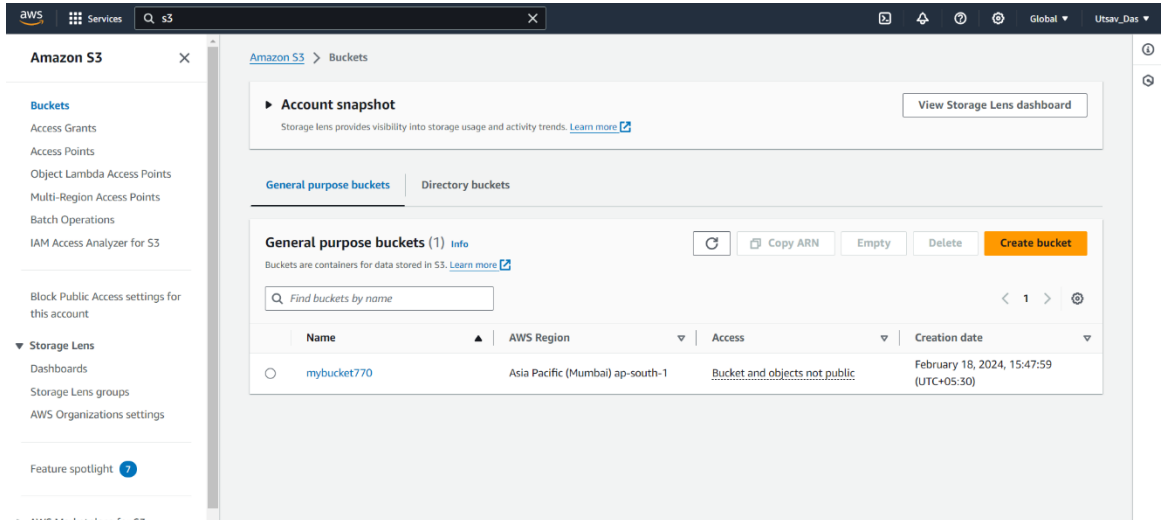


Assignment – 5

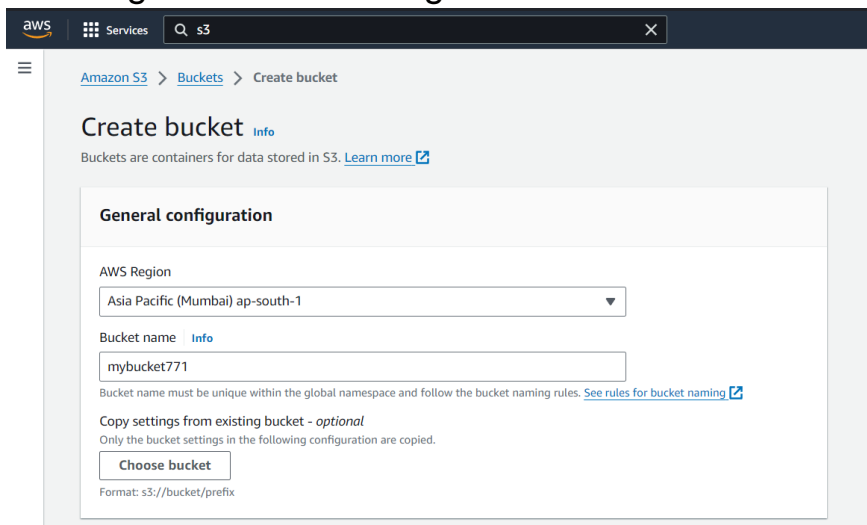
Problem Statement:

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

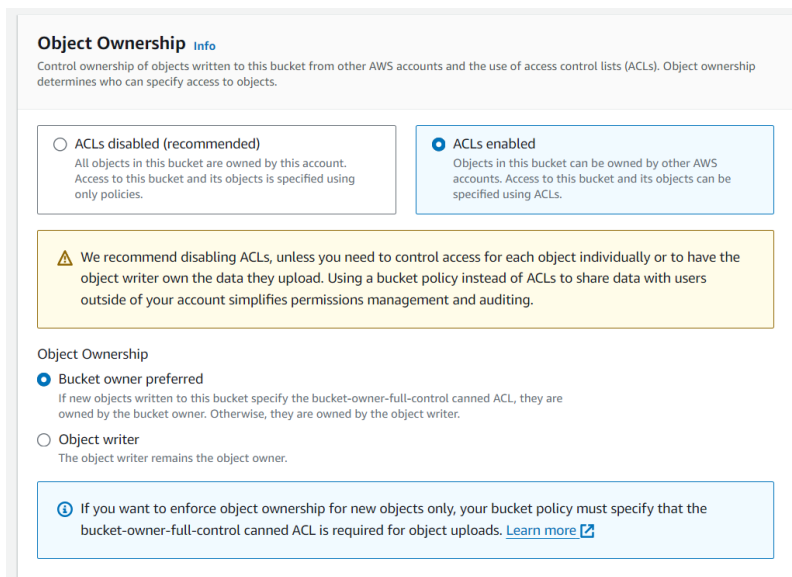
- 1) Click on S3 and click on Create bucket.



