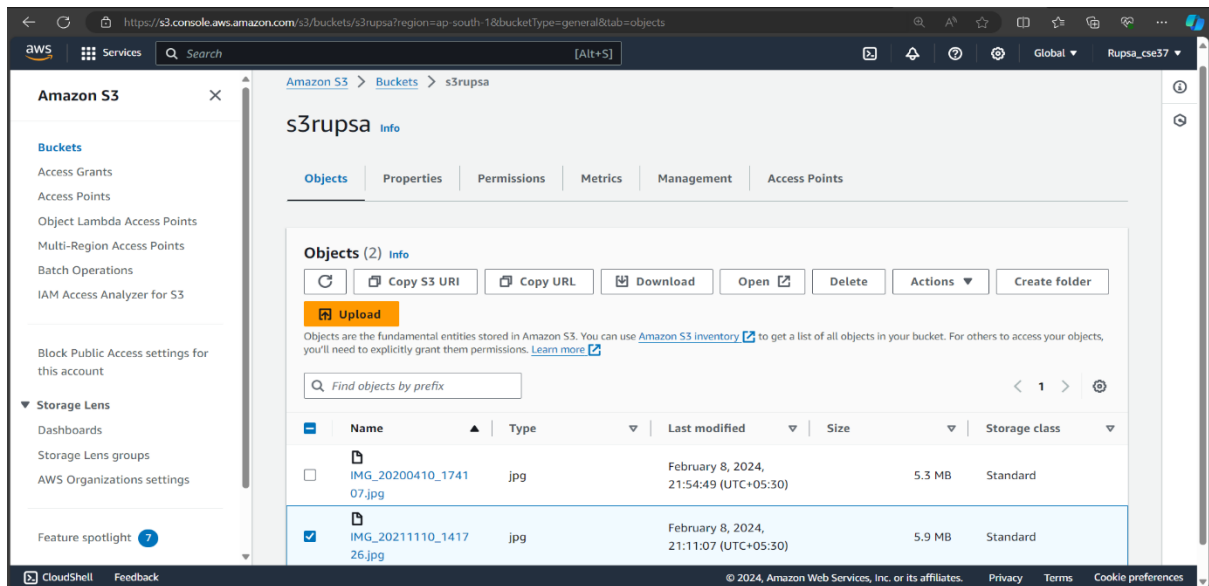
6. Click on 'Add files' then tick off the 'Name' of the file and click on 'Upload'.



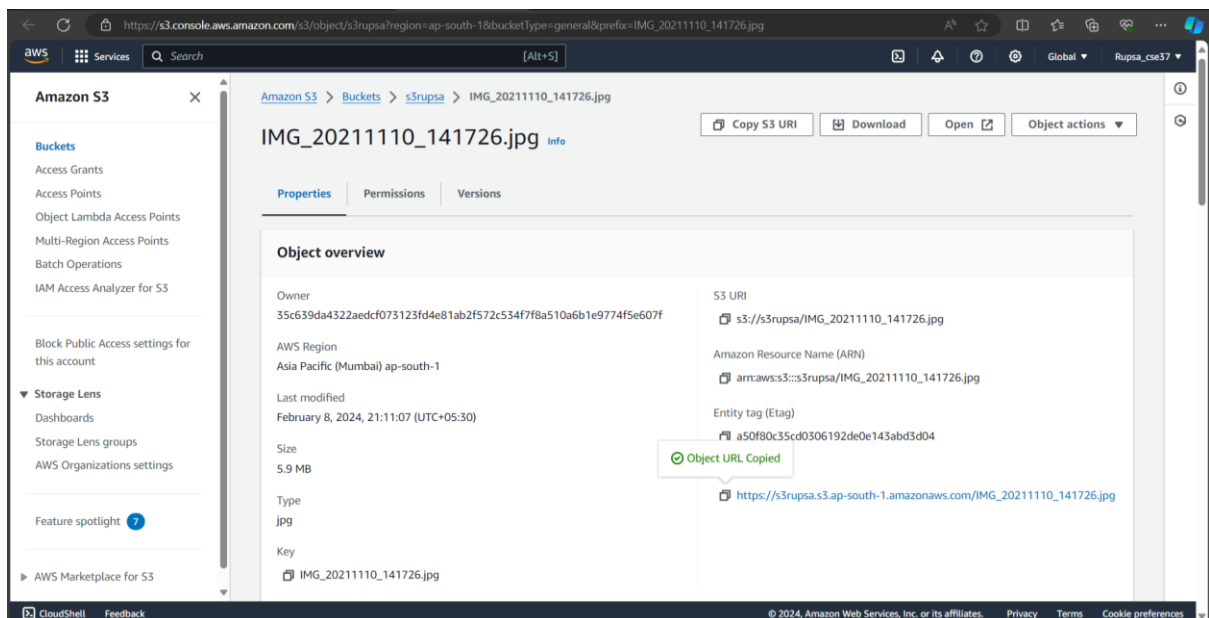
7. File is uploaded successfully , tap on 'Close' and click on 'Name'.



