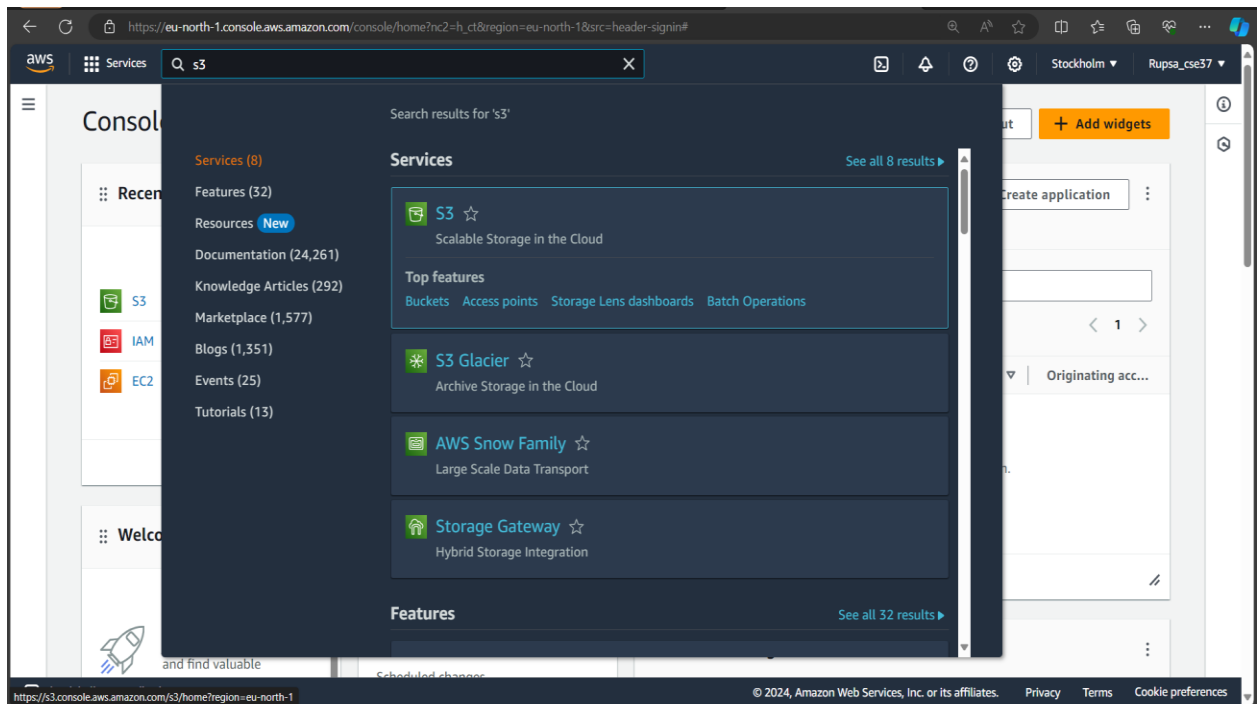


PROBLEM STATEMENT :

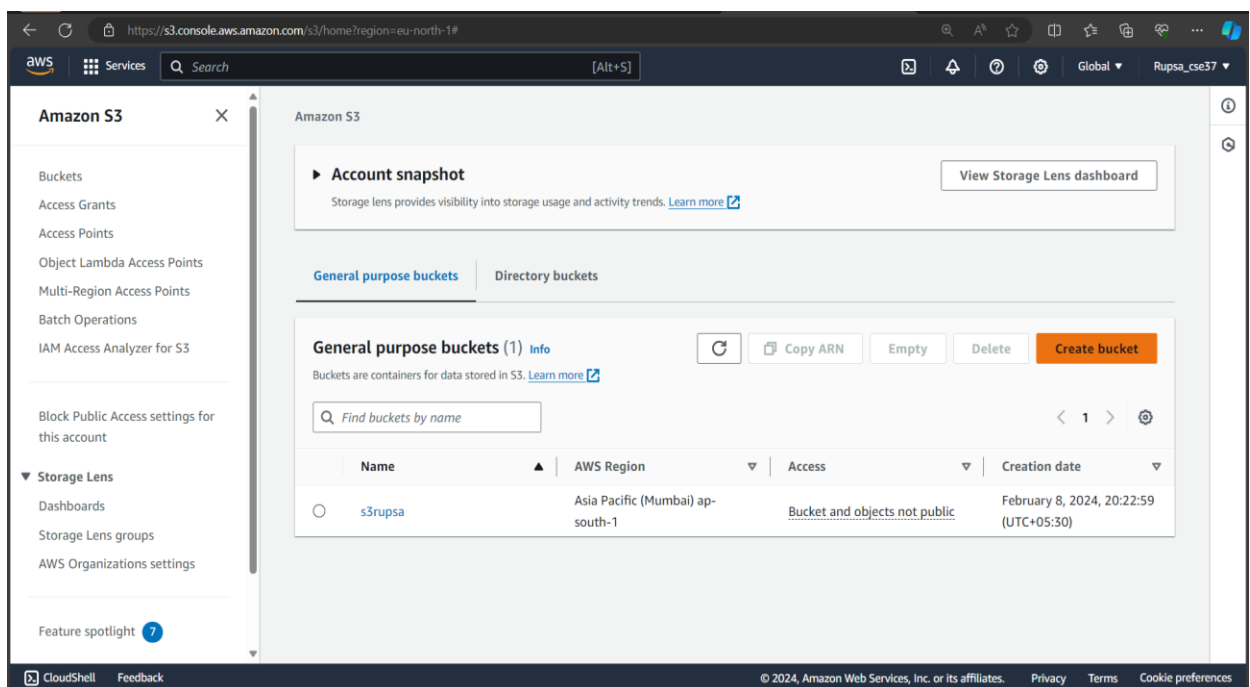
5) Create a public bucket in AWS. Upload a file and check by reassigned URL whether you can access the file or not.

