Assignment : 5
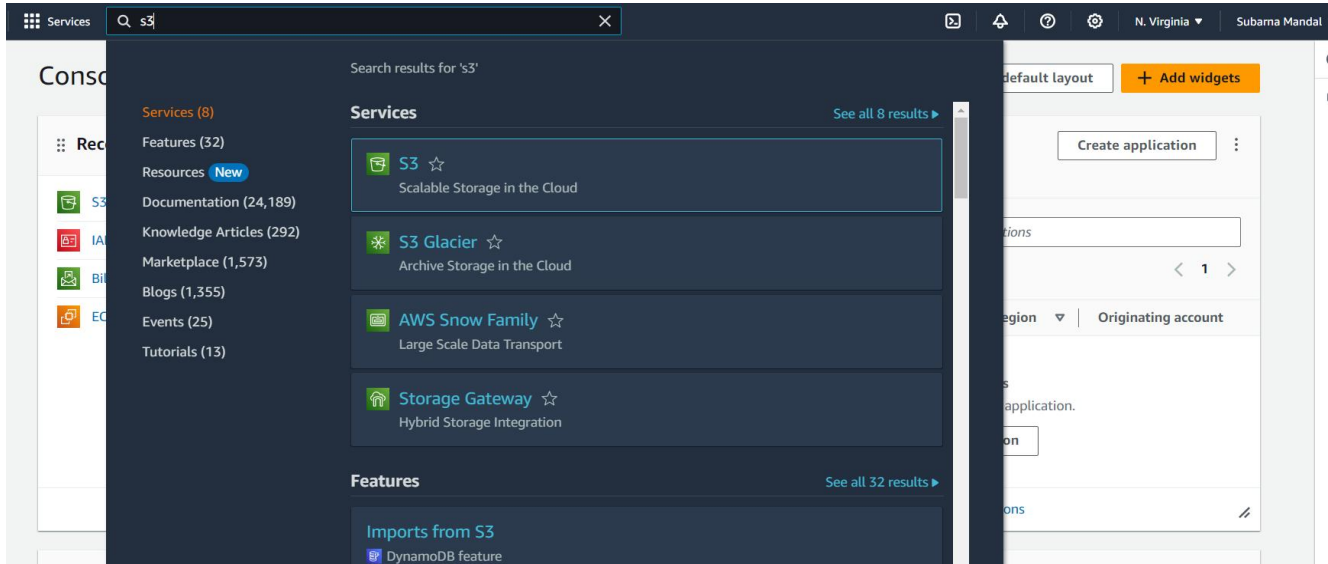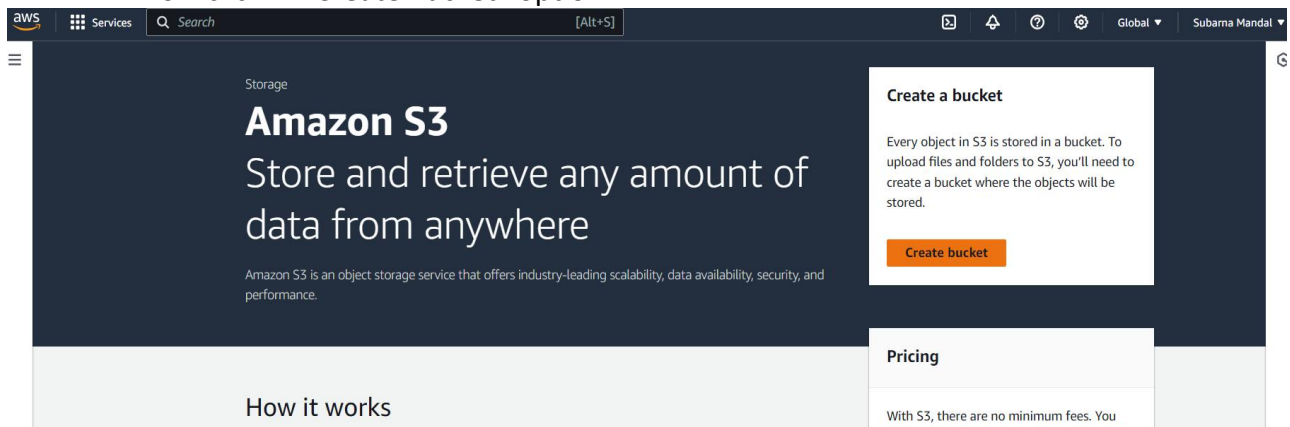
<u>Statement :</u> Create a public bucket in AWS.Upload a file and give the necessary permissions to check the file URL is working or not.(Public access) and check on I understand check box.

