

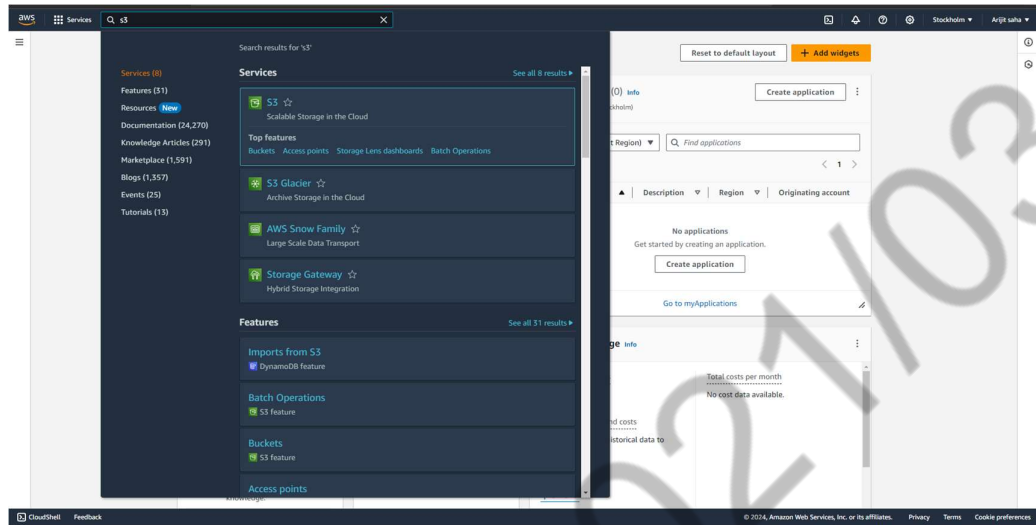
Assignment: 5

Problem statement:

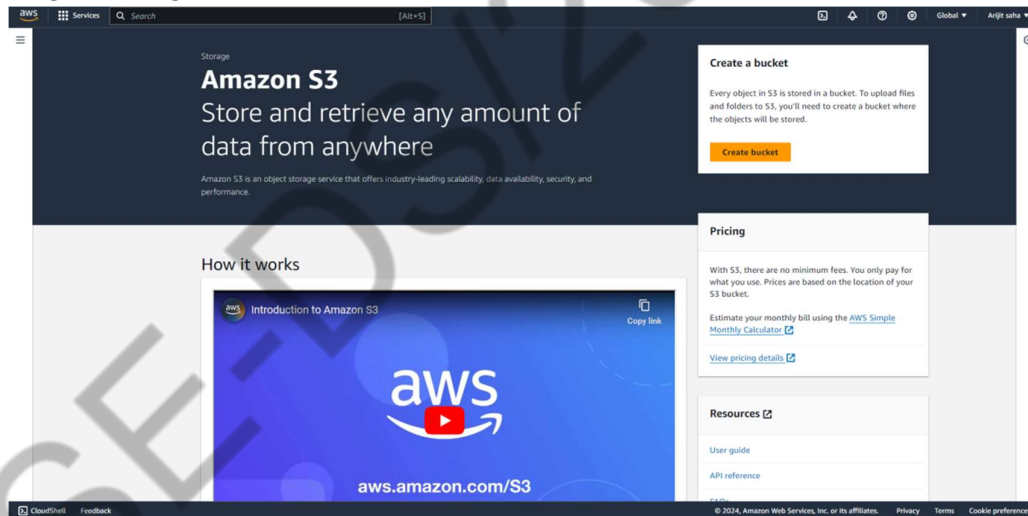
Create a public bucket in AWS. Upload a file and check by reassigned URL whether you can access the file or not.

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'.



3. 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'.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name [Info](#)

mainak-public-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.

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 created 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

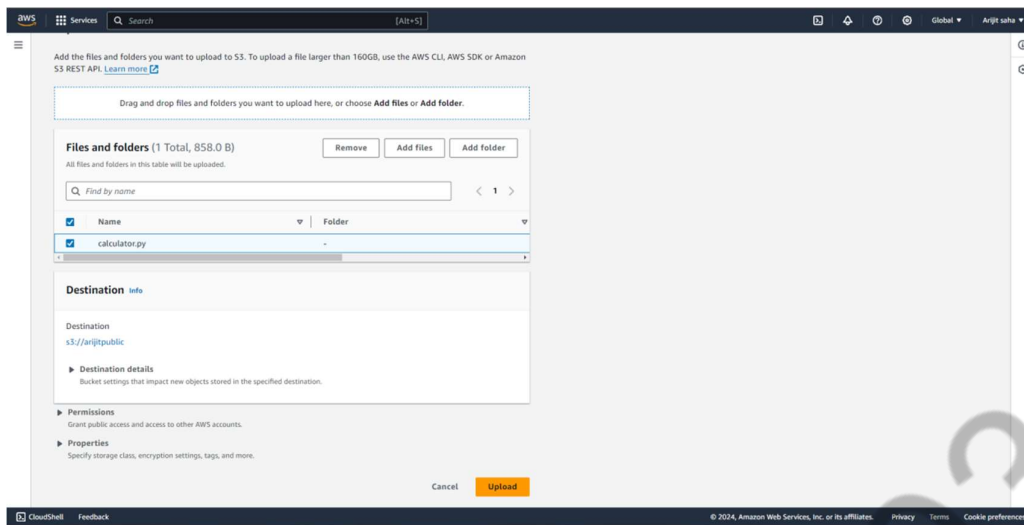
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.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

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

4. 'mainak-public-packet' bucket is created successfully then click on the bucket name 'mainak-public-packet'.