Bucket creation and checking for access->

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



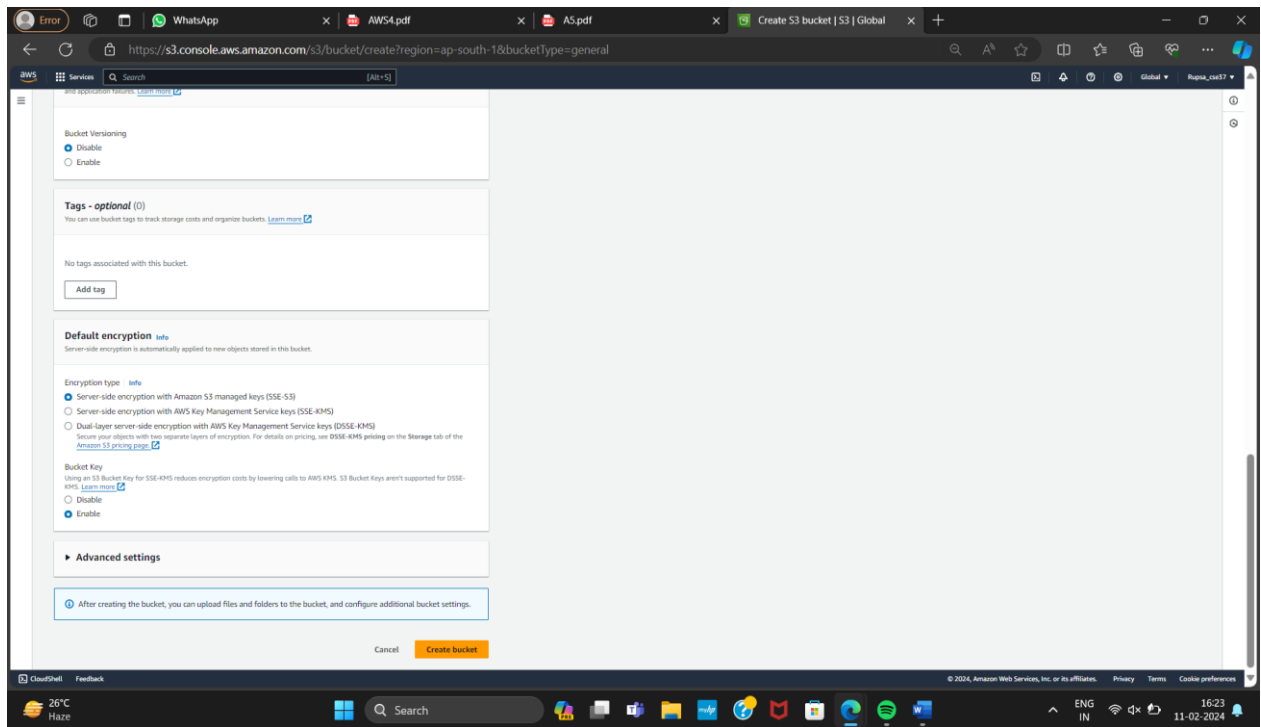
2. Click on 'Create bucket'.



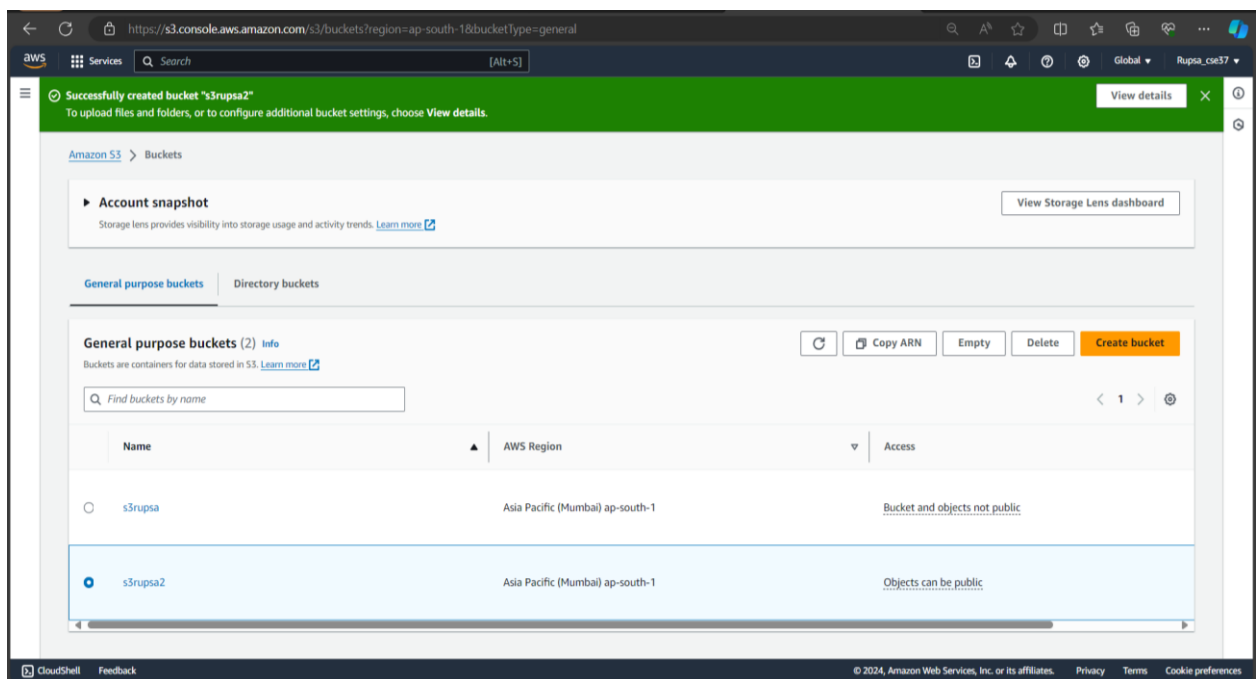
- Fill up the required details->'AWS region','Bucket name', click on 'ACLs enabled', uncheck 'Block all public access' , tick off 'I acknowledge....' and click on 'Create bucket'.