<u>Steps---</u>
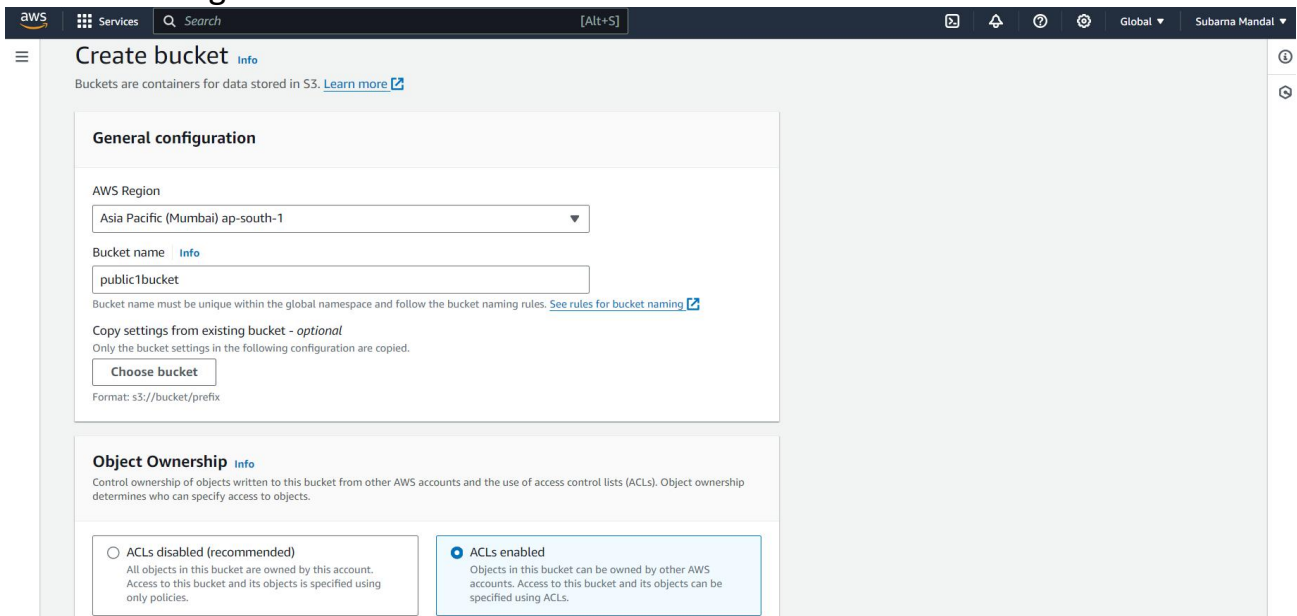
1. First sign in to your AWS account and search for "**S3**" (Simple Storage Services - where we will create the Bucket) in the search bar.