- 2) Give region Mumbai and give bucket name.



- 3) Click on ACLs enabled.



- 4) 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'.

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.

- 5) Click on Create 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.

[Cancel](#) [Create bucket](#)

- 6) Click on bucket name.

Successfully created bucket "mybucket772"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

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

[View Storage Lens dashboard](#)

General purpose buckets | Directory buckets

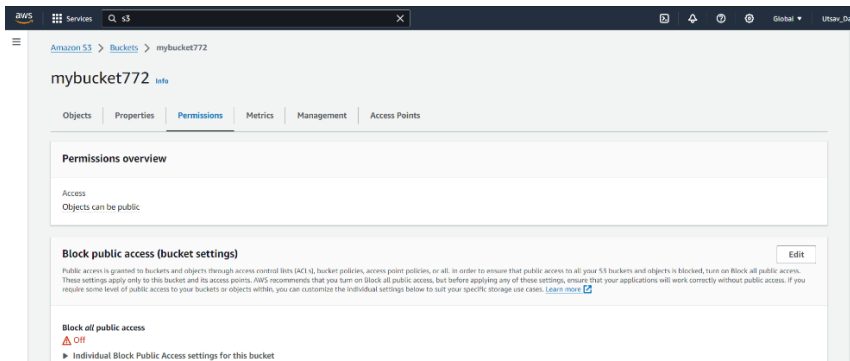
General purpose buckets (2) [Info](#)
Buckets are containers for data stored in S3. [Learn more](#)

[Find buckets by name](#)

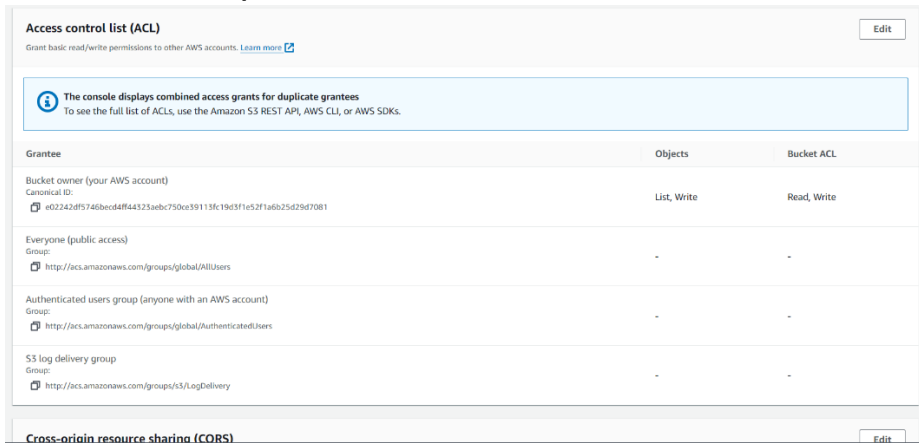
[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Name	AWS Region	Access	Creation date
<input type="radio"/> mybucket770	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 18, 2024, 15:47:59 (UTC+05:30)
<input type="radio"/> mybucket772	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 18, 2024, 16:28:00 (UTC+05:30)

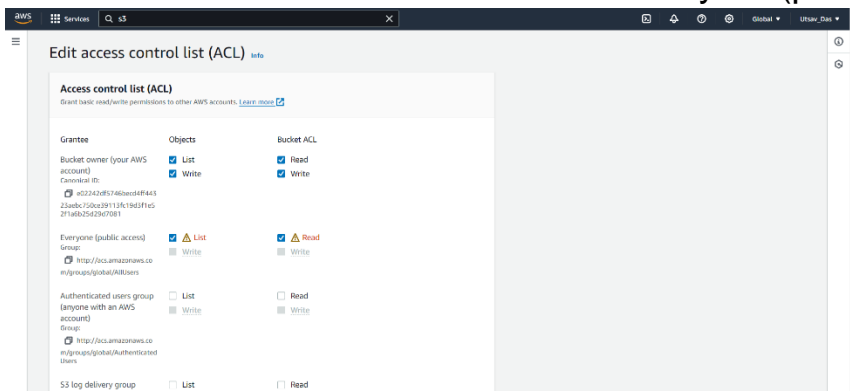
7) Click on Permission.