The screenshot shows the 'Create bucket' page in the AWS S3 console. The browser address bar shows the URL: <https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general>. The page has a dark blue header with the AWS logo and navigation tabs for 'Services' and 'Search'. The main content area is titled 'Create bucket' with a sub-header 'Buckets are containers for data stored in S3. [Learn more](#)'. Below this, there are two main sections: 'General configuration' and 'Object Ownership'. In the 'General configuration' section, the 'AWS Region' is set to 'Asia Pacific (Mumbai) ap-south-1'. The 'Bucket name' is 's3rapsa2'. There is a note that the bucket name must be unique within the global namespace. Below this, there is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button. The 'Object Ownership' section has two radio buttons: 'ACLs disabled (recommended)' and 'ACLs enabled'. The 'ACLs enabled' option is selected. Below this, there is a warning box that says 'We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.' Below the warning box, there is a section for 'Object Ownership' with two radio buttons: 'Bucket owner preferred' and 'Object writer'. The 'Bucket owner preferred' option is selected. Below this, there is a note that says 'If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)'.

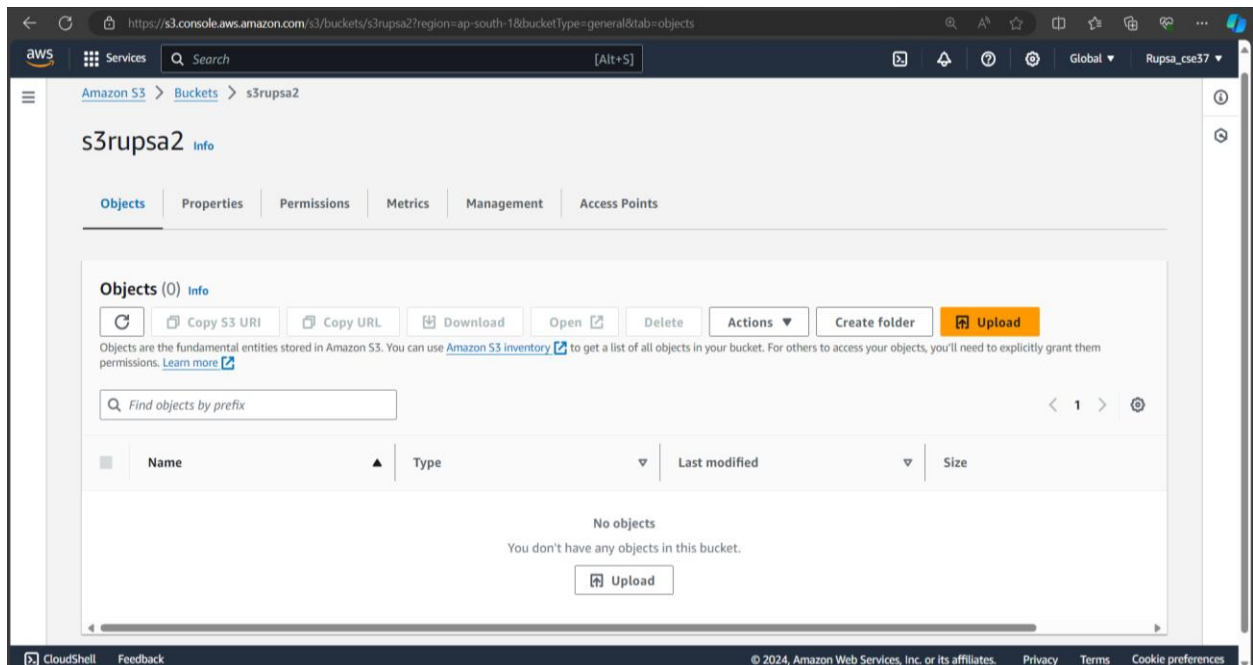
The screenshot shows the 'Create bucket' page in the AWS S3 console, continuing from the previous section. The browser address bar shows the URL: <https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general>. The page has a dark blue header with the AWS logo and navigation tabs for 'Services' and 'Search'. The main content area is titled 'Create bucket' with a sub-header 'Buckets are containers for data stored in S3. [Learn more](#)'. Below this, there are two main sections: 'Object Ownership' and 'Block Public Access settings for this bucket'. The 'Object Ownership' section has two radio buttons: 'Bucket owner preferred' and 'Object writer'. The 'Bucket owner preferred' option is selected. Below this, there is a note that says 'If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)'. The 'Block Public Access settings for this bucket' section has a checkbox for 'Block all public access'. This checkbox is unchecked. Below this, there are four sub-sections, each with a checkbox and a description: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. All four checkboxes are unchecked. Below these sub-sections, there is a warning box that says '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.' Below the warning box, there is a checkbox for 'I acknowledge that the current settings might result in this bucket and the objects within becoming public.' This checkbox is checked. Below this, there is a section for 'Bucket Versioning' with a checkbox for 'Enable bucket versioning'. This checkbox is unchecked.



