

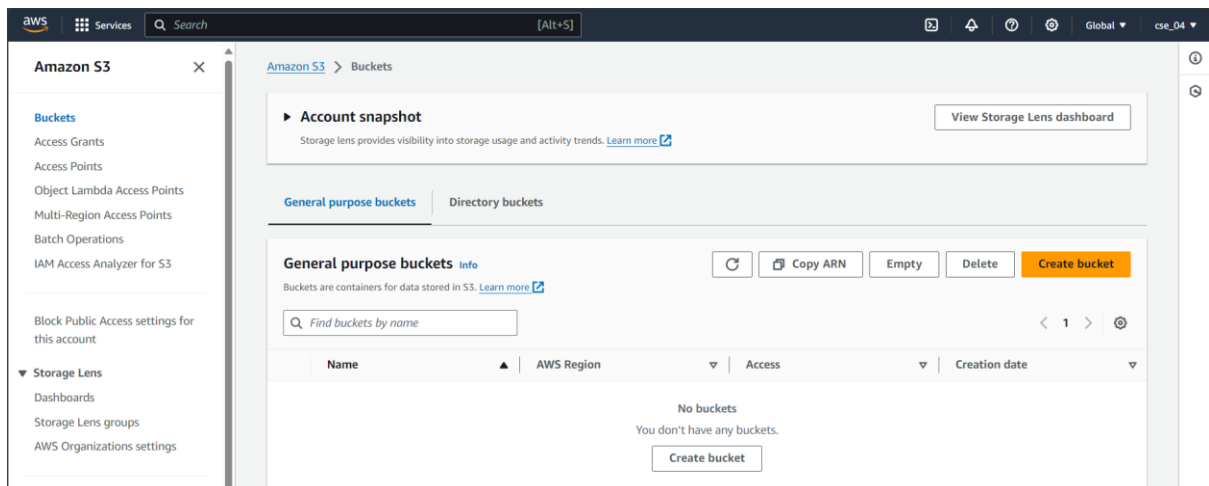
Assignment 5:

Problem Statement: Create a public Bucket in AWS. Upload a file and give the necessary permission to check whether the file URL is working.

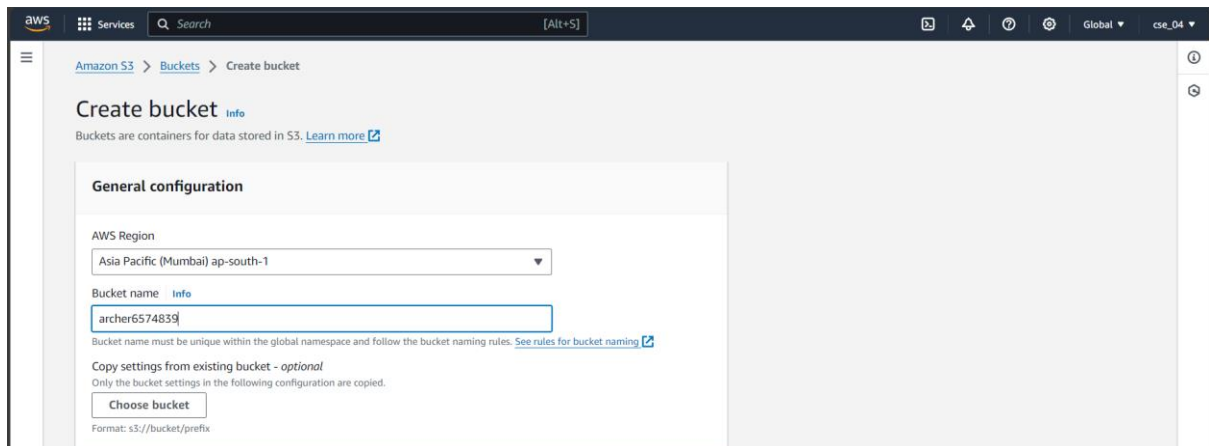
Steps:

Steps are same like private but some changes are there:

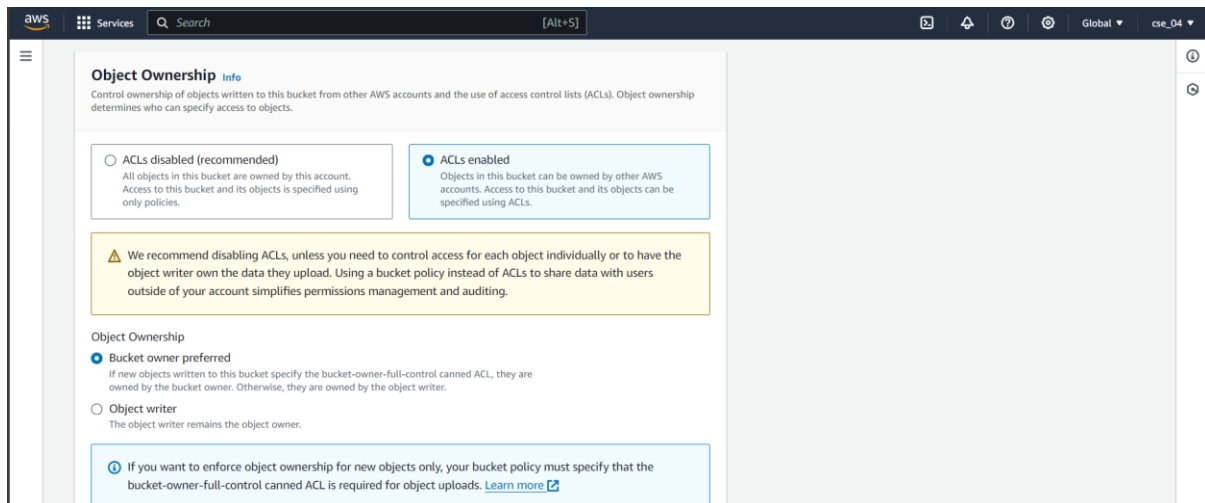
1. Click on **S3** and click on **Create bucket**.



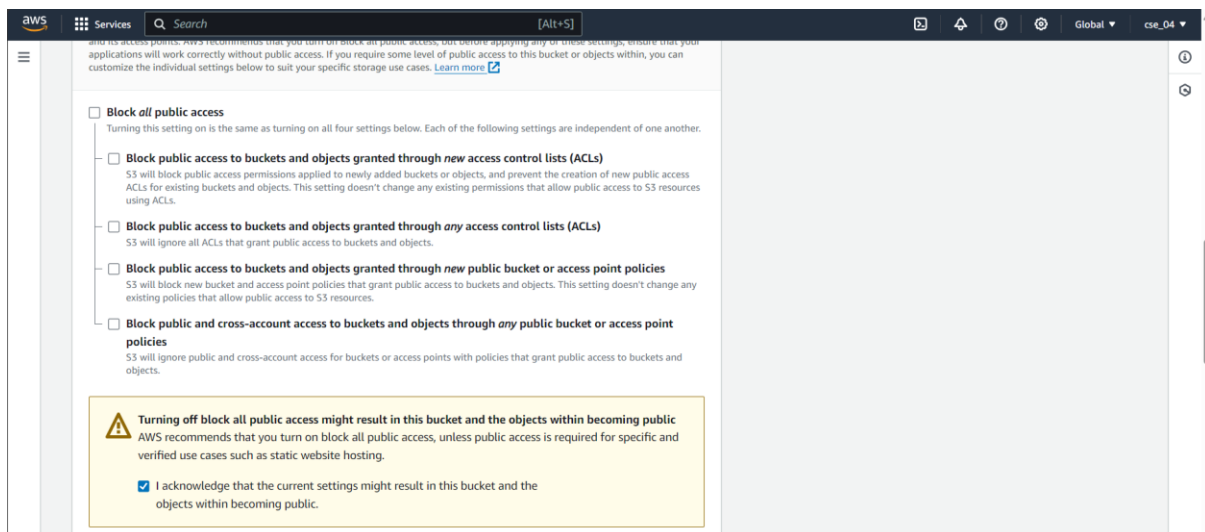
2. Now give region Mumbai and give bucket name.