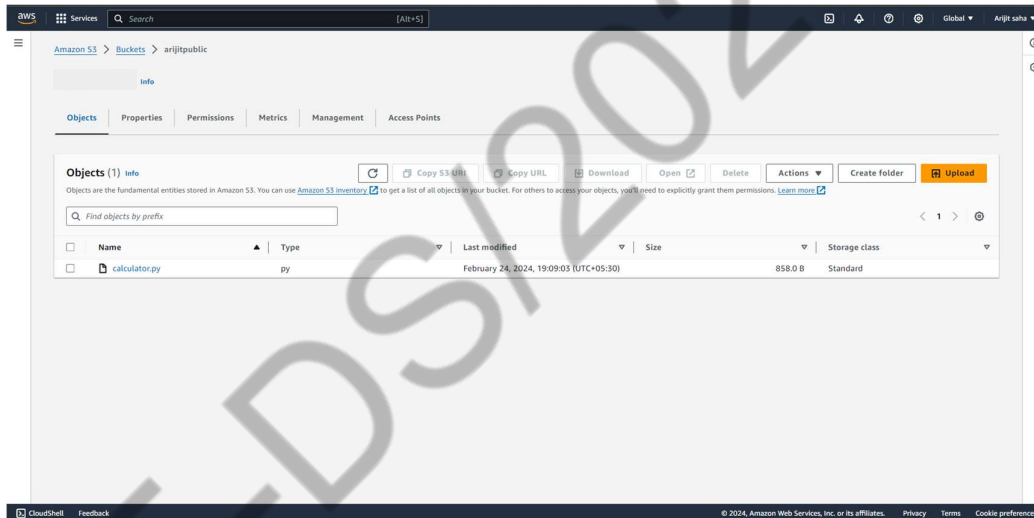
5. Under 'mainak-public-packet', click on 'Upload' then choose a file of your choice and upload it.



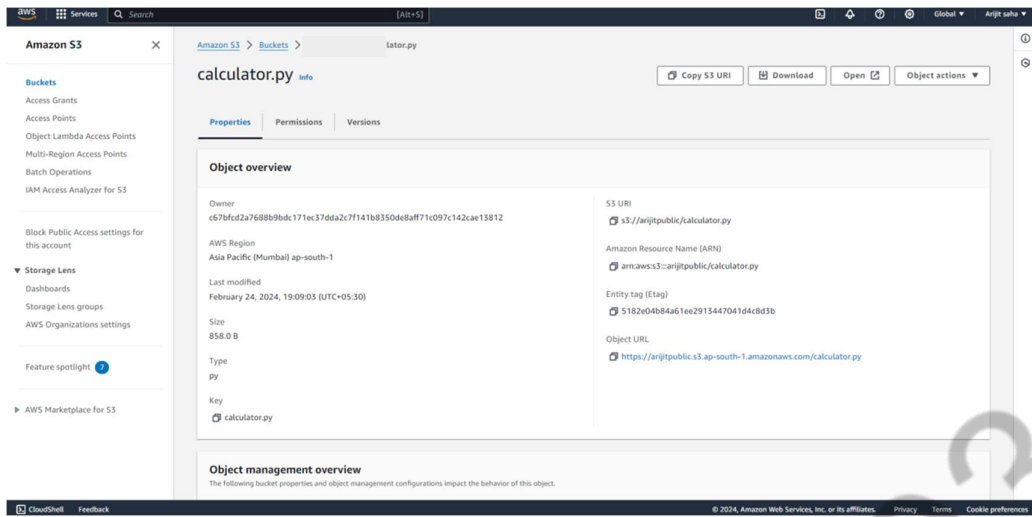
6. Click on 'Add files' then tick off the 'Name' of the file and click on 'Upload'.