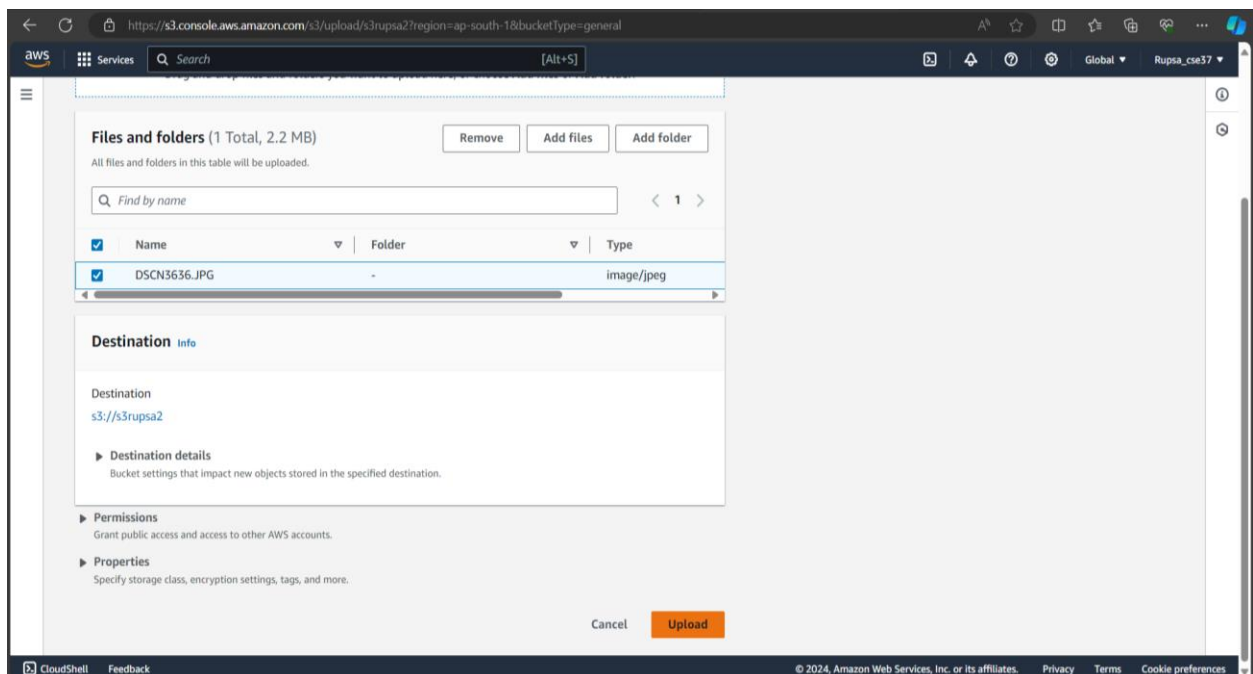
4. 's3rupsa2' bucket is created successfully then click on the bucket name 's3rupsa2'.



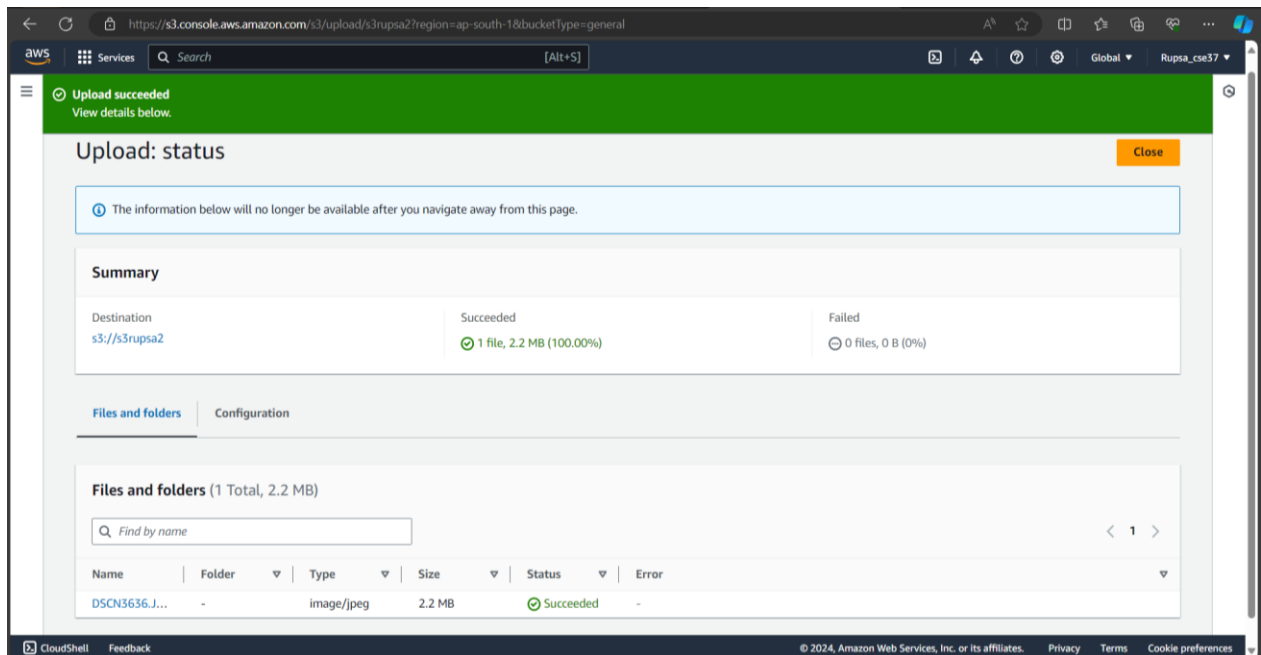
- Under 's3rupsa2', click on 'Upload' then choose a file of your choice and upload it.