3. Now click on **ACLs enabled**.



4. Now uncheck **Block all Public Access** and click on check box 'I acknowledge that the current settings might result in this bucket and the objects within becoming public'.



5. Now click on **Create bucket**.

The screenshot shows the 'Create bucket' dialog box in the AWS console. The 'Default encryption' section is active, showing options for encryption type and bucket key. The 'Encryption type' section has three radio buttons: 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' (selected), 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)', and 'Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)'. The 'Bucket Key' section has two radio buttons: 'Disable' and 'Enable' (selected). At the bottom, there are 'Cancel' and 'Create bucket' buttons.

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**

6. Now click on **bucket name**.

The screenshot shows the 'Buckets' page in the AWS console. A green banner at the top says 'Successfully created bucket "archer6574839"'. Below the banner, there's a section for 'General purpose buckets' with a table listing the bucket. The bucket 'archer6574839' is listed with the region 'Asia Pacific (Mumbai) ap-south-1' and access 'Objects can be public'. There are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

Successfully created bucket "archer6574839"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

[Amazon S3](#) > [Buckets](#)

► **Account snapshot** [View Storage Lens dashboard](#)
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets | **Directory buckets**

General purpose buckets (1) [Info](#) [Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

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

Find buckets by name

Name	AWS Region	Access	Creation date
<input type="radio"/> archer6574839	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 18, 2024, 21:29:59 (UTC+05:30)

7. Click on **Permissions**.

The screenshot shows the 'Permissions' page for the 'archer6574839' bucket. The 'Permissions overview' section shows 'Access' and 'Objects can be public'. The 'Block public access (bucket settings)' section has an 'Edit' button. Below it, the 'Block all public access' section shows a red triangle icon and the text 'Off'. There's a link to 'Individual Block Public Access settings for this bucket'.

[Amazon S3](#) > [Buckets](#) > archer6574839

archer6574839 [Info](#)

[Objects](#) | [Properties](#) | **[Permissions](#)** | [Metrics](#) | [Management](#) | [Access Points](#)

Permissions overview

Access
[Objects can be public](#)

Block public access (bucket settings) [Edit](#)
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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
⚠ Off
► [Individual Block Public Access settings for this bucket](#)

8. Now click on **edit** option of ACLs.

Access control list (ACL) Edit

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 5e6a91f25a6aa05b6f897d7aa768c1483d5a526f796984a2eb44d8a22c284784	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

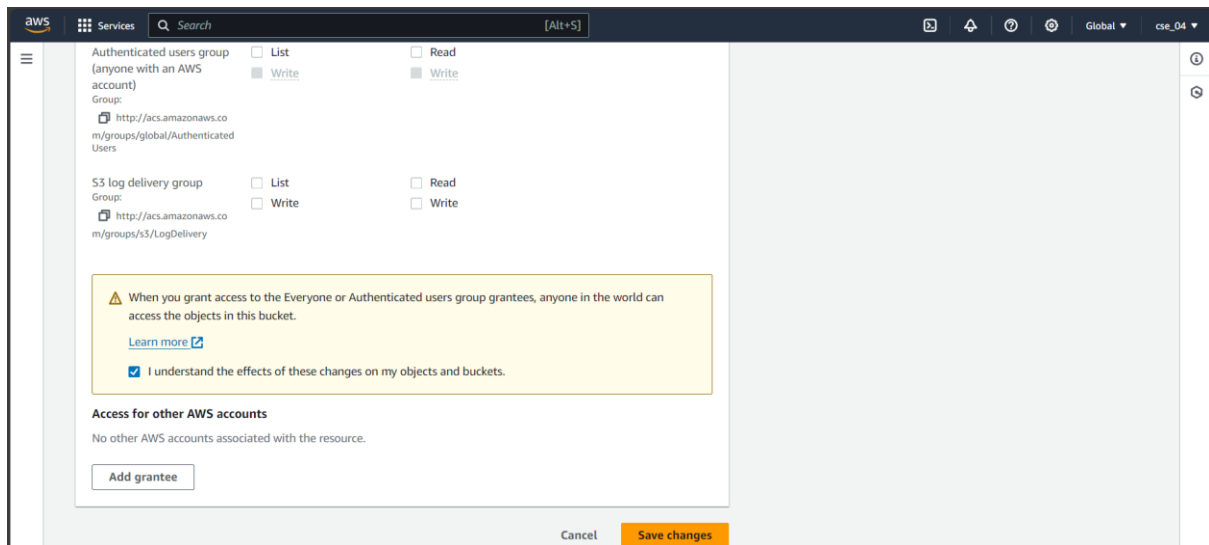
9. After this click on check box of **list** and **read** in **Everyone (public Access)**.