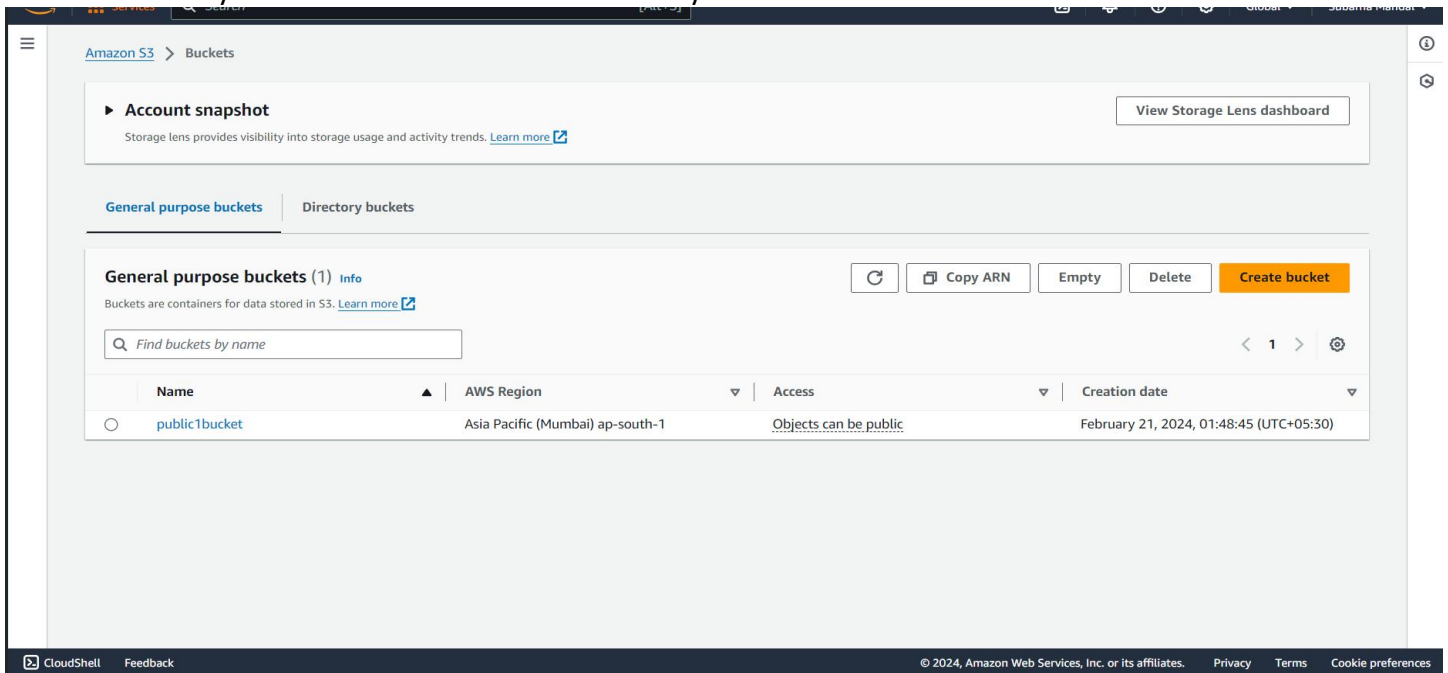2.Now click in "Create Bucket" option.
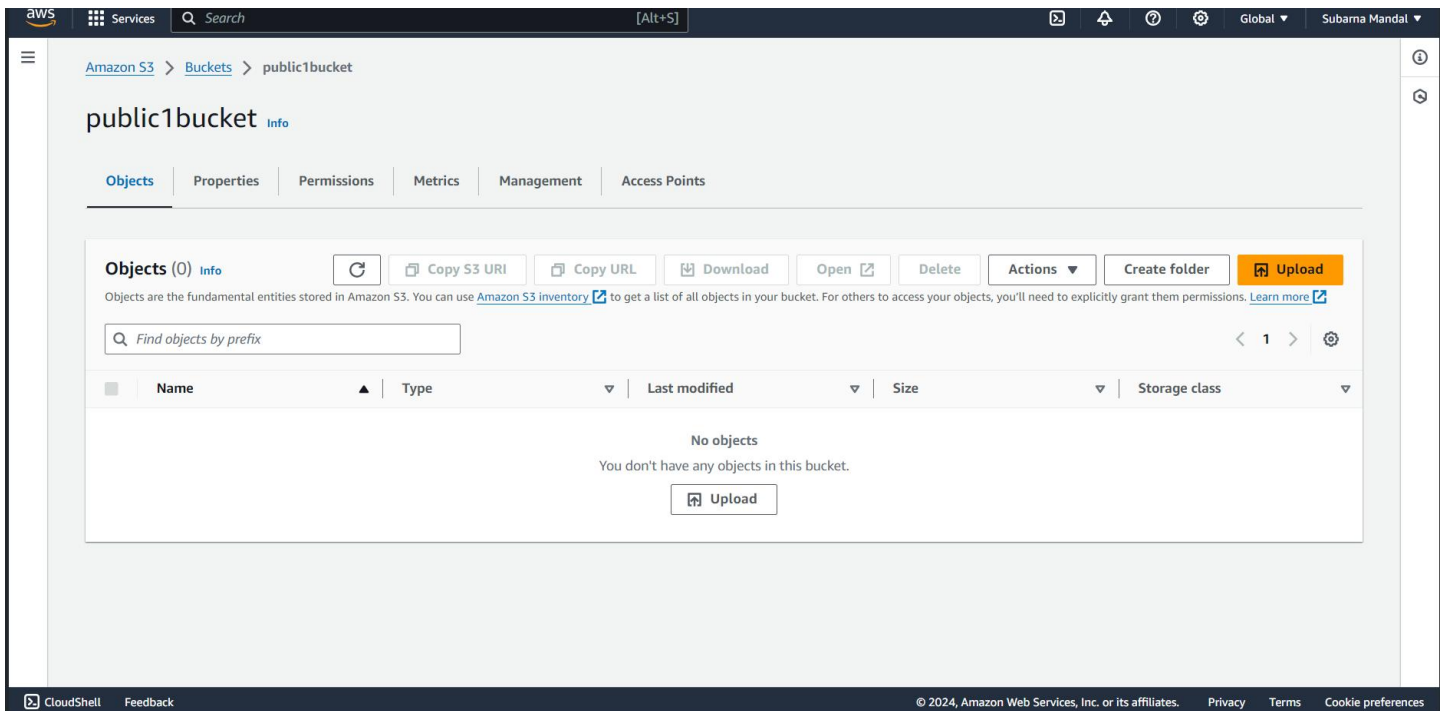

