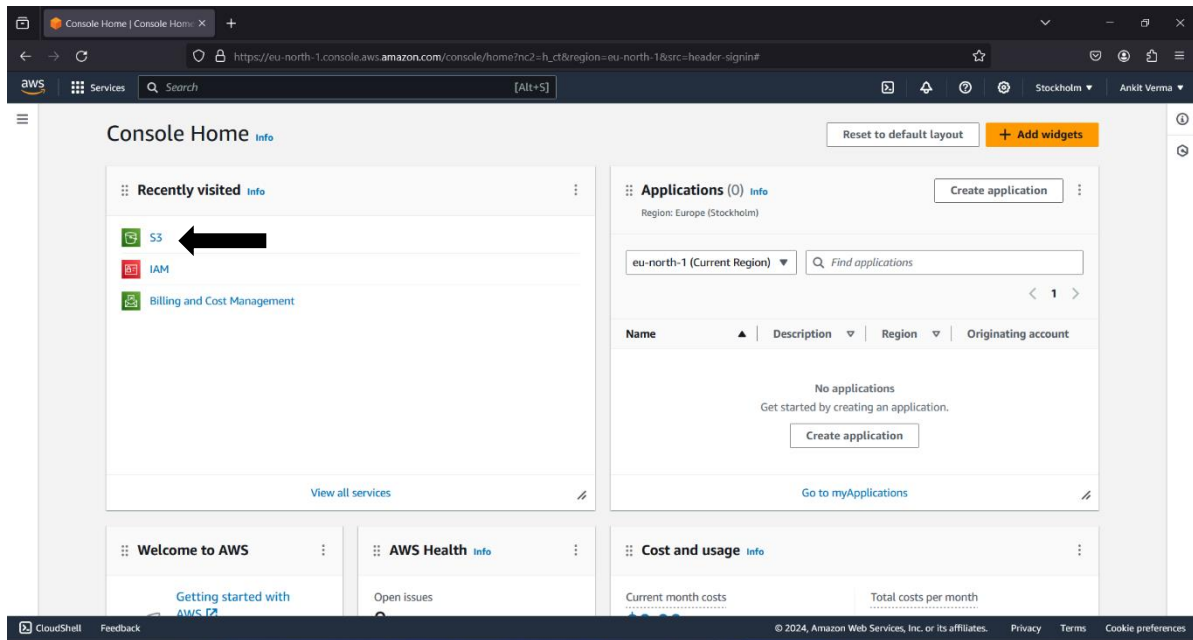


Assignment: 5

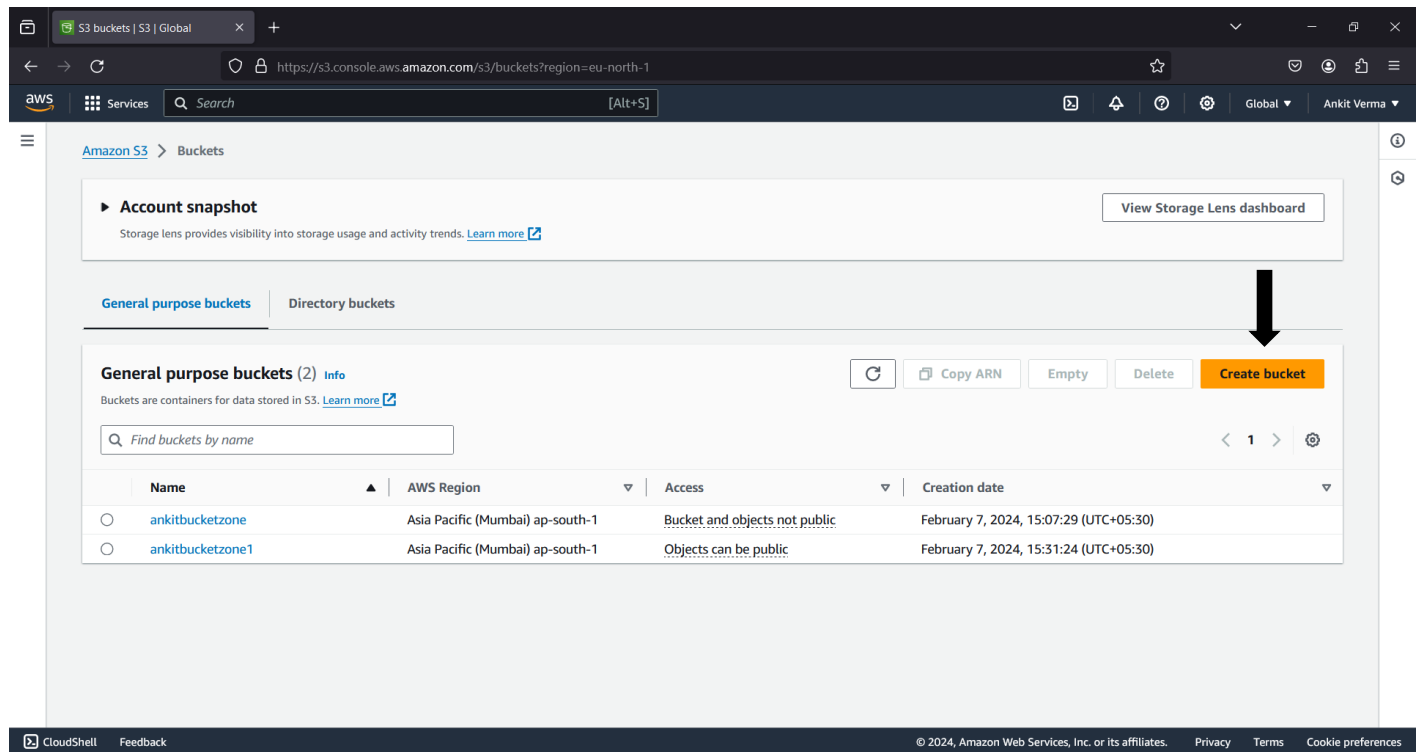
Problem Statement: Create a Public Bucket. Upload a file and give the necessary permissions to check whether the file URL is working