Edit access control list (ACL) Info

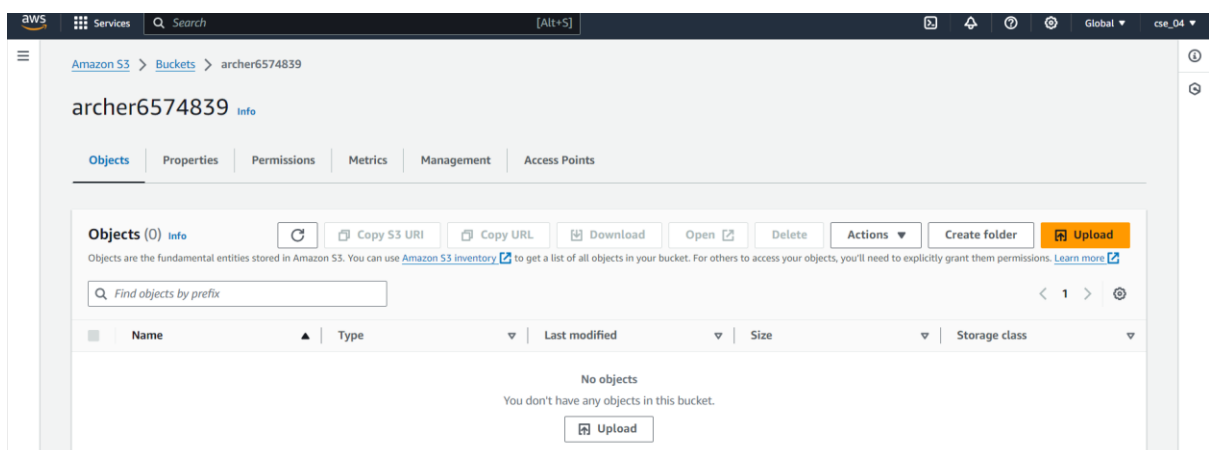
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 5e6a91f25a6aa05b6f897d7aa768c1483d5a526f796984a2eb44d8a22c284784	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account)	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

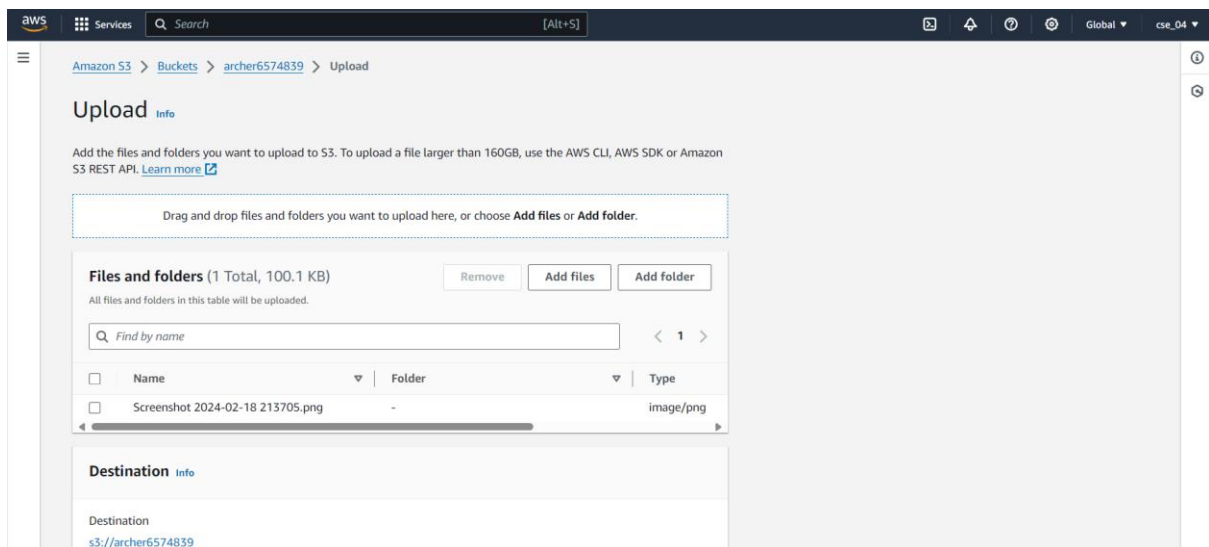
10. Now click on check box **I understand the effects of these changes on my objects and buckets** and finally click on **save changes**.



