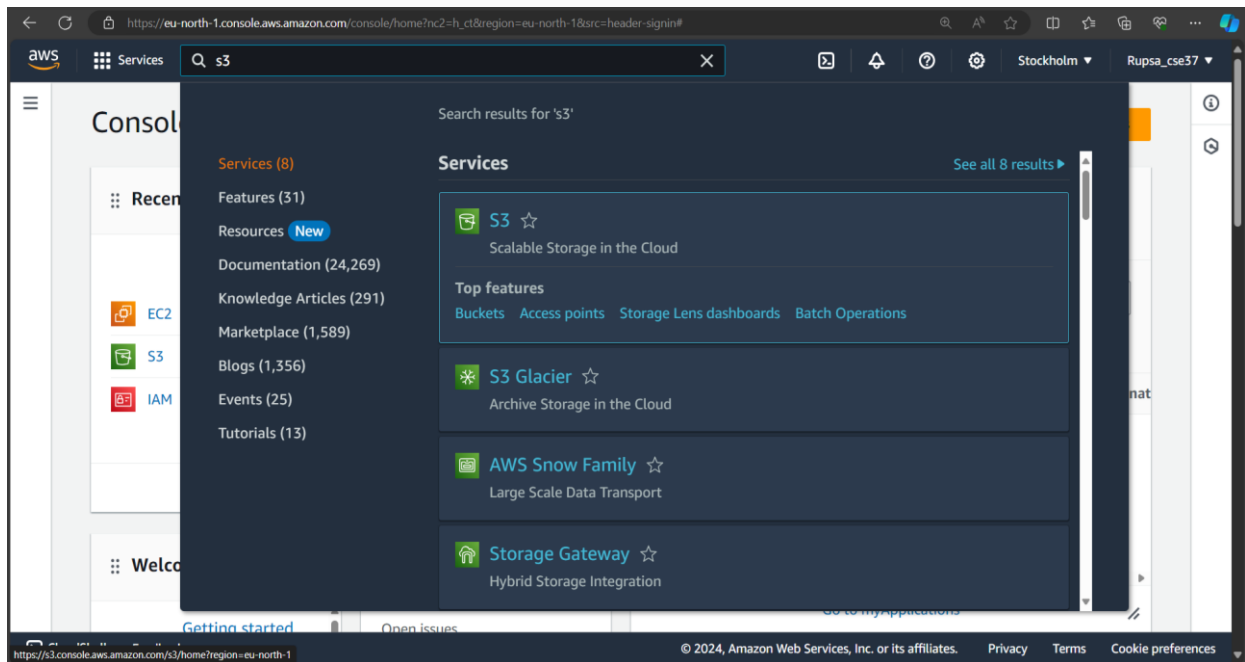


## PROBLEM STATEMENT :

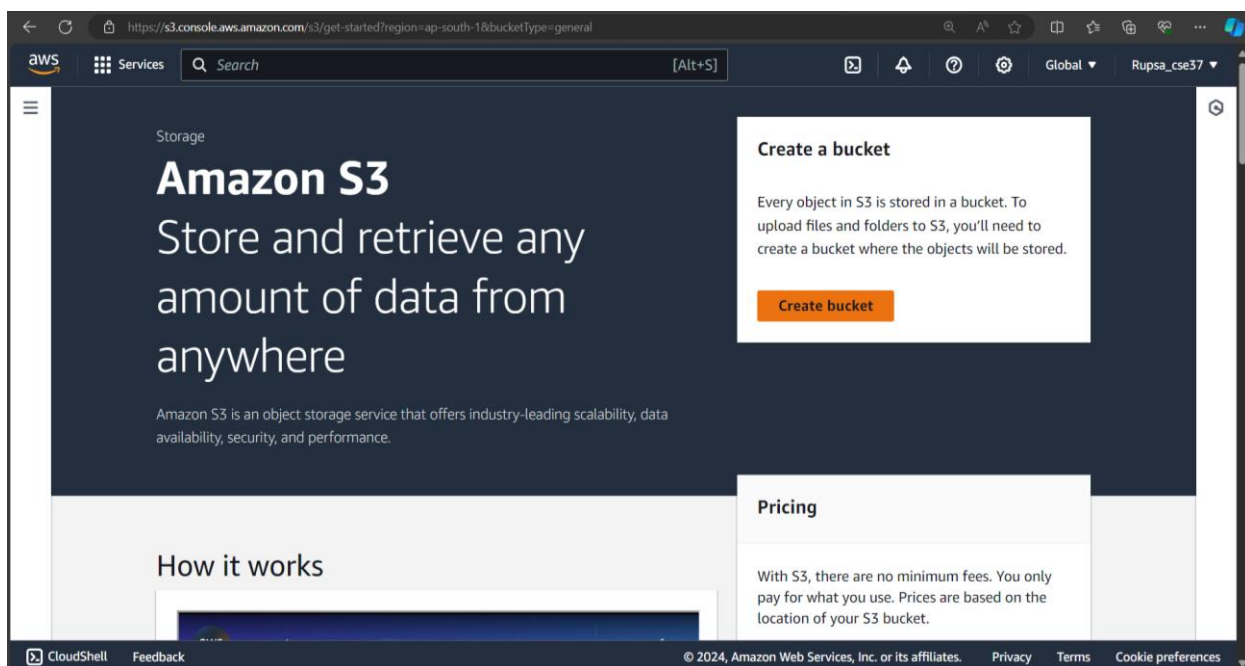
6) Upload a static website on S3.