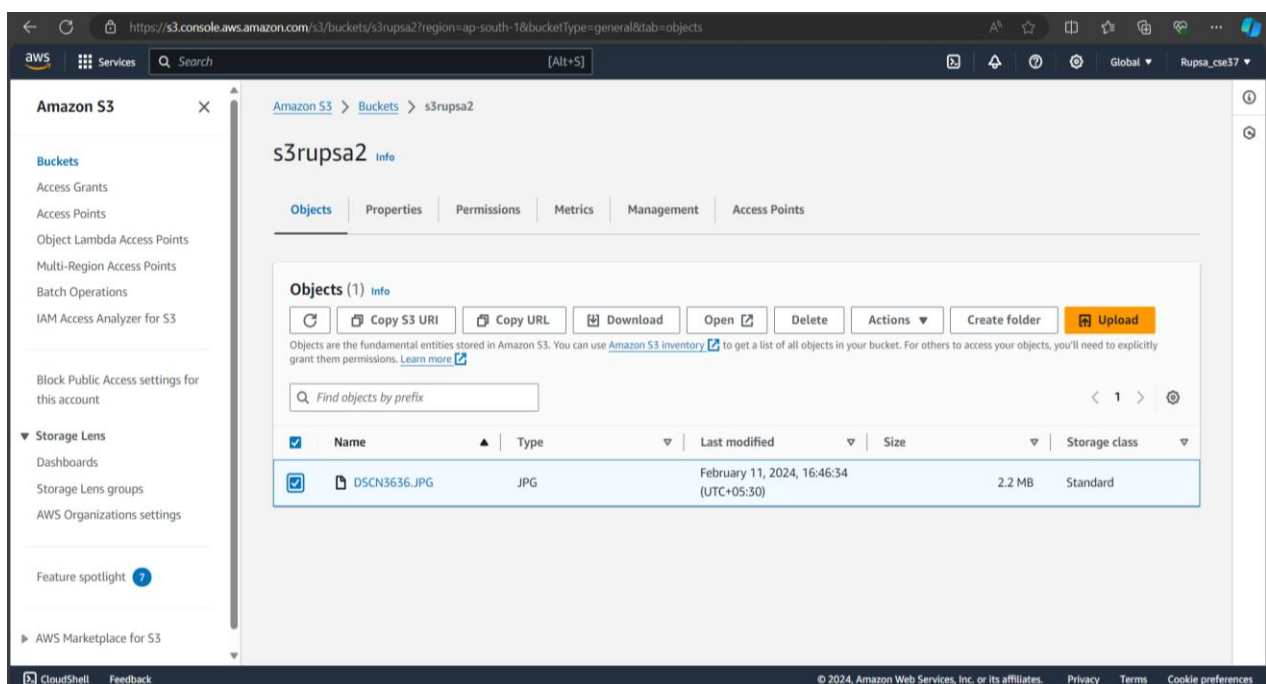
- Click on 'Add files' then tick off the 'Name' of the file and click on 'Upload'.



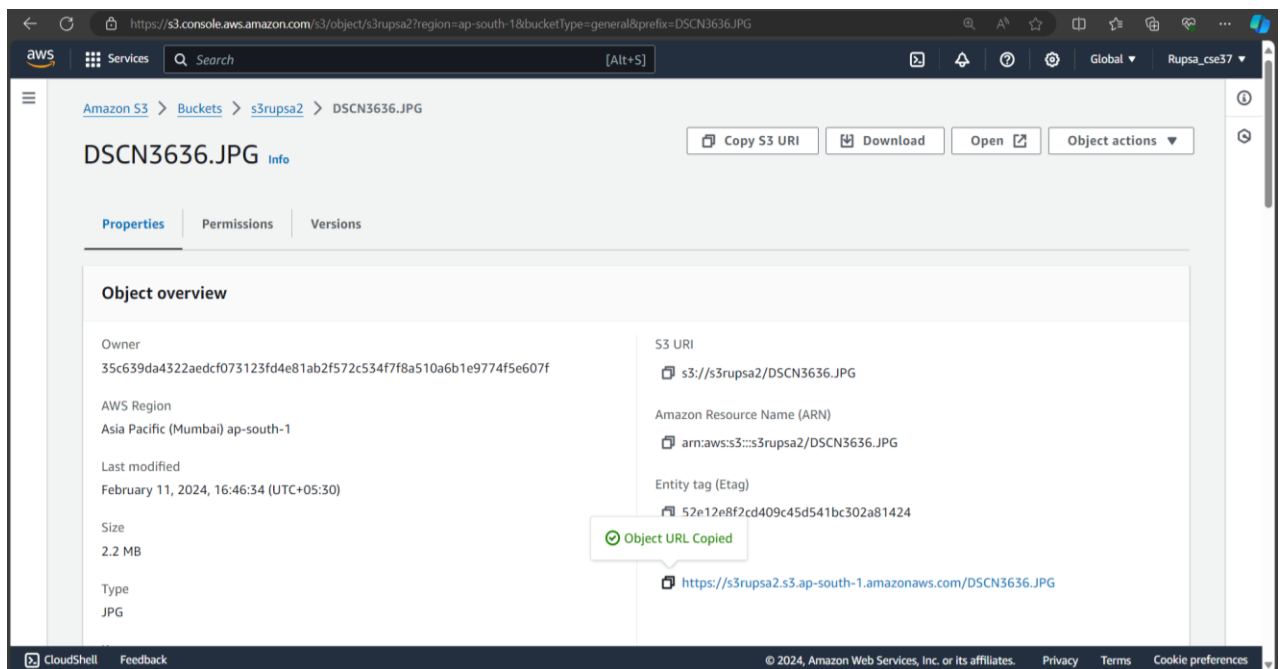
7. File is uploaded successfully , tap on 'Close' and click on 'Name'.



