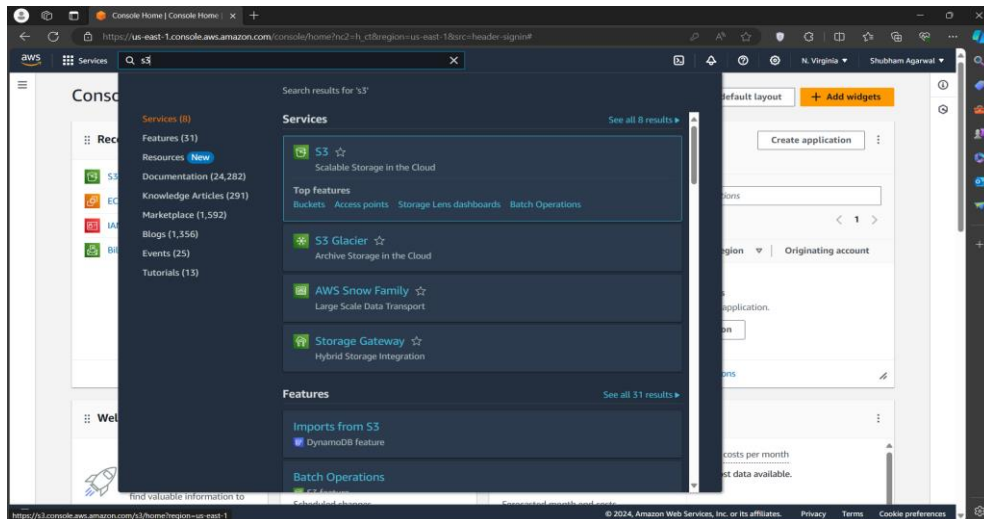


Assignment No: 4

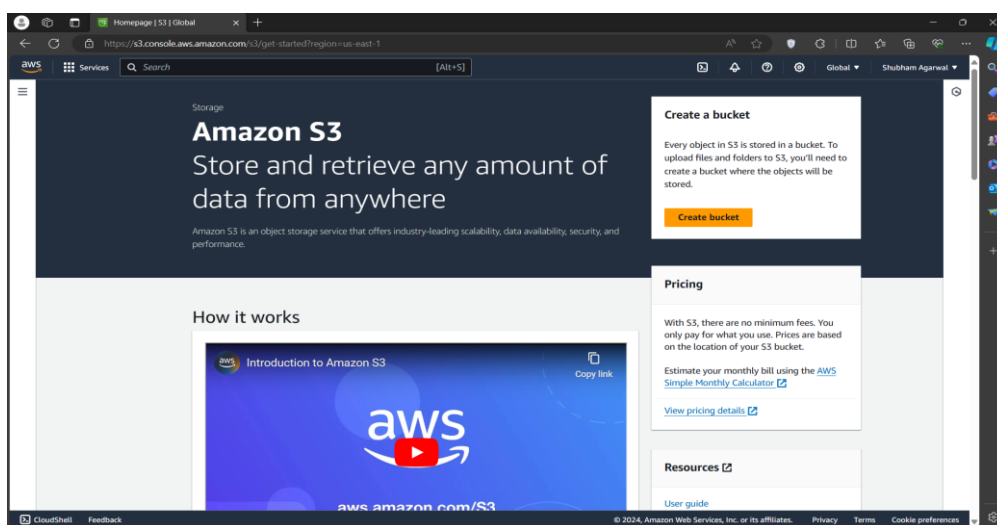
Problem Statement: Create a private bucket in AWS. Upload a file and check by reassigned URL whether you can access the file or not

The **steps are** as follows:-

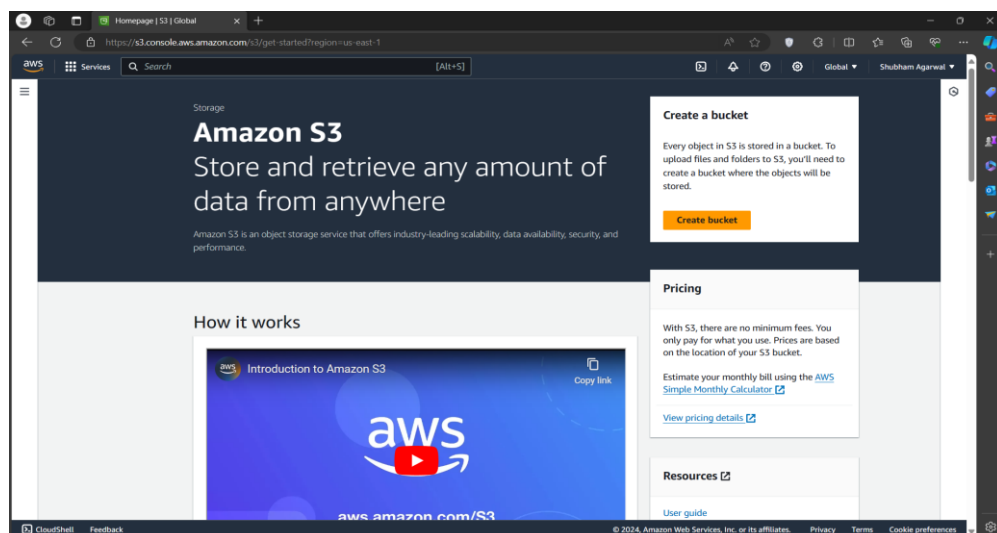
1. Access the **AWS console**, search for **S3**, and select the top option from the search results.