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

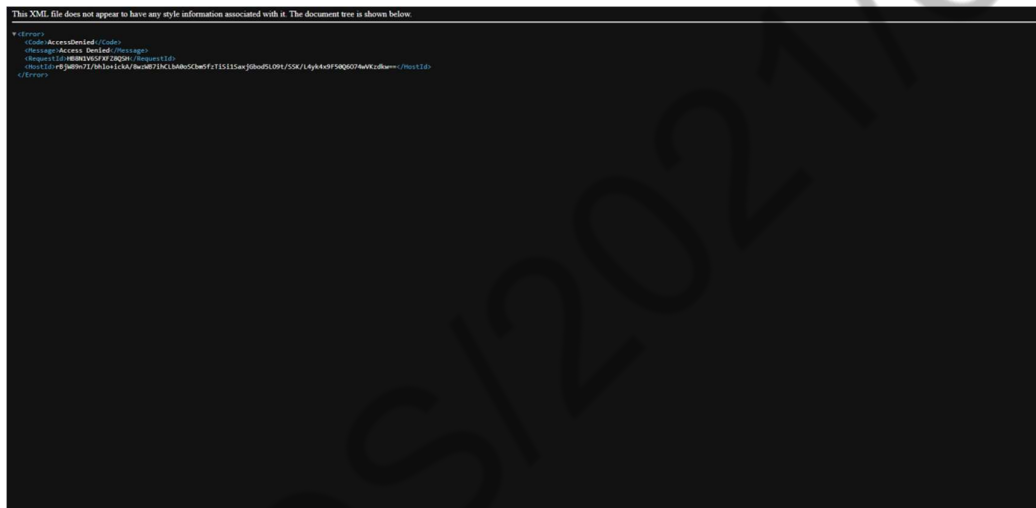
8. Under 'mainak-public-packet', tick off any one of the file(checkbox) and click on the file.



9. Copy the 'Object URL'.

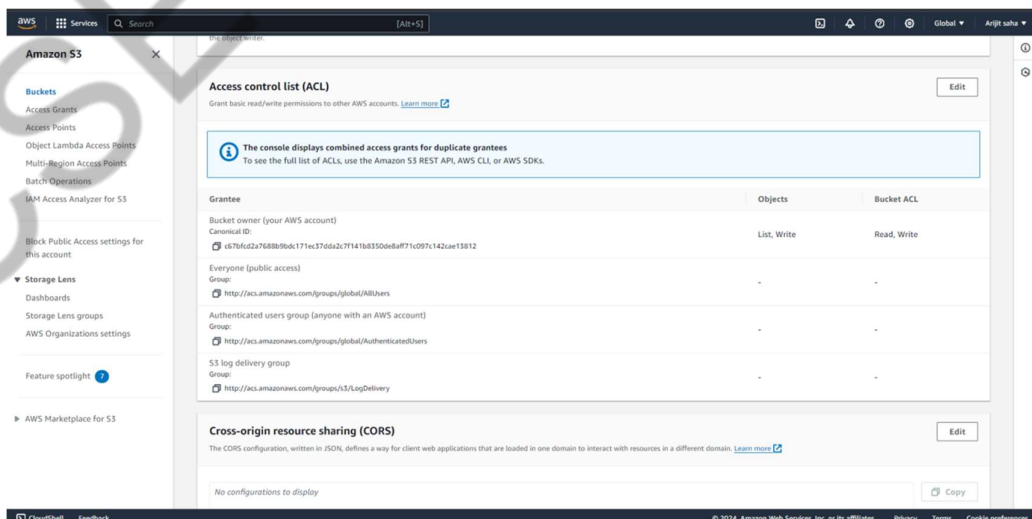


10. Now open the 'Incognito mode' and paste the 'Object URL'. You will see that the file cannot be accessed.

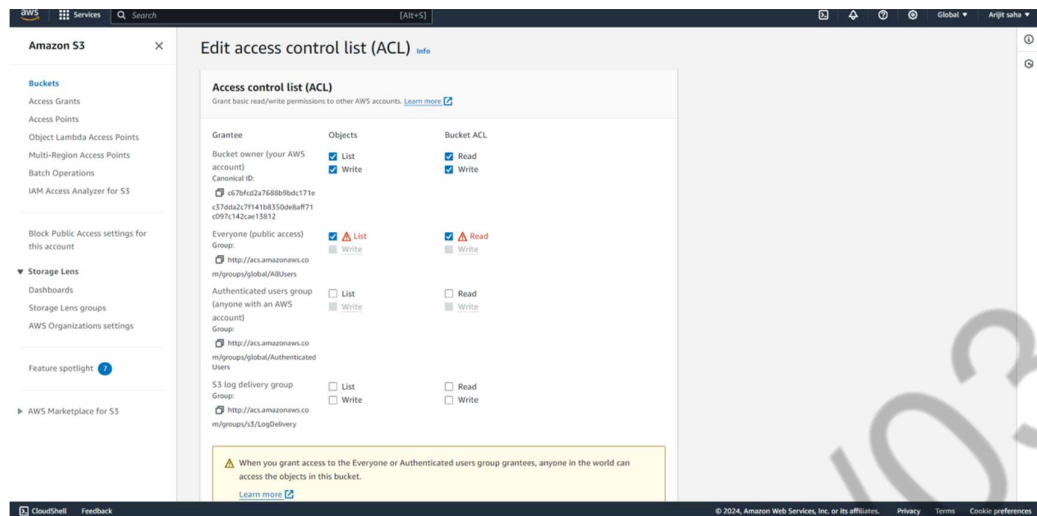


To give access to the file, follow the steps given below.

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.