### ***Steps to upload a static website on S3->***

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



2. Click on 'Create bucket'.



3. Fill up the required details->'Aws Region', 'Bucket name', click on 'ACLs enabled', uncheck 'Block all public access...', tick off 'I acknowledge...' and then click on 'Create bucket'.

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

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  
awsinsps

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.

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.

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

**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 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**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

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

No tags associated with this bucket.

**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](#)

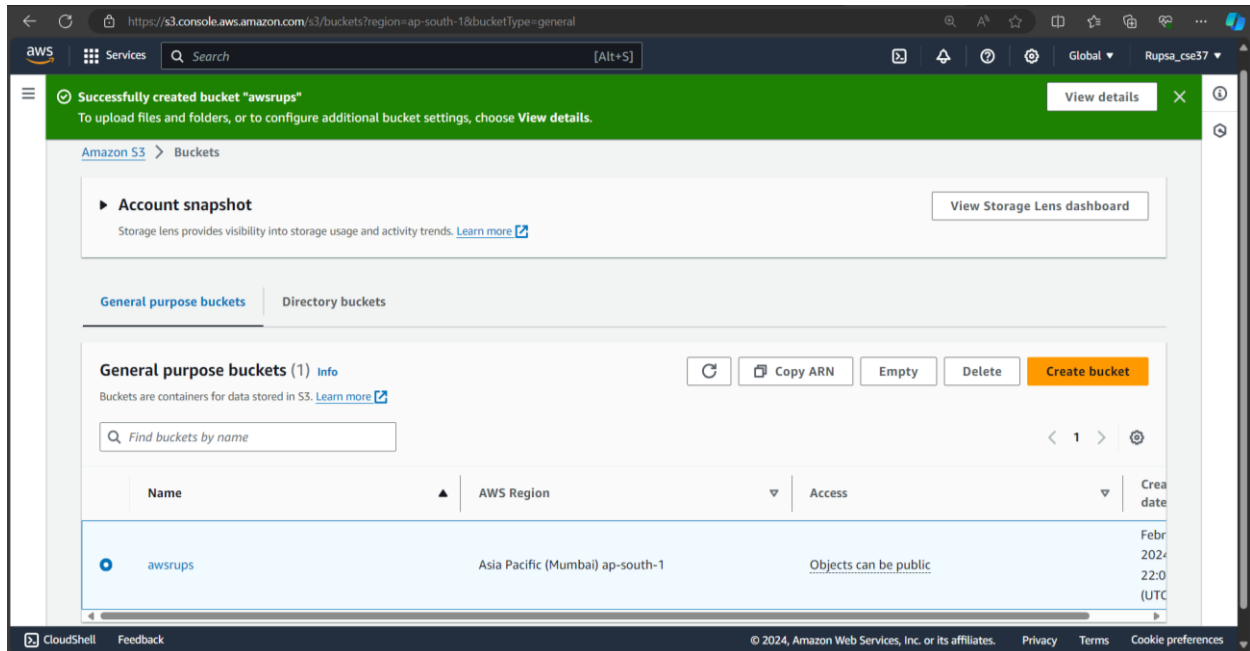
☐ Disable

☒ Enable

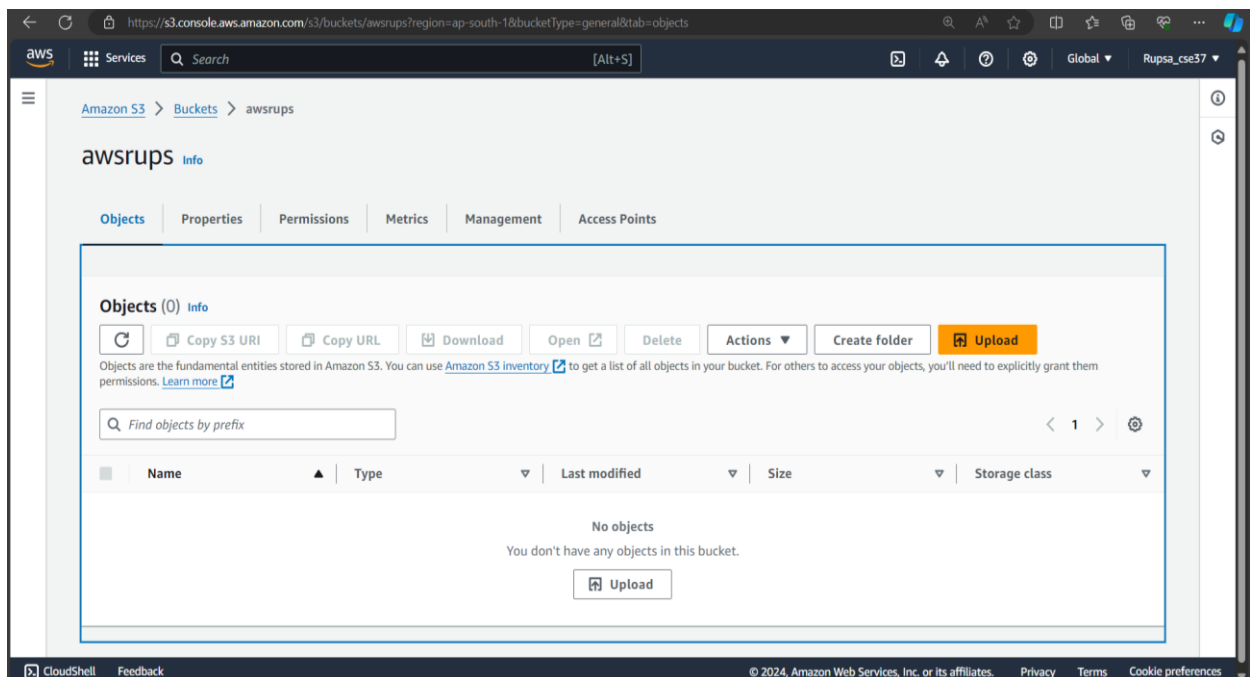
**Advanced settings**

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

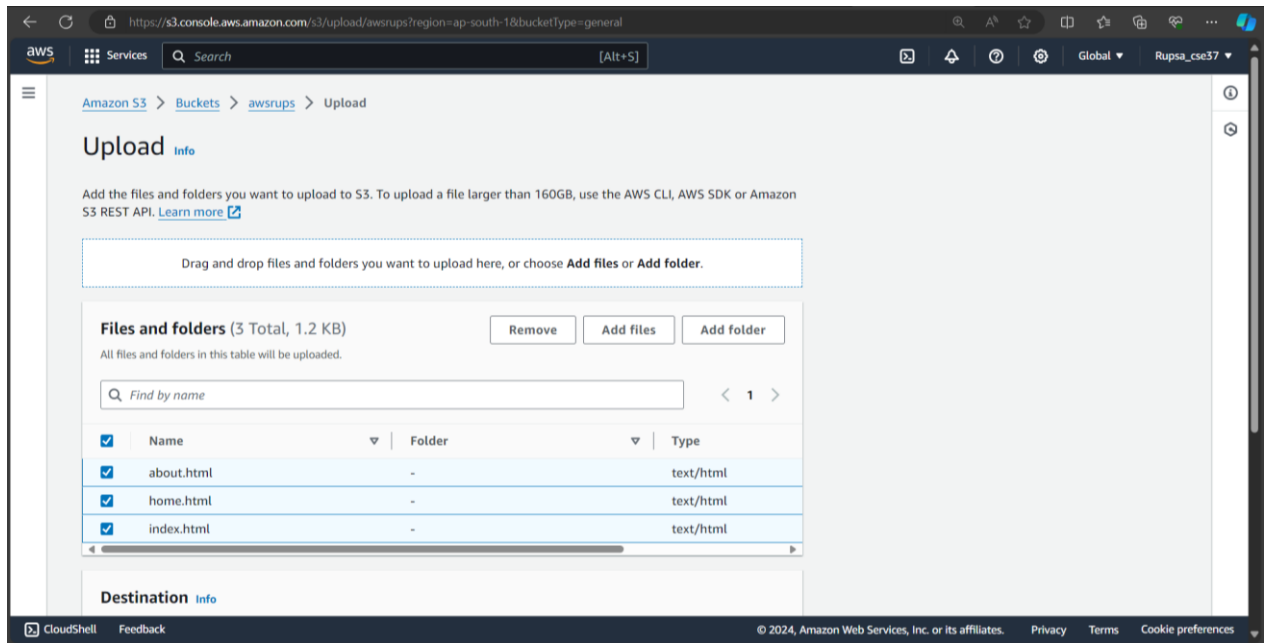
4. 'awsruops' bucket is created successfully then click on the bucket name 'awsruops'.