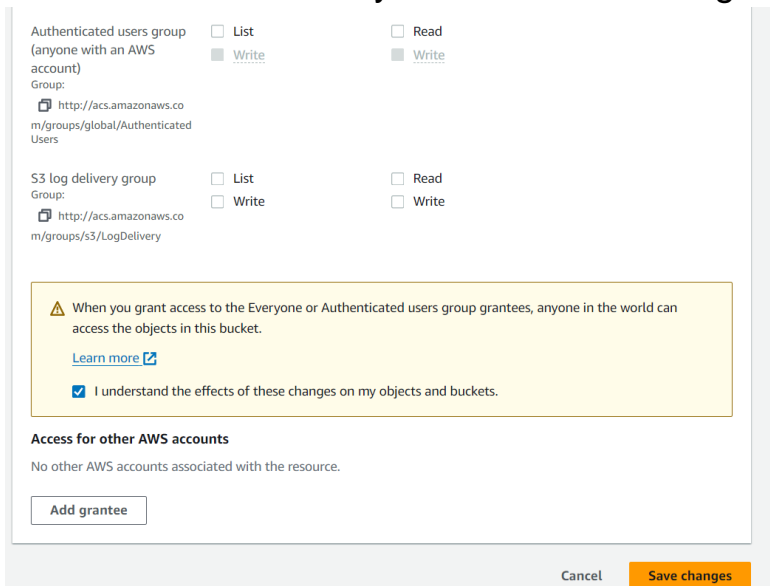
8) Click on edit option of ACLs



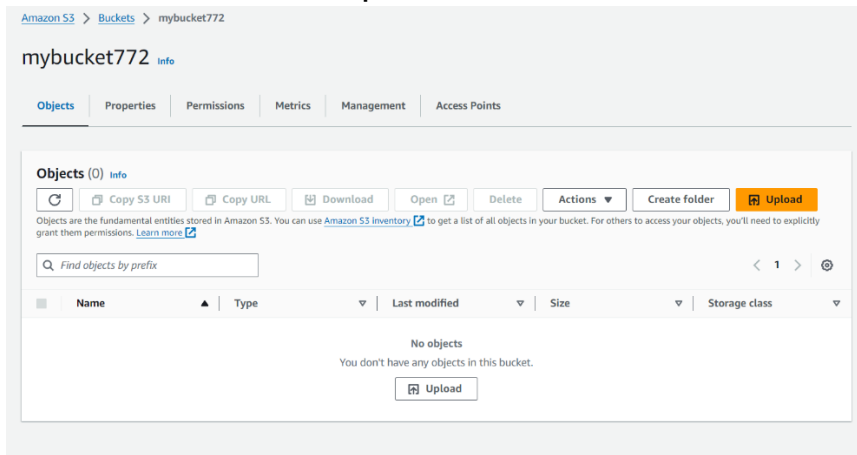
9) Click on check box of list and read in Everyone(public access).