2. Click on 'Create bucket'.



3. The subsequent window appears.



4. From the drop-down menu, select 'Asia Pacific (Mumbai) ap-south-1' as the AWS Region. Next, specify a bucket name, such as- 'shubhambucket0'.

Create bucket [info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-1

Bucket name [info](#)
shubhambucket0
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.
[Choose bucket](#)
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.

5. By default, the Object Ownership is set to 'ACLs disabled' in this window. We will not make any adjustments as we are creating a **private bucket**.

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.
[Choose bucket](#)
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.

Object Ownership
Bucket owner enforced

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.

6. Similarly, we will leave the settings unchanged as the 'Block all public access' checkbox is already selected by default, aligning with our intention to create a **private bucket**.

Object Ownership
Bucket owner enforced

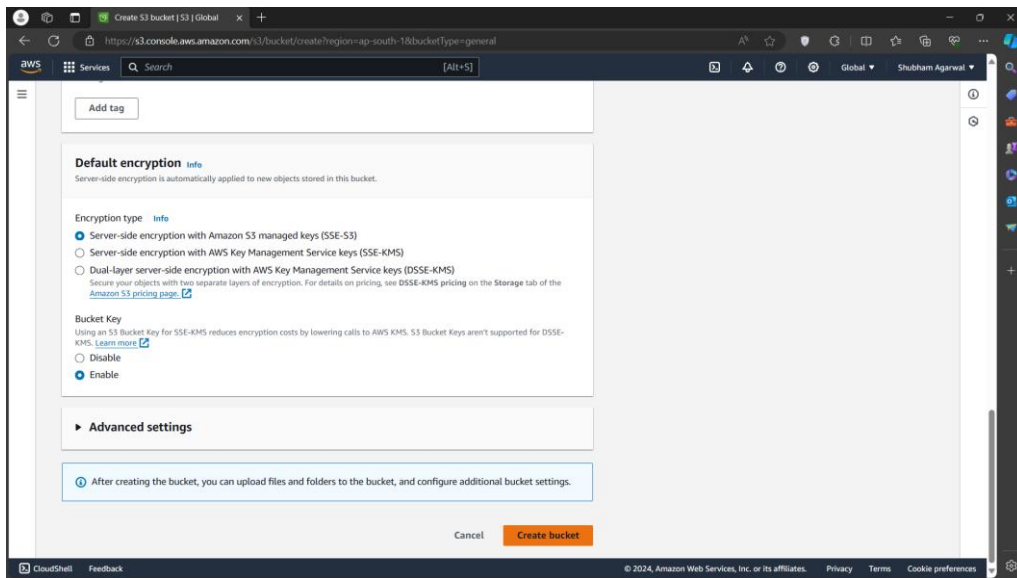
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings 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.

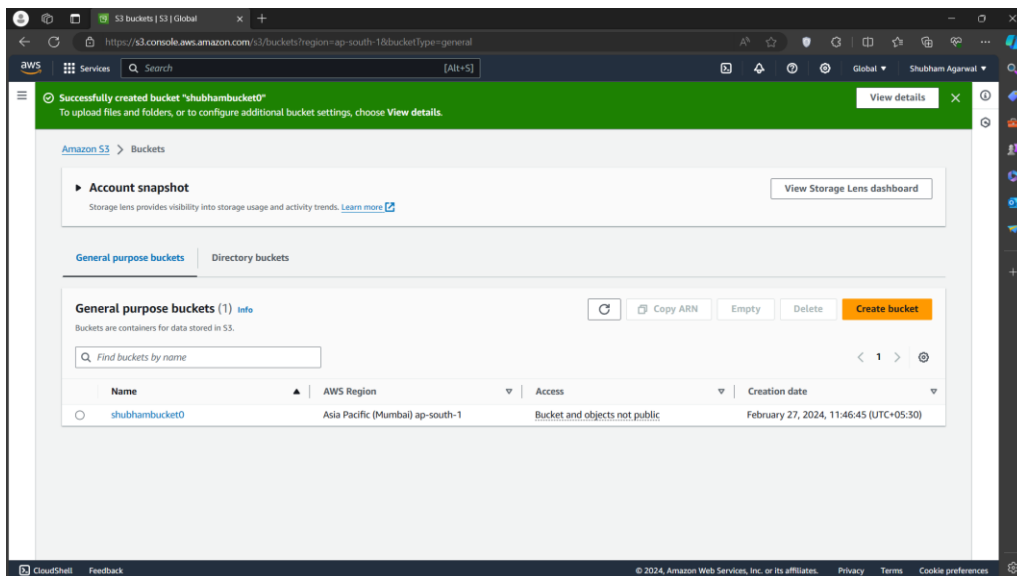
- ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing 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.

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 previous versions of an object stored in the same bucket. It also lets you restore deleted versions of objects stored in the same bucket. For more information, see [Amazon S3 Versioning](#).