3.Now give the bucket name and click on ACL's Enable.

4.Uncheck block all public access.
5.check on Acknowledgement and click on create bucket.

Object Ownership

○ Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

ⓘ 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 ↗

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.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more ↗

Bucket Versioning
● Disable
○ Enable

Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more ↗

Add tag

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.
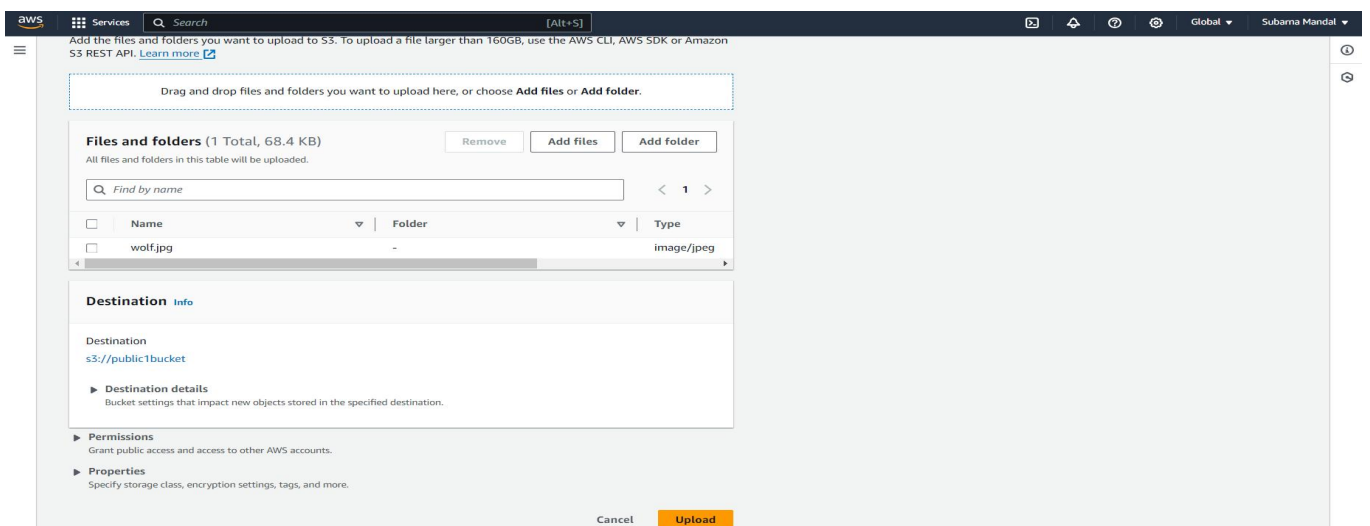
Cancel   **Create bucket**

6.you can see the bucket is successfully created. Next click on the <Bucket name>.