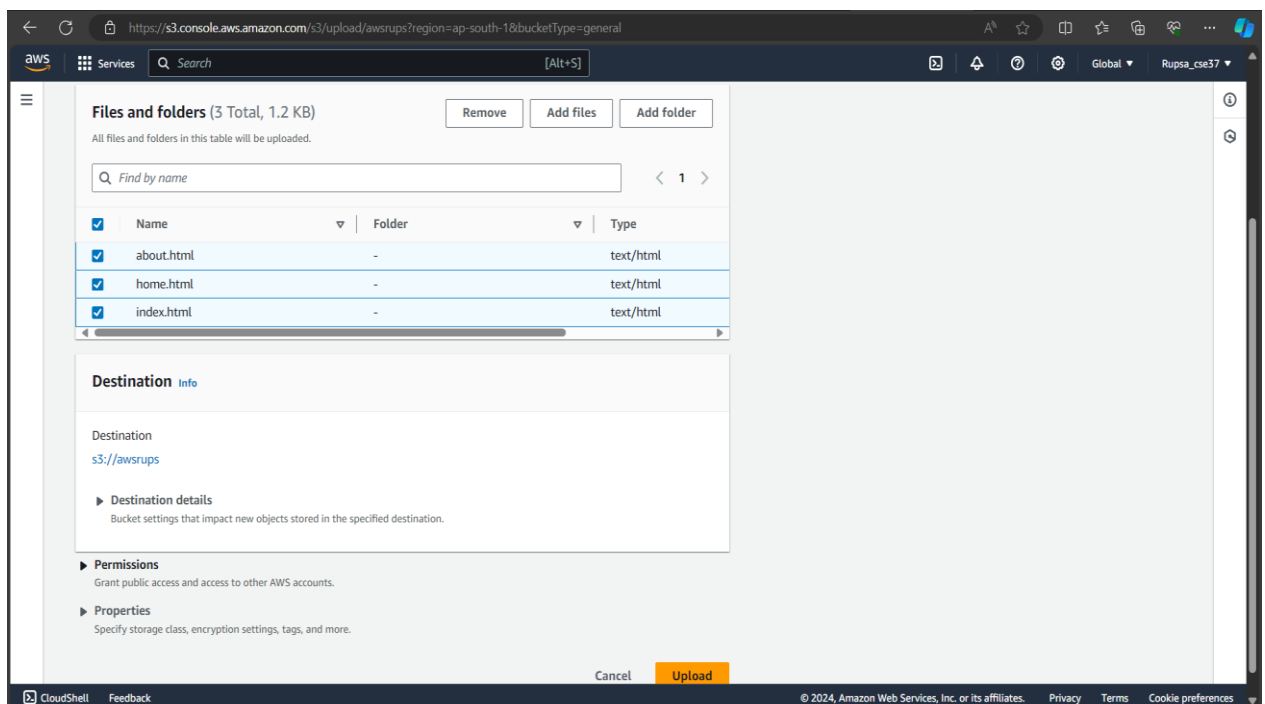
5. Under 'awsruops', click on 'Upload' then choose three html files and upload it.