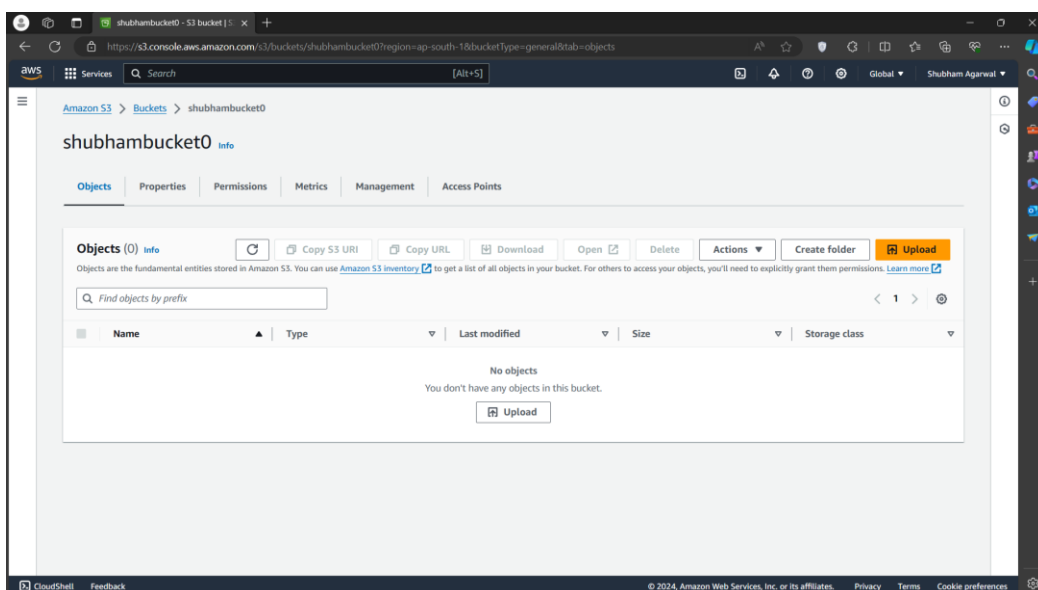
7. Now, without making any additional modifications, scroll down and proceed to click on 'Create Bucket'.



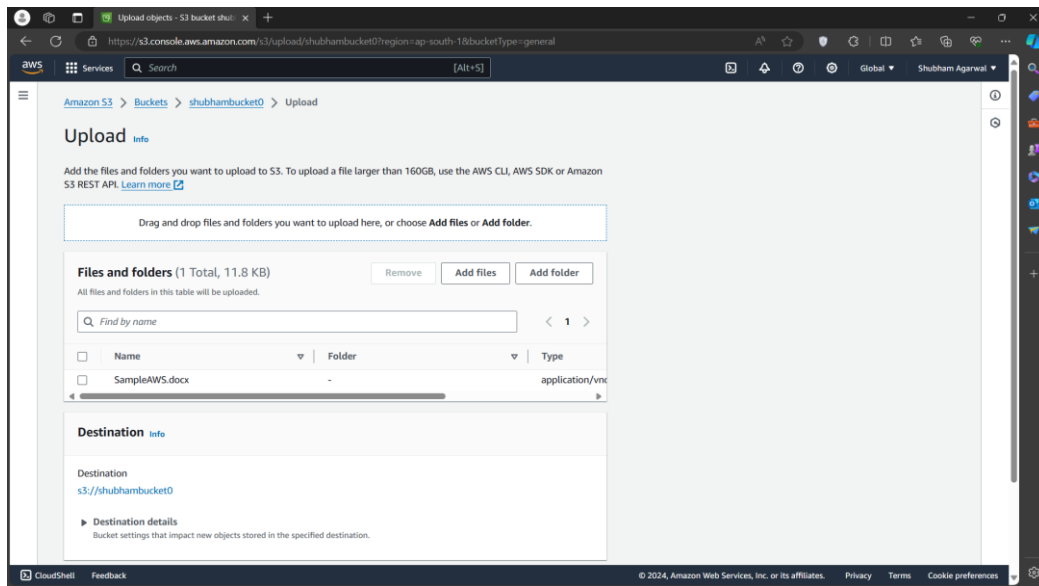
8. It's evident that the bucket has been successfully created.



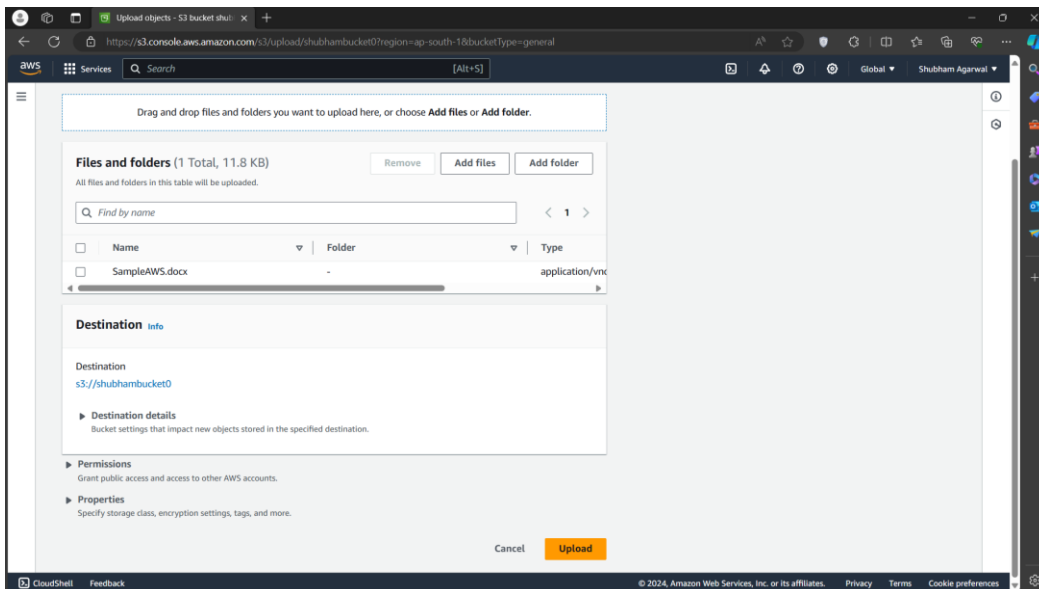
9. Now click on the bucket name.