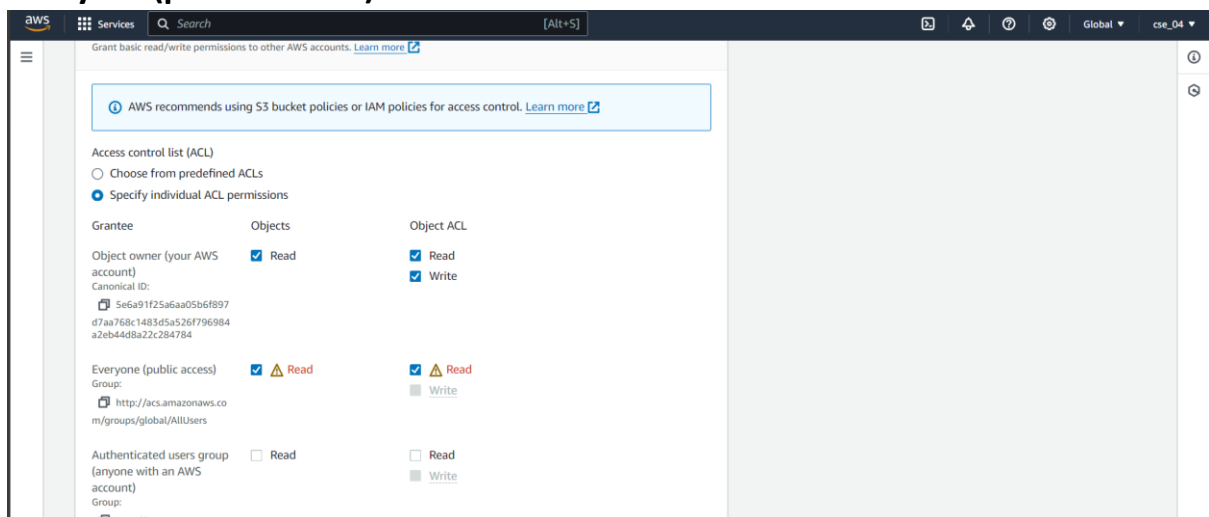
11. Now back to **buckets** option and click on **bucket name** and click on **Upload**.



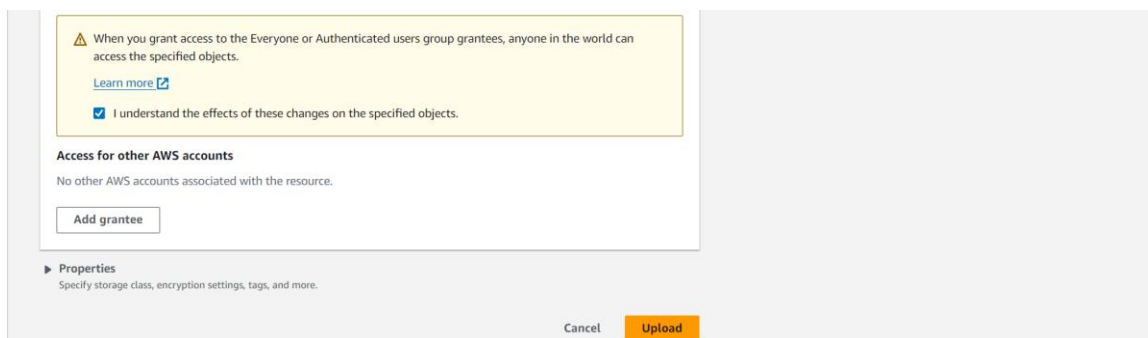
12. Click on **Add files** and upload any file.