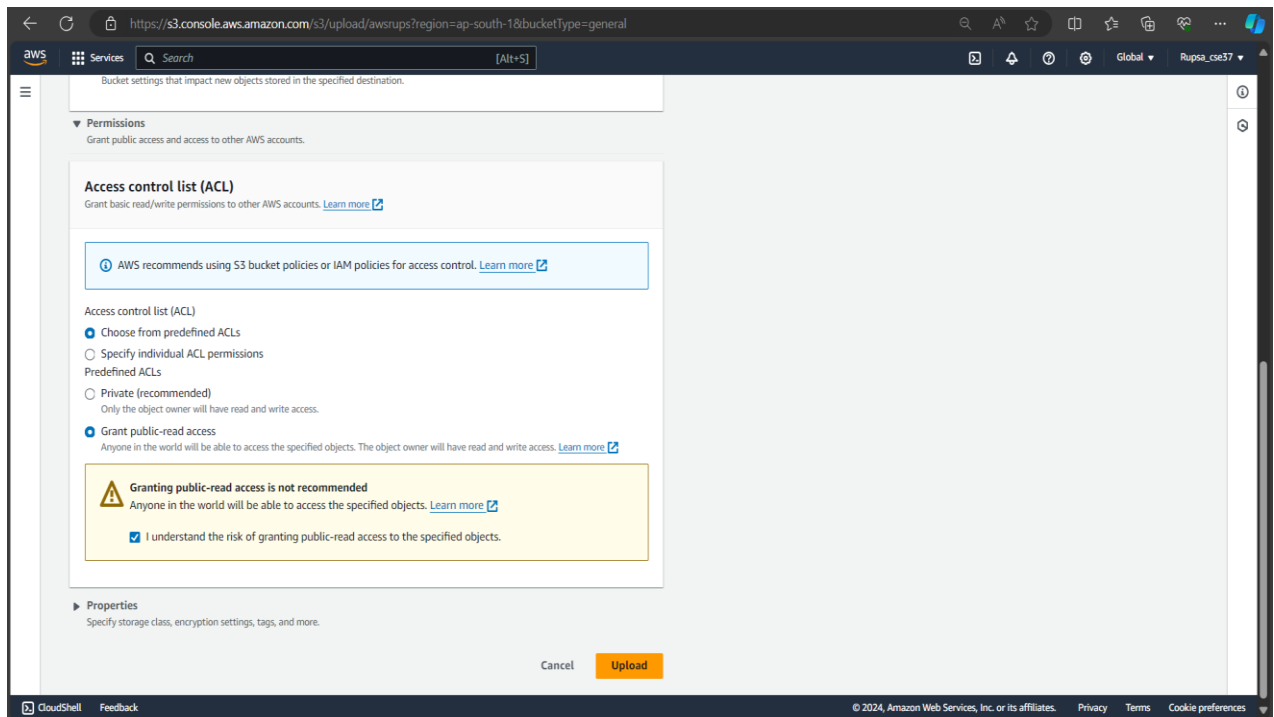
6. Click on 'Add files' and add the three html files namely 'index.html', 'about.html' and 'home.html' then tick off the 'Name' of the files.



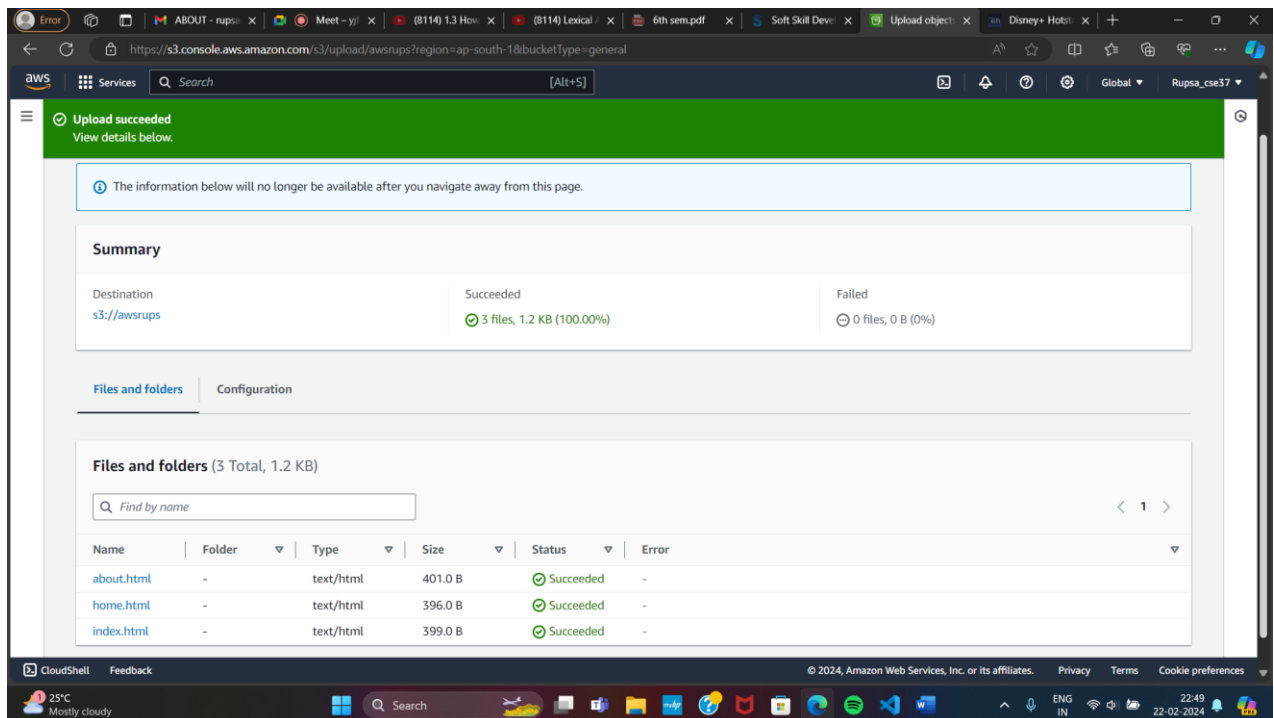
7. After ticking off 'Name' of the files go to 'Permissions' and click on it.