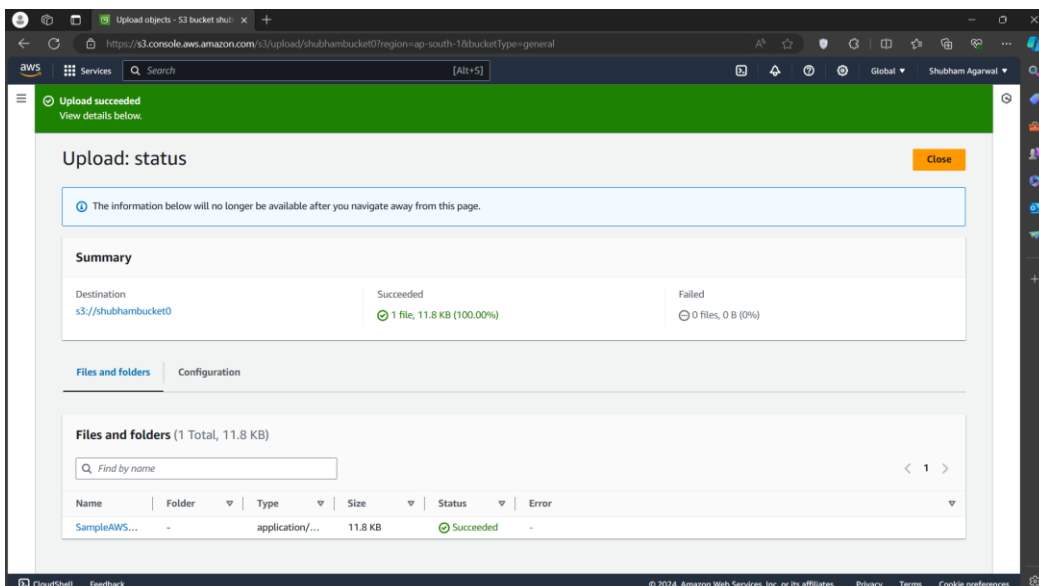
10. Choose the **Upload** option, which will lead to the opening of the subsequent window. From there, click on **Add files** and proceed to upload your desired file into the selected bucket (in this case, SampleAWS.docx).



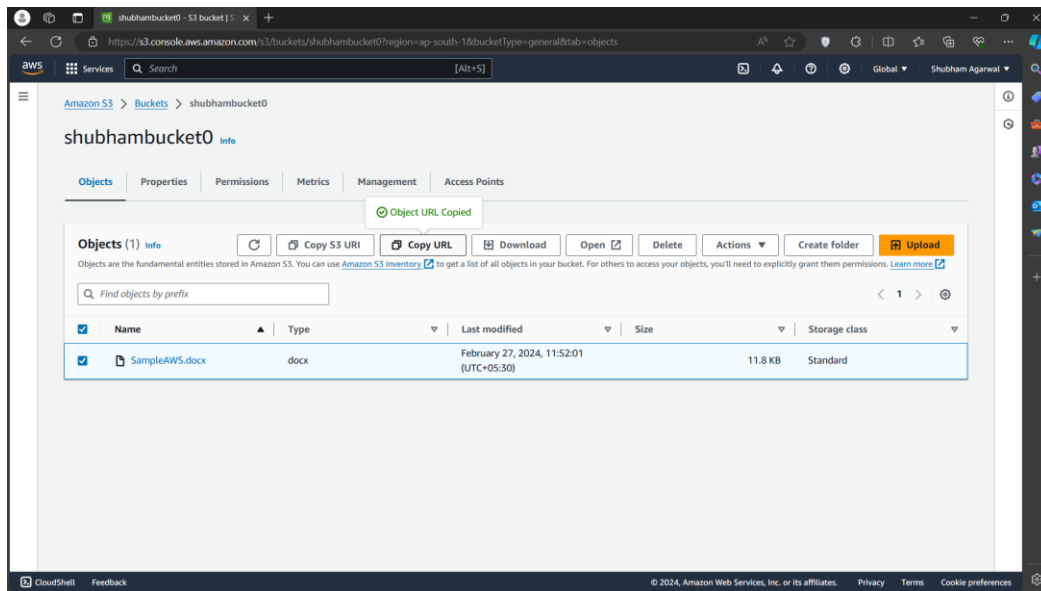
11. Scroll down and proceed to click on 'Upload'.