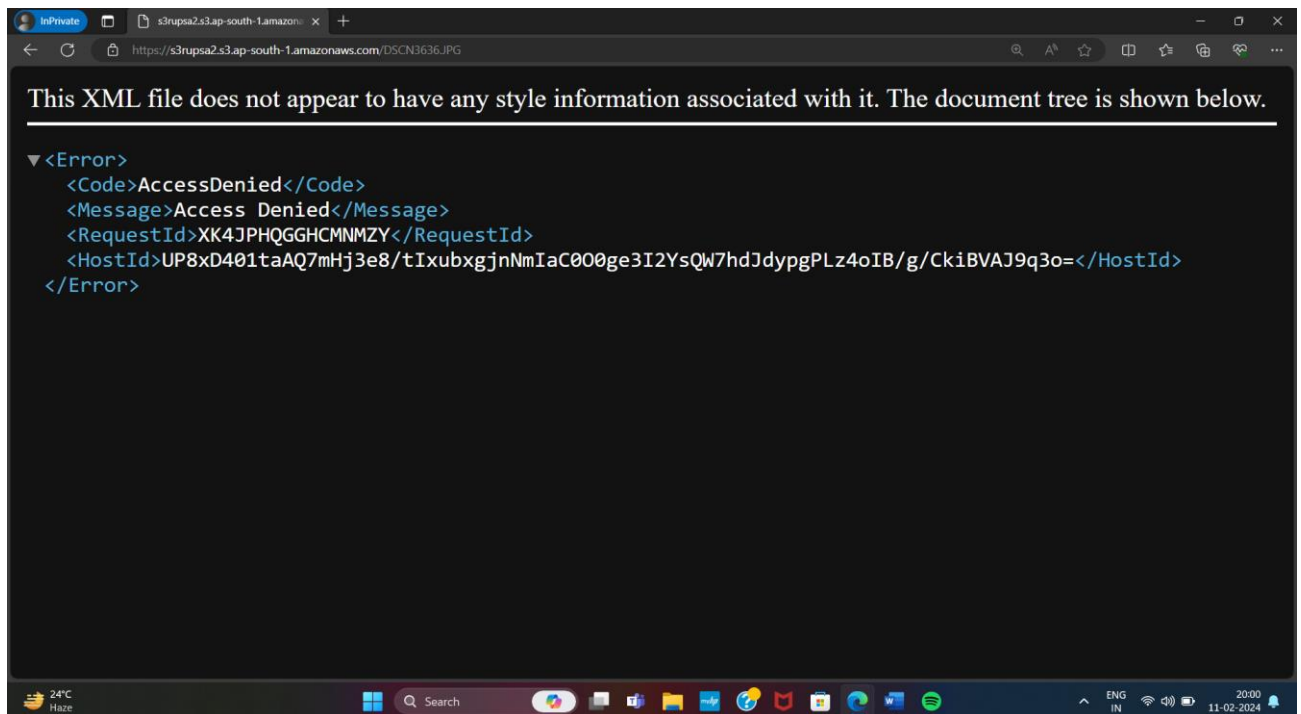
8. Under 's3rupsa2', tick off any one of the file(checkbox) and click on the file.