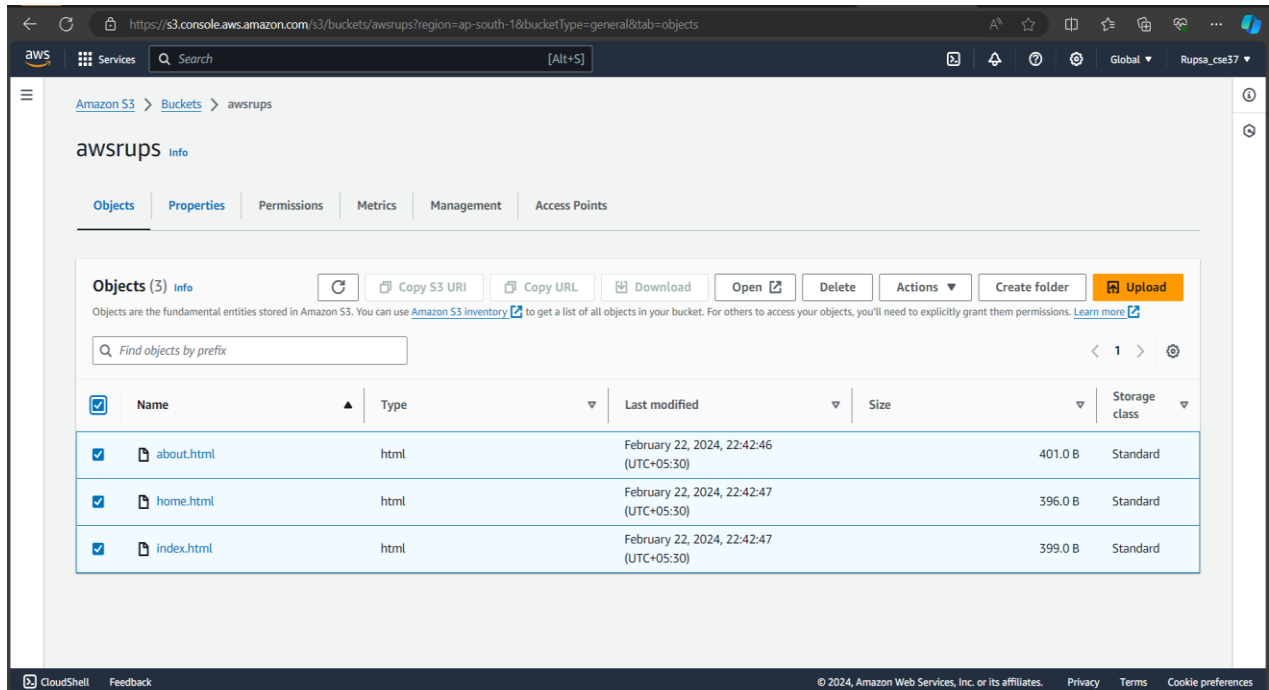
8. Under 'Permissions', click on 'Grant public-read access' then tick off the checkbox 'I understand...' and then click on 'Upload'. In this method we directly give the public access to all the selected files altogether.