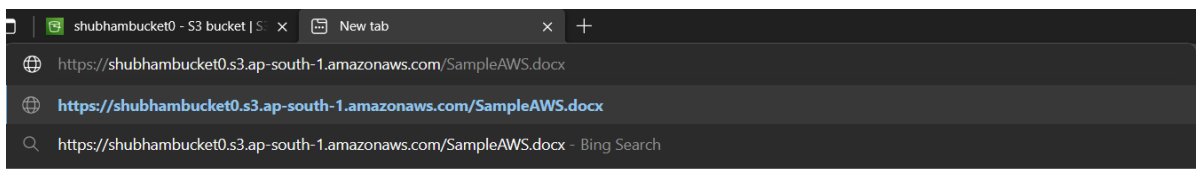
12. The notification confirms that the file has been successfully uploaded. Click on 'Close' to return.



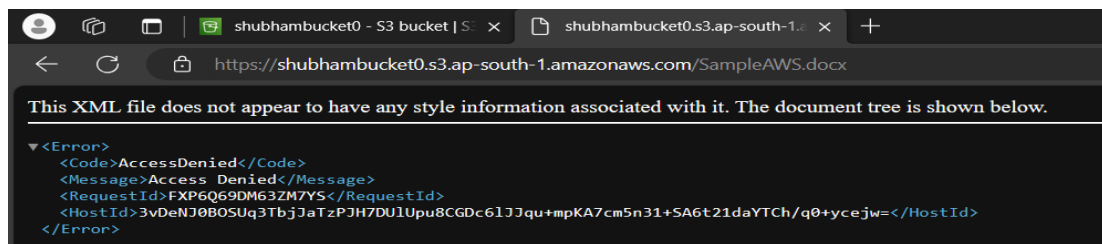
13. Now, select the checkbox next to the uploaded file, then click on 'Copy URL'.



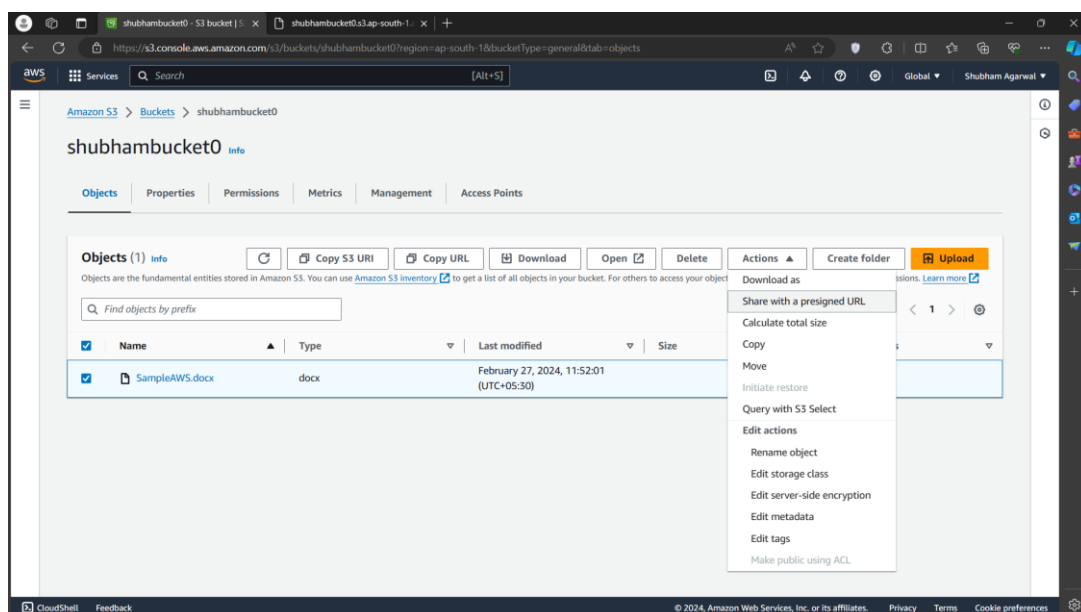
14. Navigate to a new window, paste the URL, and proceed with the search.



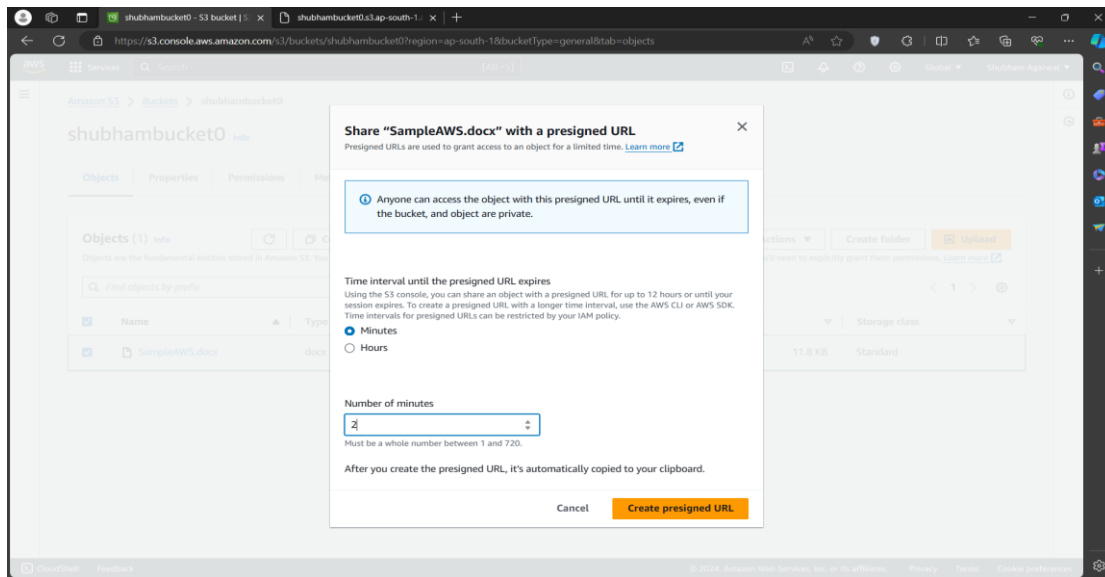
15. An error appears indicating that access to the contents is restricted since this is a private bucket.