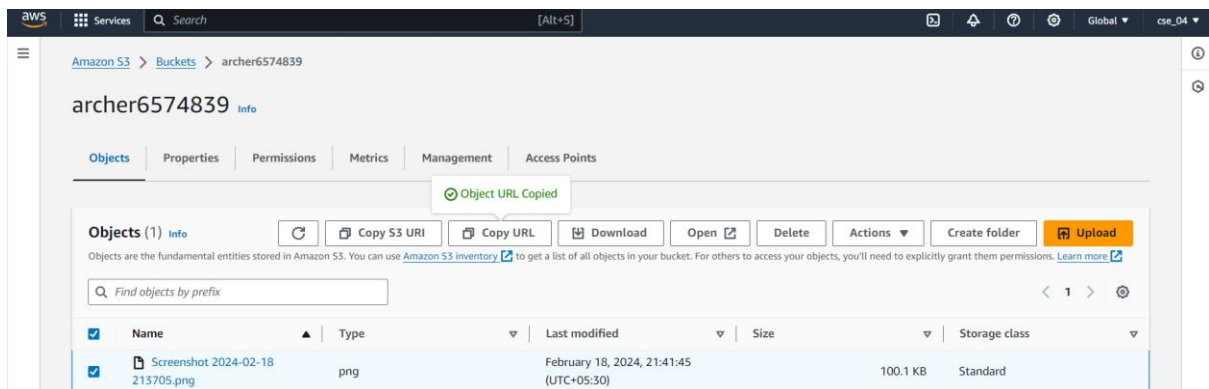
13. Now after uploading click on **Permission** dropdown and click on check box **Specify individual ACL permissions**. And click on check box of **Read in Everyone(public access)**.



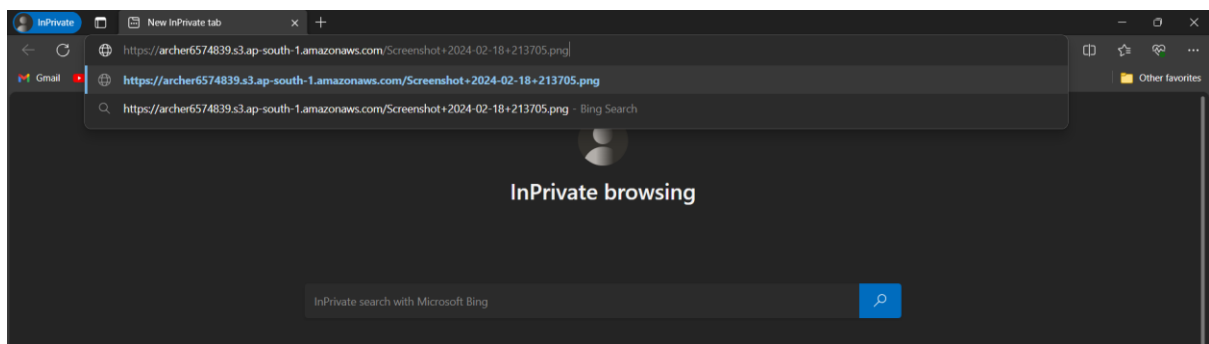
14. Now click on **I understand the effects of these changes on the specified objects** checkbox and click on **Upload**.