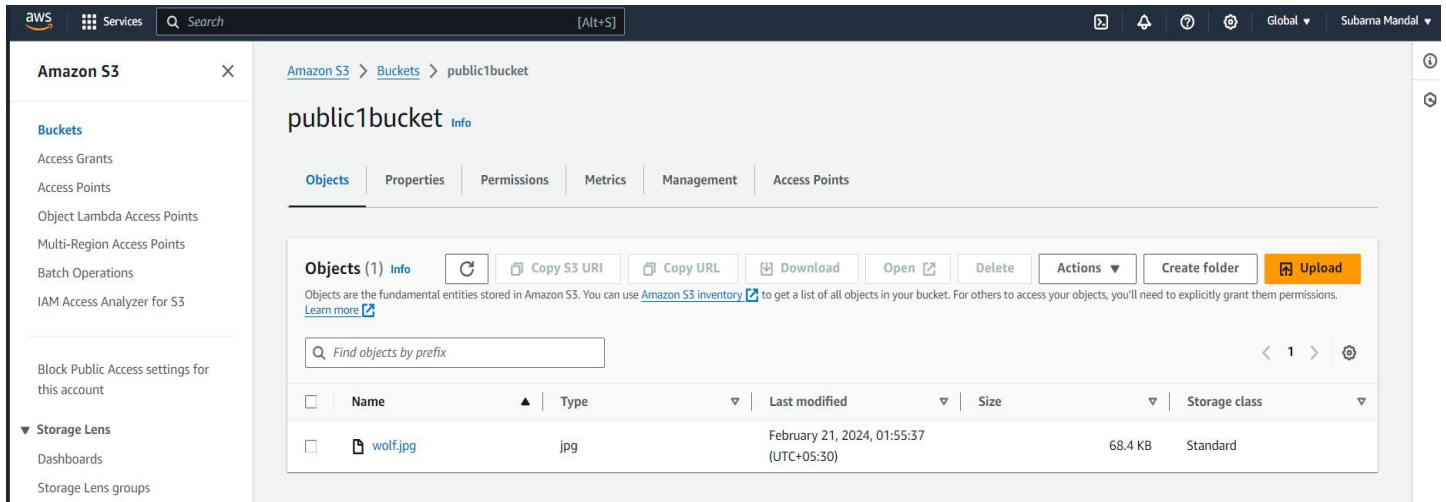

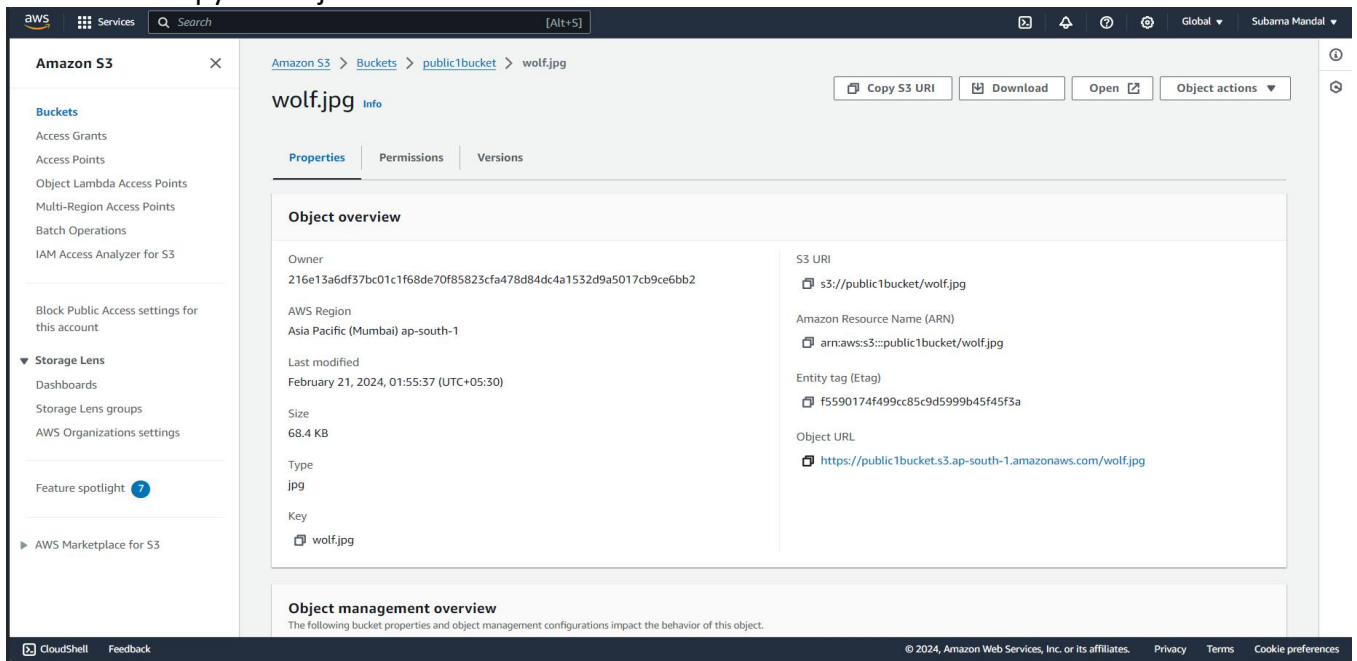7.Click on the "Upload" option.

8.Click "Add files" and upload a file.

9.File is uploaded. Now click on the <uploaded file name >
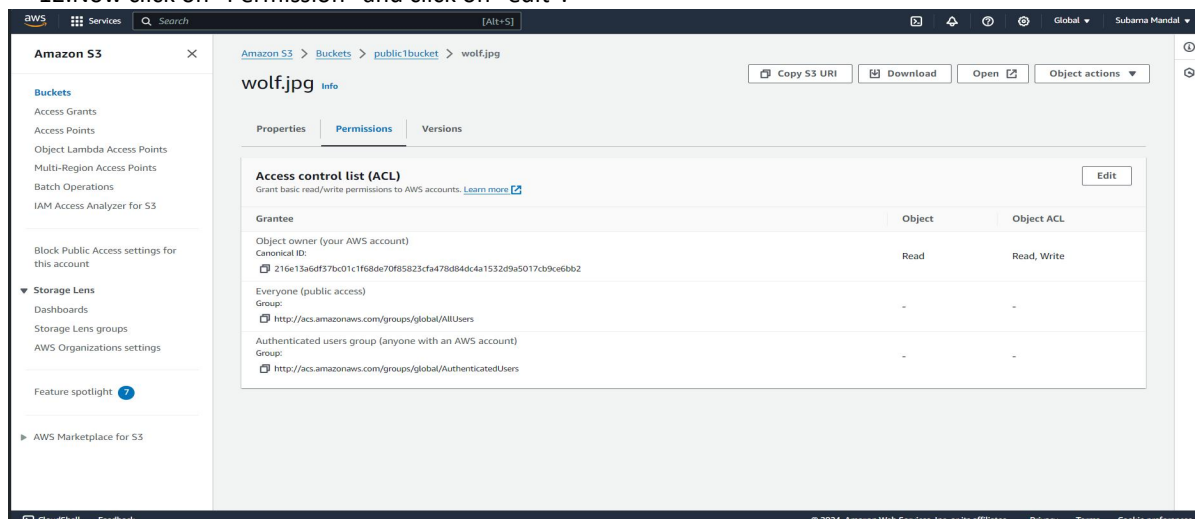

10.Copy the object URL from this .

11.Open the URL in another browser. It will show access denied.

12.Now click on "Permission" and click on "edit".

13.Now check two check boxes under Everyone (Public access) and check on I understand check box

14.Click on save changes.

15.Next copy the URL and paste it on an another browser.The file will be visiable for the given time.