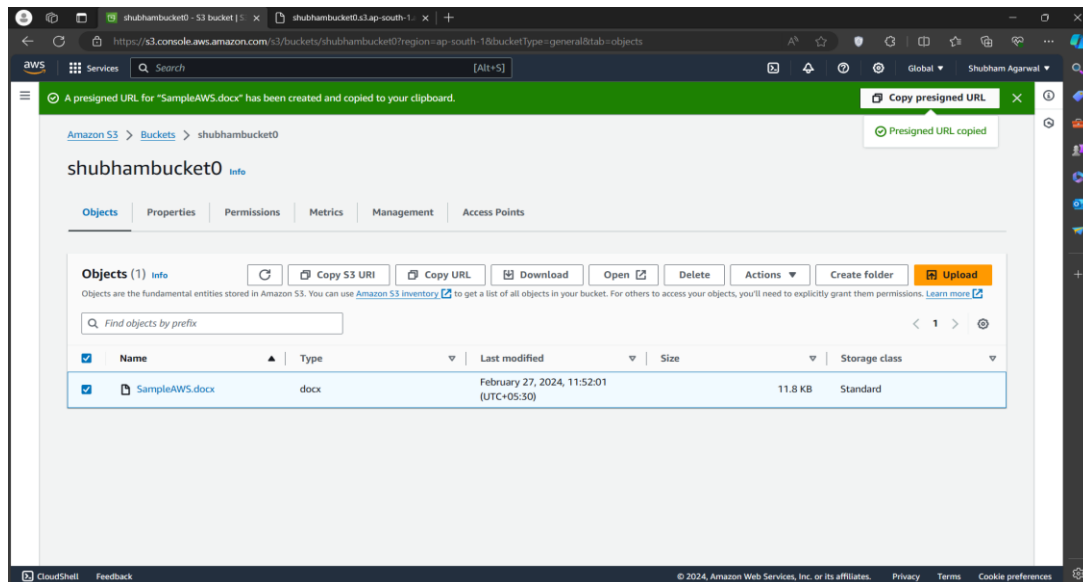
16. Close the current window, then navigate to 'Actions' and choose 'Share with a presigned URL'.



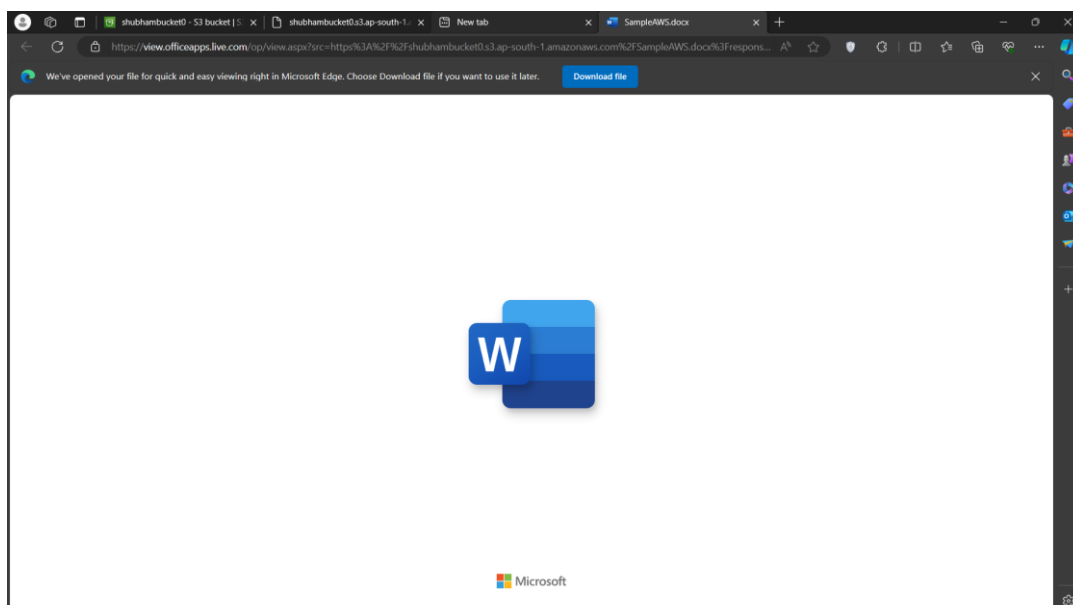
17. Select the desired duration until you want the presigned URL to expire, and click on 'Create presigned URL'.