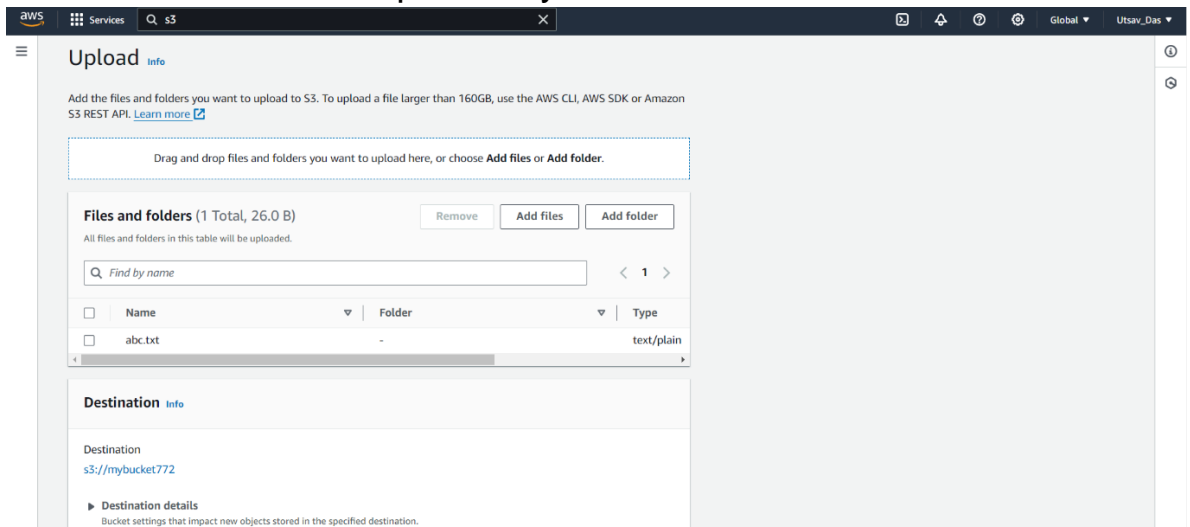
10) Click on check box 'I understand the effects of these changes on my objects and buckets' and finally click on Save changes.



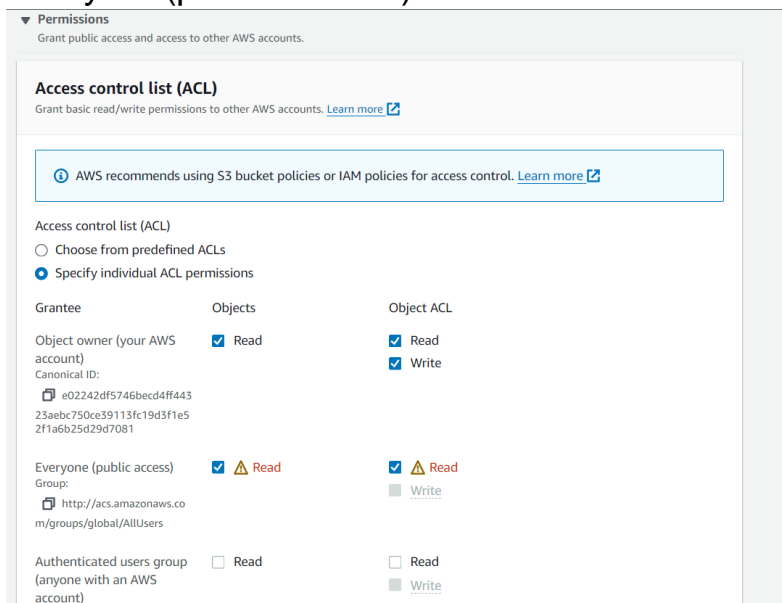
11) Go back to Buckets option and click on bucket name and click on Upload.



12) Click on Add files and upload any file.



13) After uploading click on Permission dropdown and click on check box 'Specify individual ACL permissions'. 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 option.

Authenticated users group (anyone with an AWS account)
Group: <http://acs.amazonaws.com/groups/global/AuthenticatedUsers>

☐ Read ☐ Read ☐ Write

Warning: When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the specified objects.
[Learn more](#)

☒ I understand the effects of these changes on the specified objects.

Access for other AWS accounts
No other AWS accounts associated with the resource.

[Add grantee](#)

Properties
Specify storage class, encryption settings, tags, and more.

[Cancel](#) [Upload](#)

15) After successful upload now go back to Bucket again. Click on bucket name and now click on file option checkbox. Then click on Copy URL option.

Amazon S3 > Buckets > mybucket772

mybucket772 [Info](#)

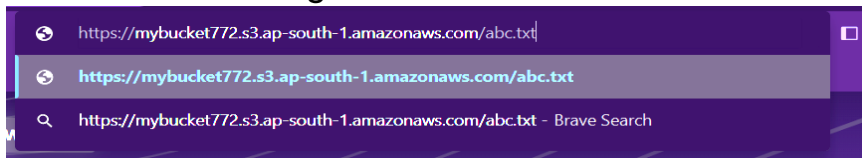
[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (1) [Info](#) [Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	abc.txt	txt	February 18, 2024, 16:51:50 (UTC+05:30)	26.0 B	Standard

16) Paste URL in incognito mode.



17) Anyone can access it now as it is public.