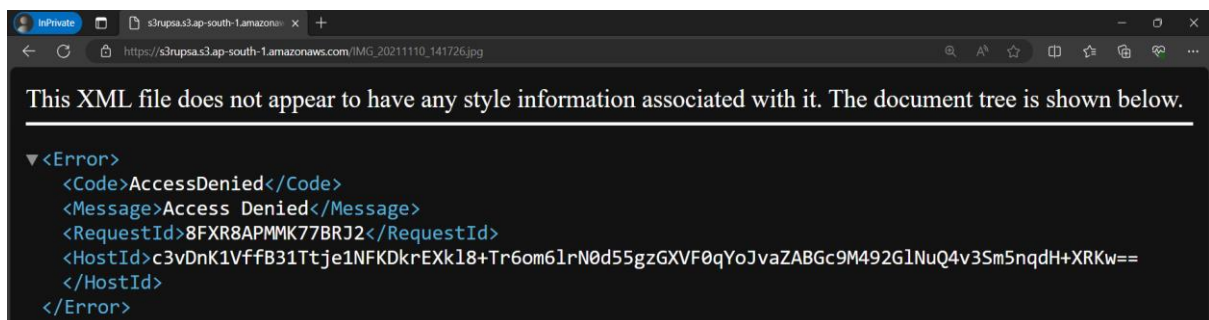
8. Under 's3rupsa', tick off any one of the files(checkbox) and click on that file.



9. Copy the 'Object URL'.

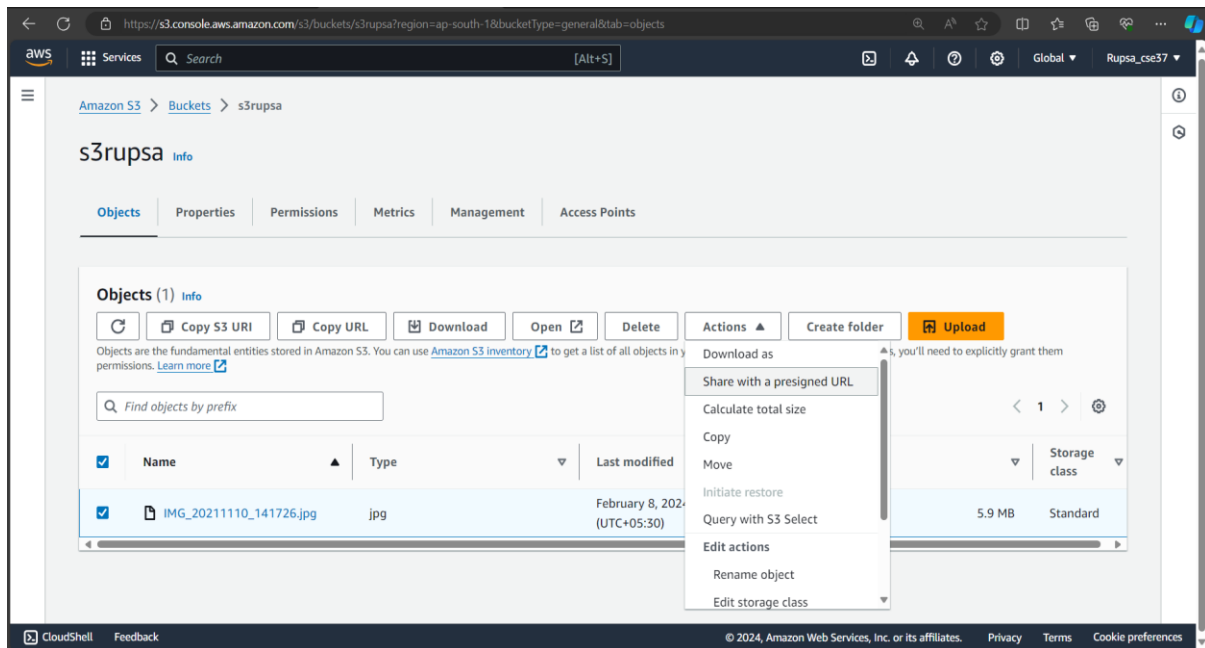


10. Now open the 'Incognito mode' and paste the 'Object URL'. We will see that the file cannot be accessed as it was a private bucket.