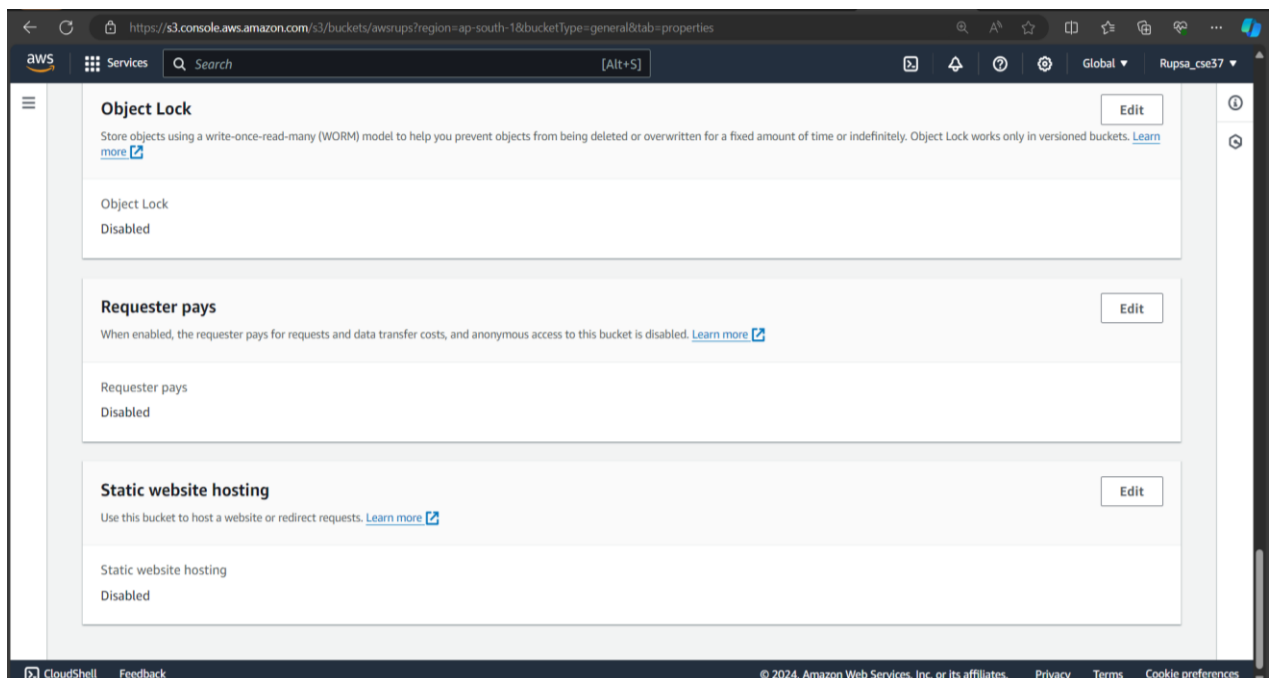
9. All the three files are successfully uploaded.



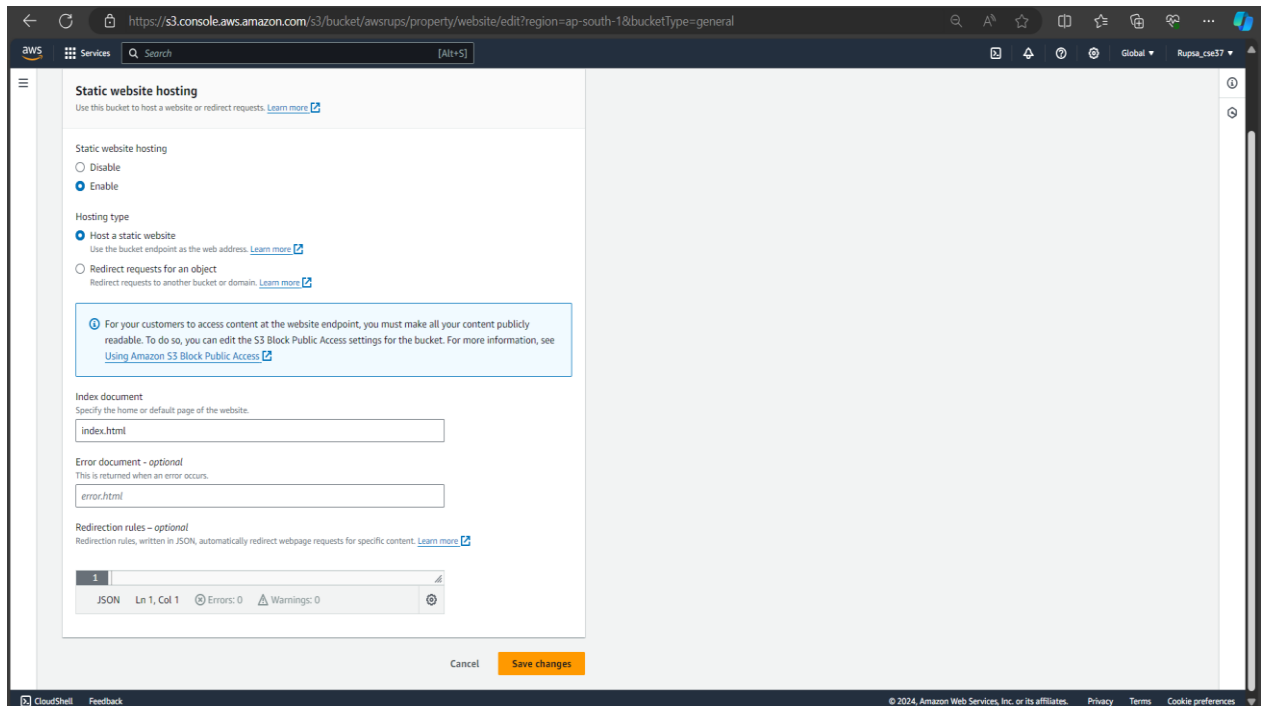
10. Under 'awsruops', select the 'Name' of the files and go to 'Properties'.