9. Copy the 'Object URL'.

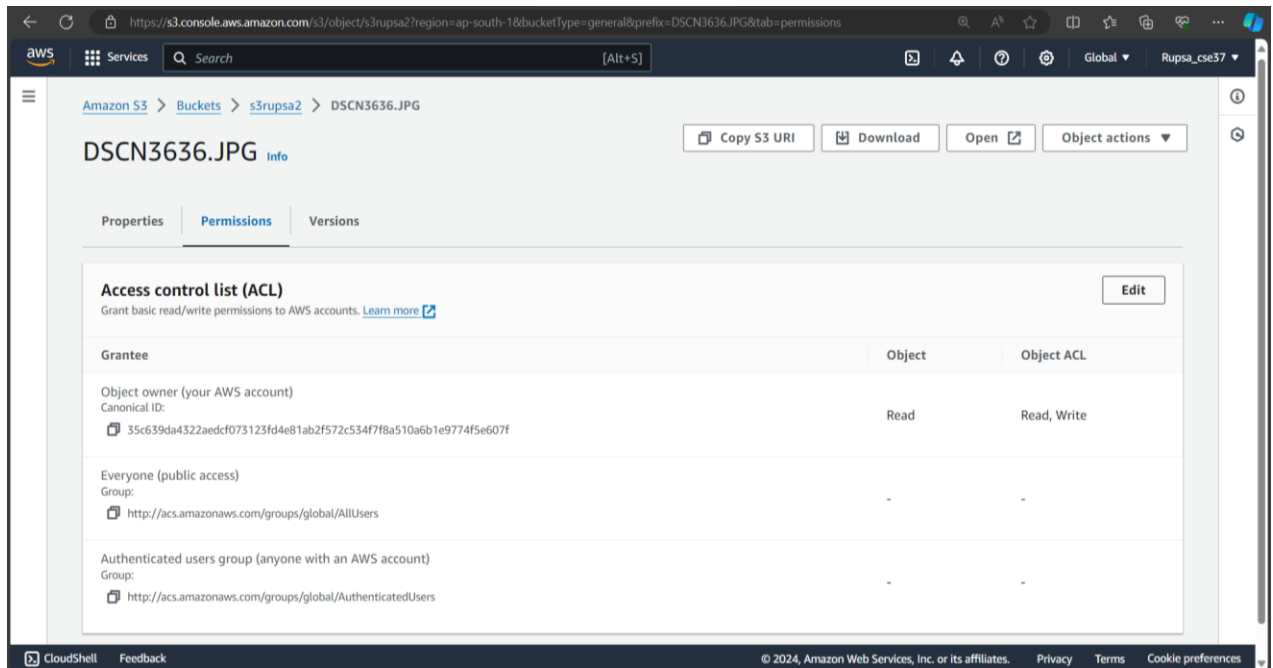


10. Now open the 'Incognito mode' and paste the 'Object URL'. You will see that the file cannot be accessed.

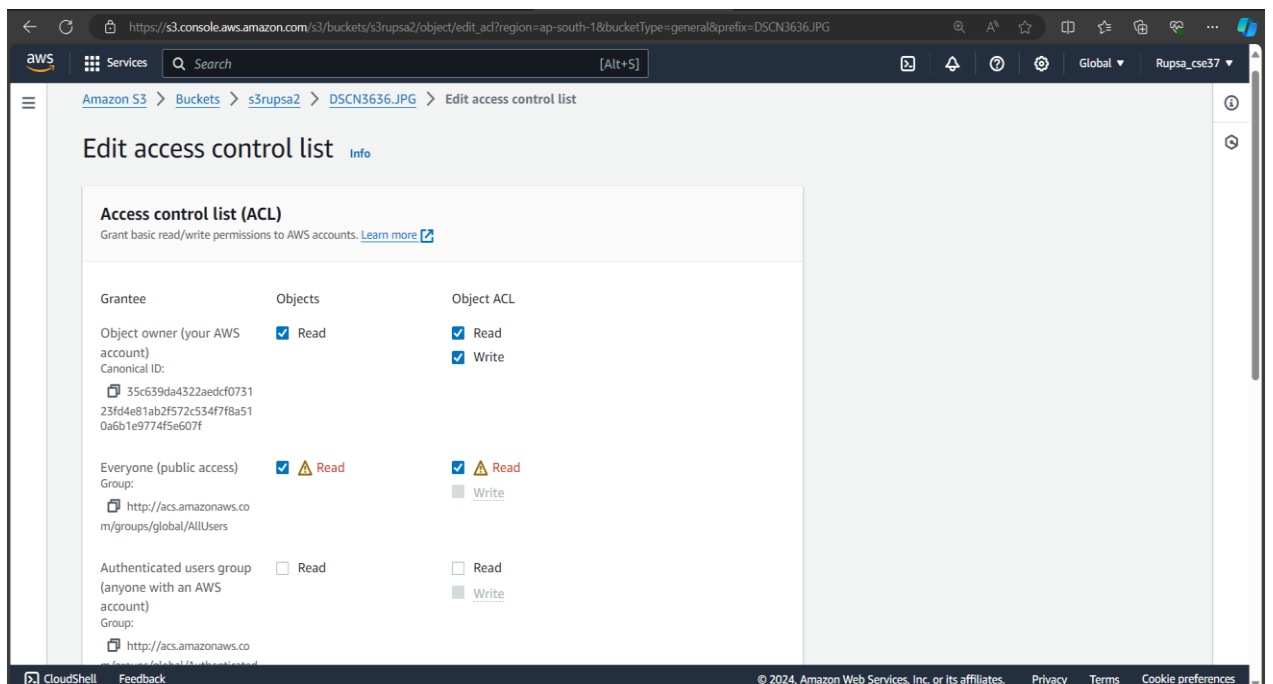


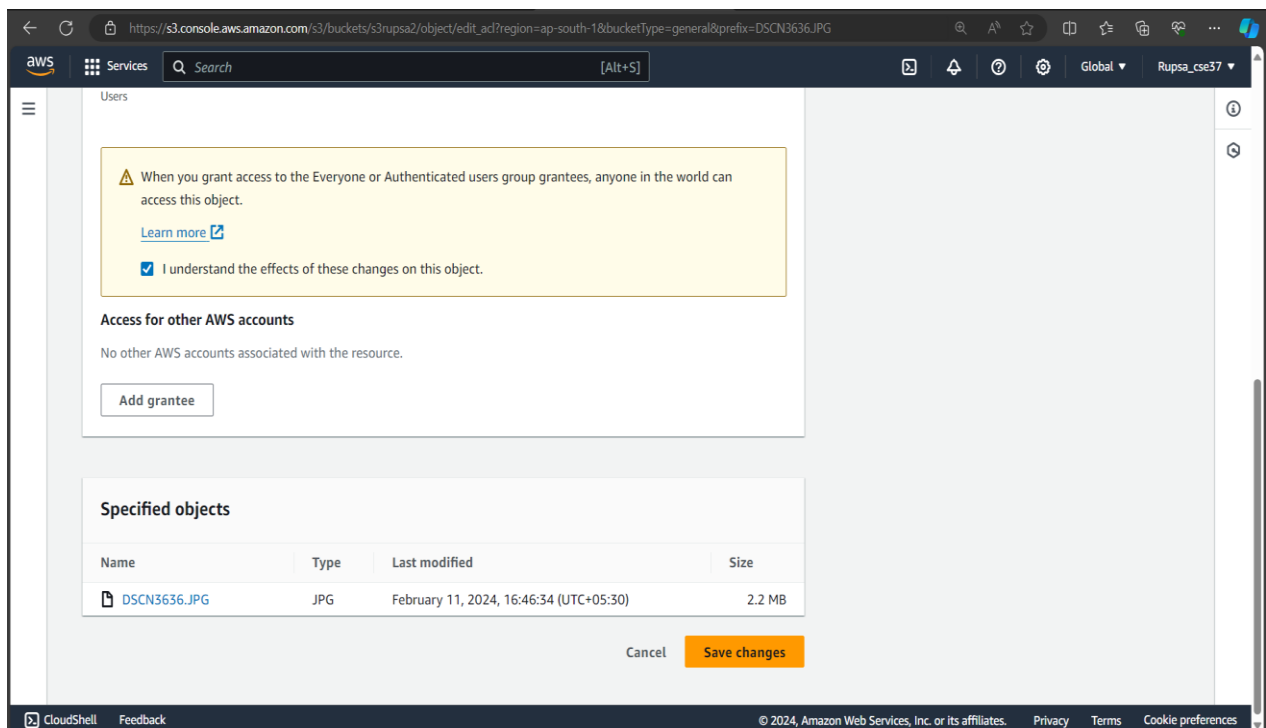
To give access to the file , follow the steps given below.

11. In the file info. click on ‘Permissions’ and then click on ‘Edit’ beside ‘Access control list(ACL)’.