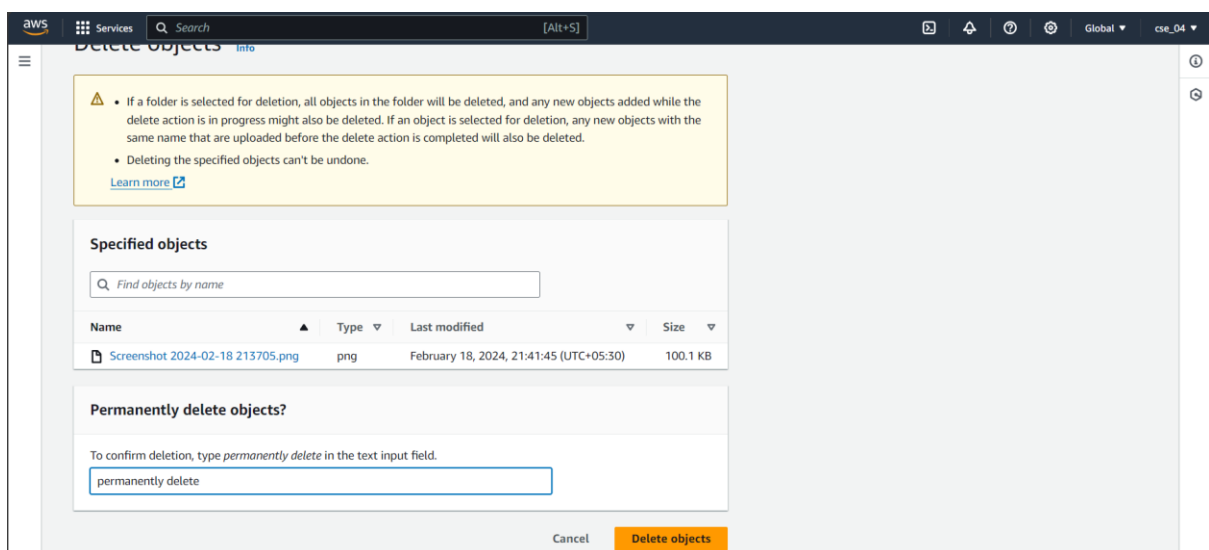
15. After successful upload now go back to bucket again. Click on **bucket name** and now click on **file** option checkbox. And then click on **Copy URL** option.



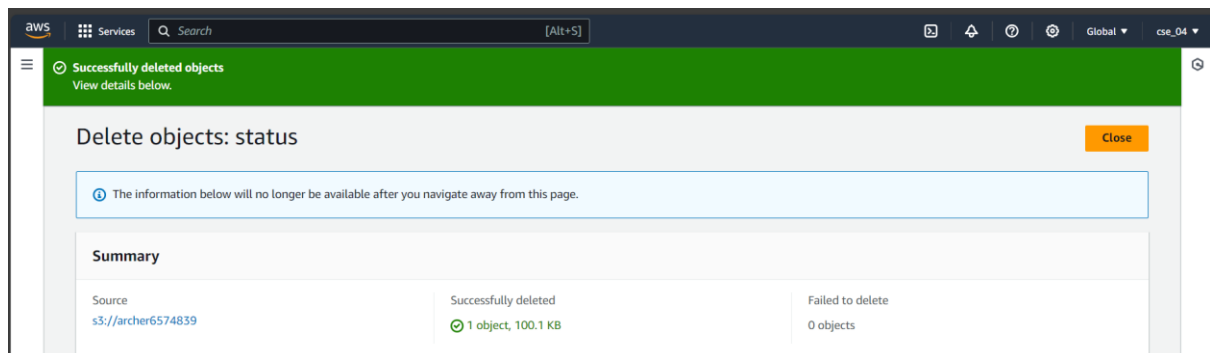
16. Now paste URL in incognito mode.



17. Anyone can access it now as it is public. Now to delete it click on **file's name** checkbox and click on **Delete** option. For permanently delete now type confirmation and click on **Delete objects**.



18. After this file will be successfully deleted. Now click on **close**.



19. Now this bucket's object is already emptied and after this click on **Delete** option after selecting check box of **bucket name**. Now for deleting type confirmation and click on **Delete bucket**.