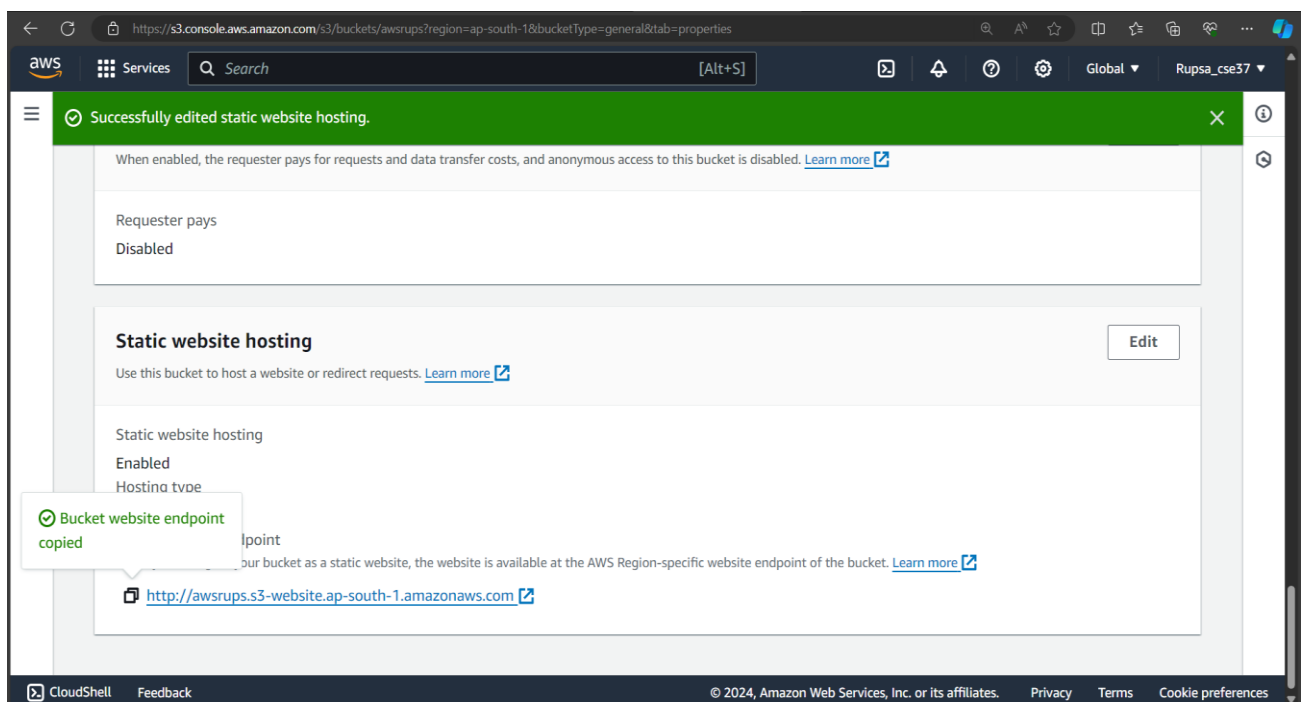
11. Under 'Properties', go to 'Static website hosting' and click on 'Edit'.



12. Under 'Static website hosting', click on 'Enable', then fill in the name of index document and click on 'Save changes'.



13. The 'Static website hosting' is successfully edited. Now under 'Static website hosting', copy the 'Bucket website endpoint'.



14. Open a new browser in incognito mode and paste the 'Bucket website endpoint' on the address bar.