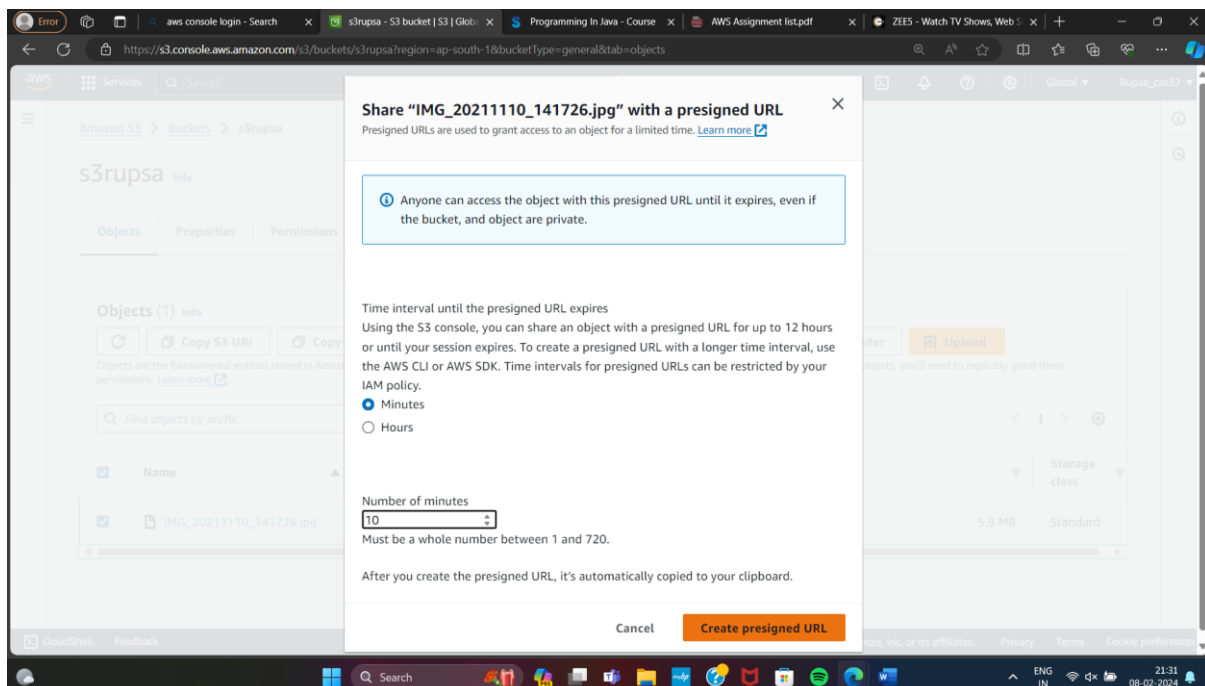


*To give access to the file , follow the steps given below.*

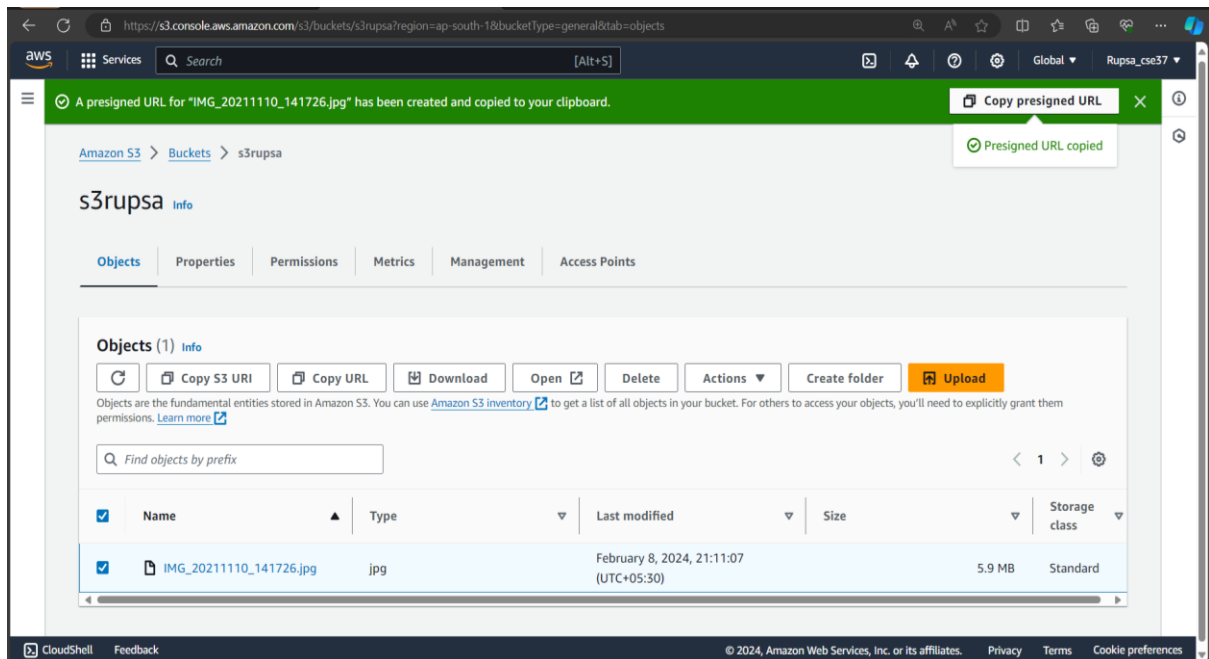
11. Go back to AWS account , select the bucket(s3rupsa) then go to 'Actions' and from there select 'Share with a presigned URL'.



12. Now according to our choice select either 'Minutes' or 'Hours' then give the number and click on 'Create presigned URL' so that the file can be accessed via presigned URL.



13. A presigned URL is created then copy the URL and paste it on 'Incognito mode'.



14. Now paste the presigned URL in the 'Incognito mode' then we can notice that the file can be accessed for 10 minutes.