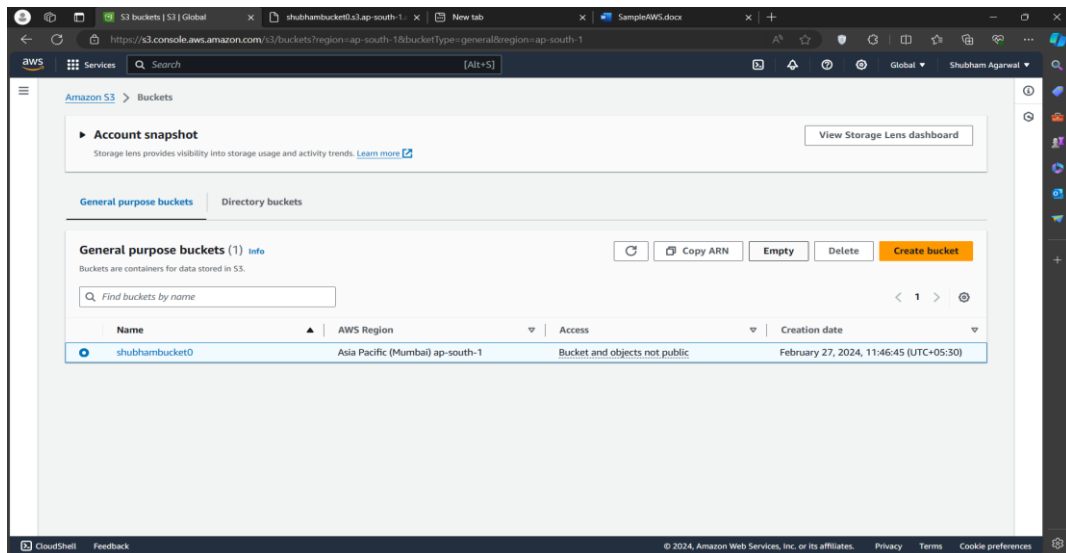
18. Copy the presigned URL.



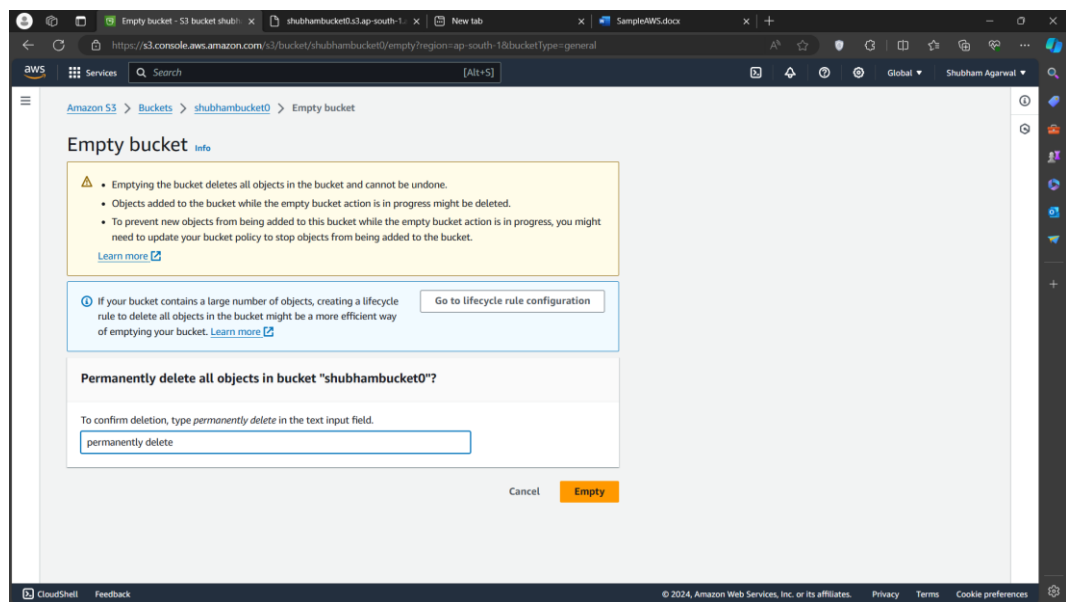
19. Open a new window and paste the URL. Now, you can view the uploaded file.



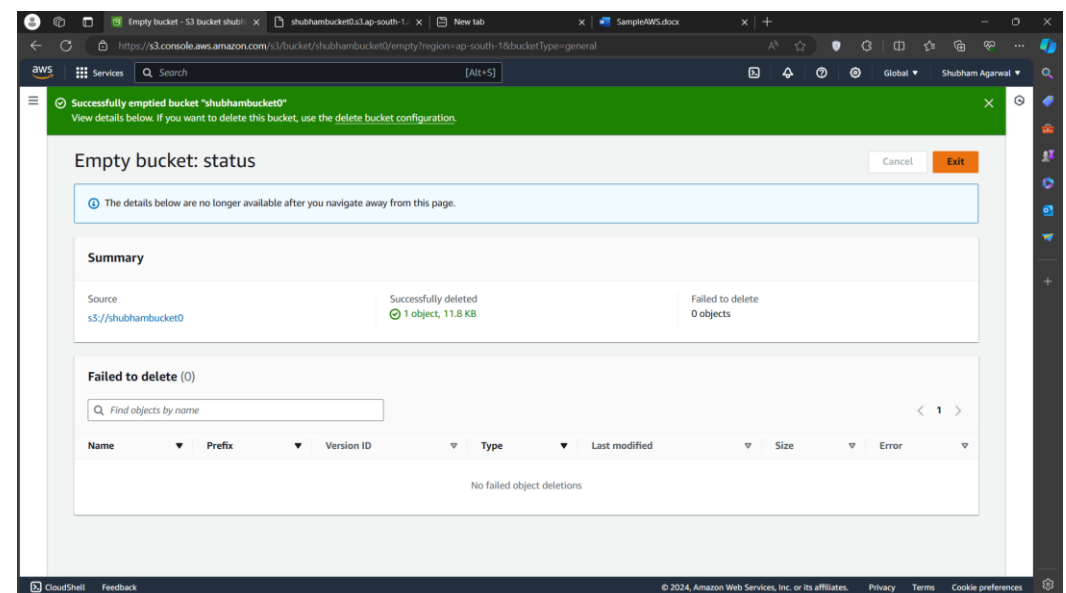
20. To delete the bucket, it must first be emptied. Therefore, close this window and return to your list of buckets. Select the desired bucket and proceed to click on 'Empty'.