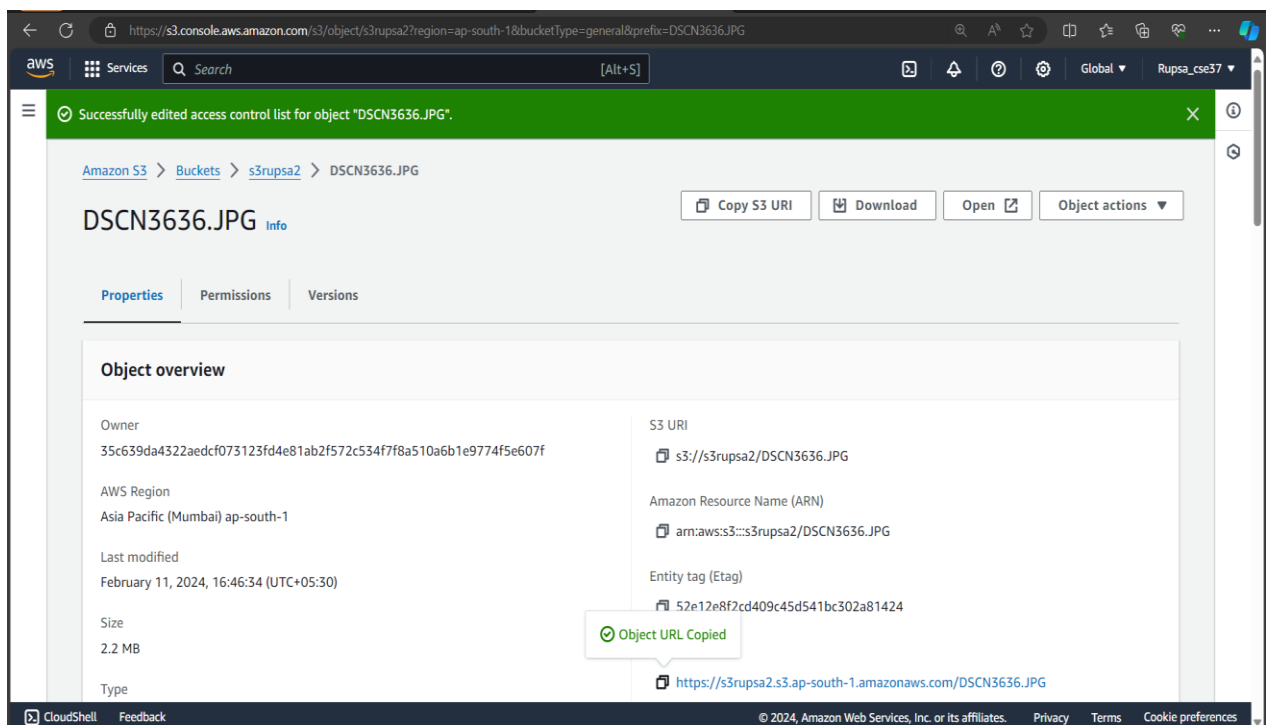


12. Now, tick off the Read checkboxes of ‘Everyone(public access)’, then tick off the checkbox ‘I understand...’ and click on ‘Save changes’.





13. Now, again copy the Object URL.



14. In the 'Incognito mode', paste the Object URL. We find that now the file can be accessed publicly.