» The steps to create private bucket:-

Step 1: Click on the “S3” button.



Step 2: Click on “Create Bucket”.



Step 3: Select “Mumbai”, give a Name to the Bucket. Select “ACLs enabled”.

Upload objects - S3 bucket aws x Upload objects - S3 bucket aws x Create S3 bucket | S3 | Global x +

https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general

Create bucket [Info](#)

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

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name [Info](#)

awsbucket1

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.

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 4: Click “Block all public access” & tick the “I acknowledge” checkbox.

Upload objects - S3 bucket aws x Create S3 bucket | S3 | Global x harry-potter.jpg (JPEG Image, 500 x +

https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general

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

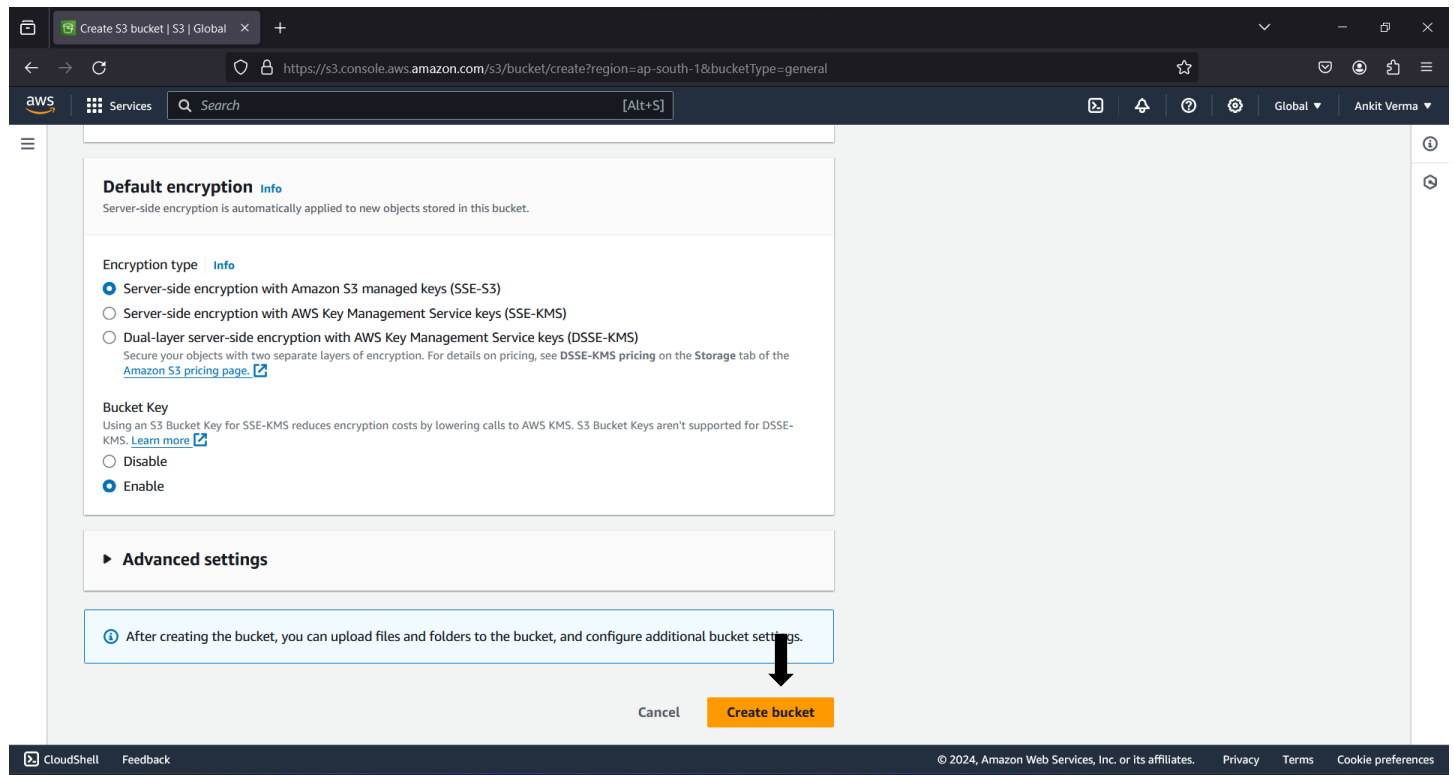
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