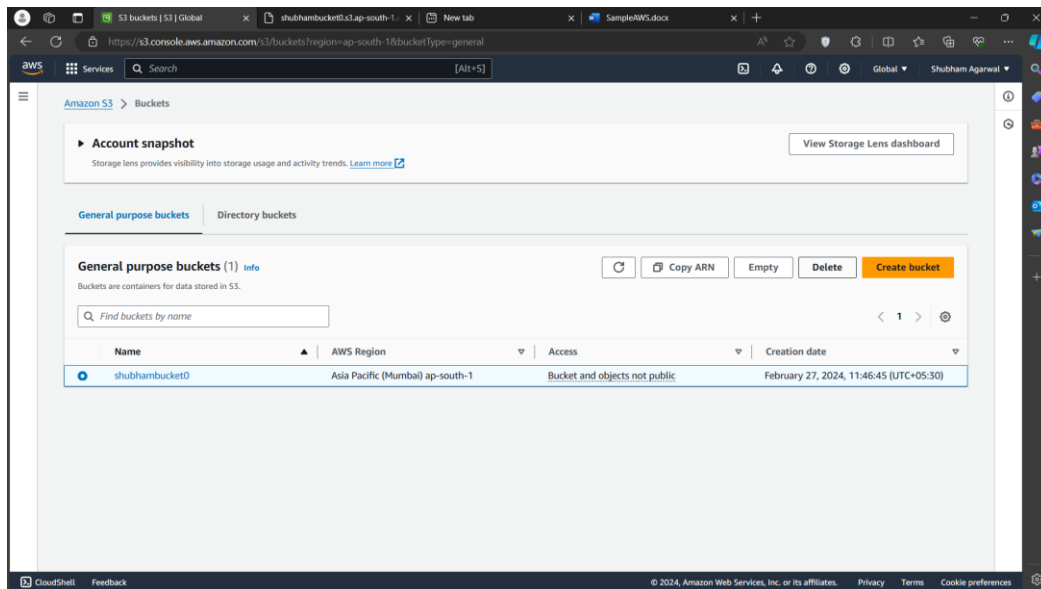
21. To confirm the action, input 'permanently delete' and then click on 'Empty'.



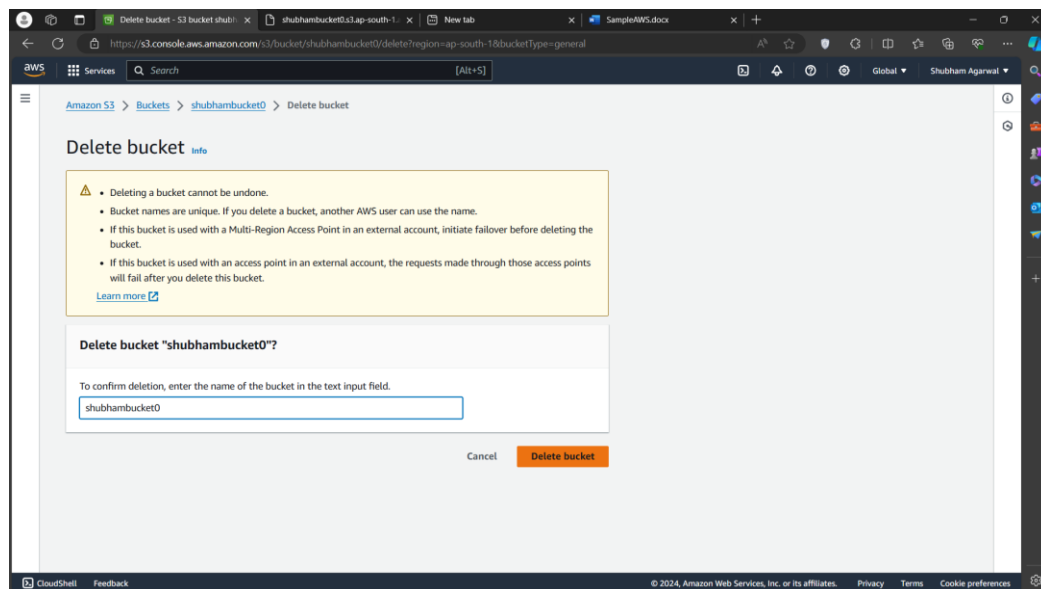
22. Once the action has been successfully completed, click on 'Exit'.



23. Now, again select your bucket and choose 'Delete'.



24. To confirm the deletion, enter your bucket name. Then, click on 'Delete bucket'.



25. The deletion has been successfully completed.