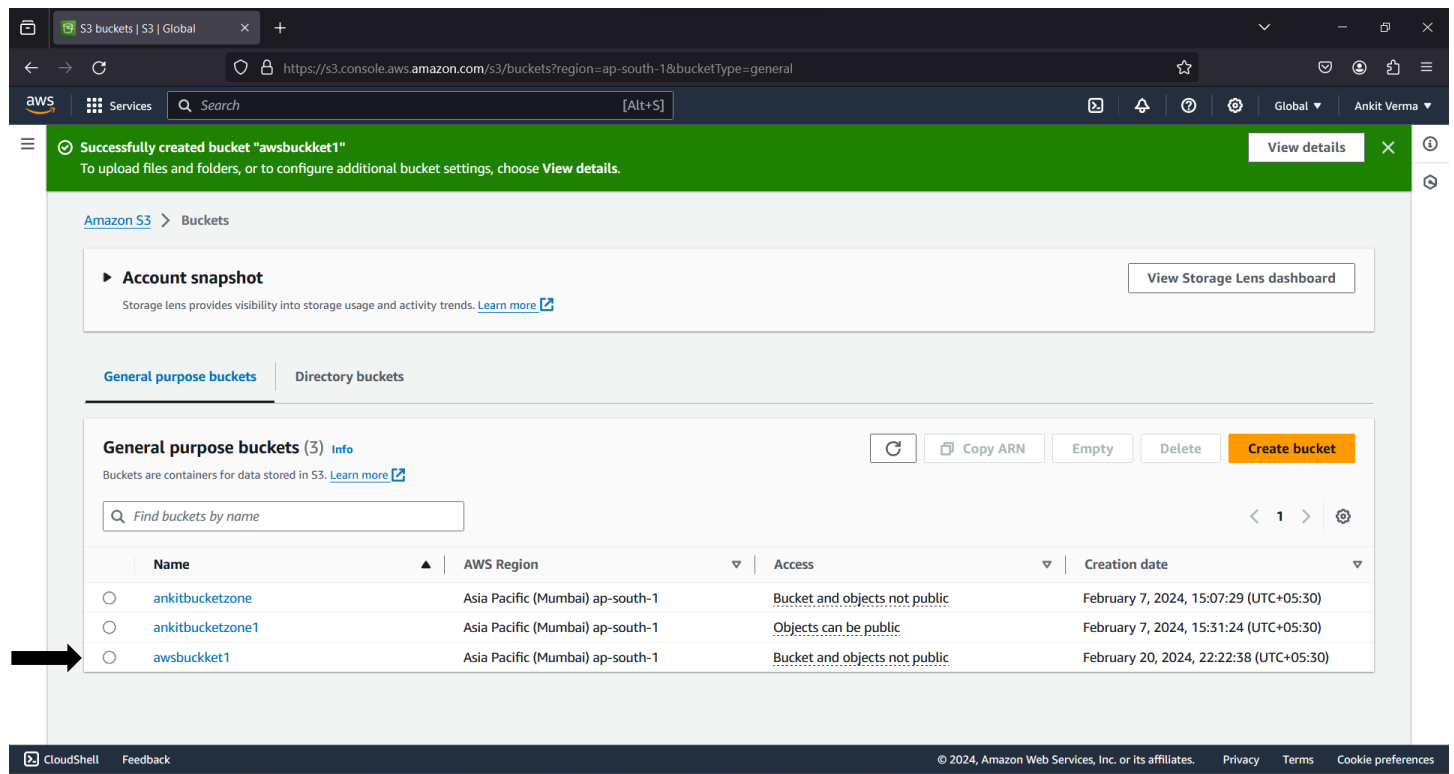
CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

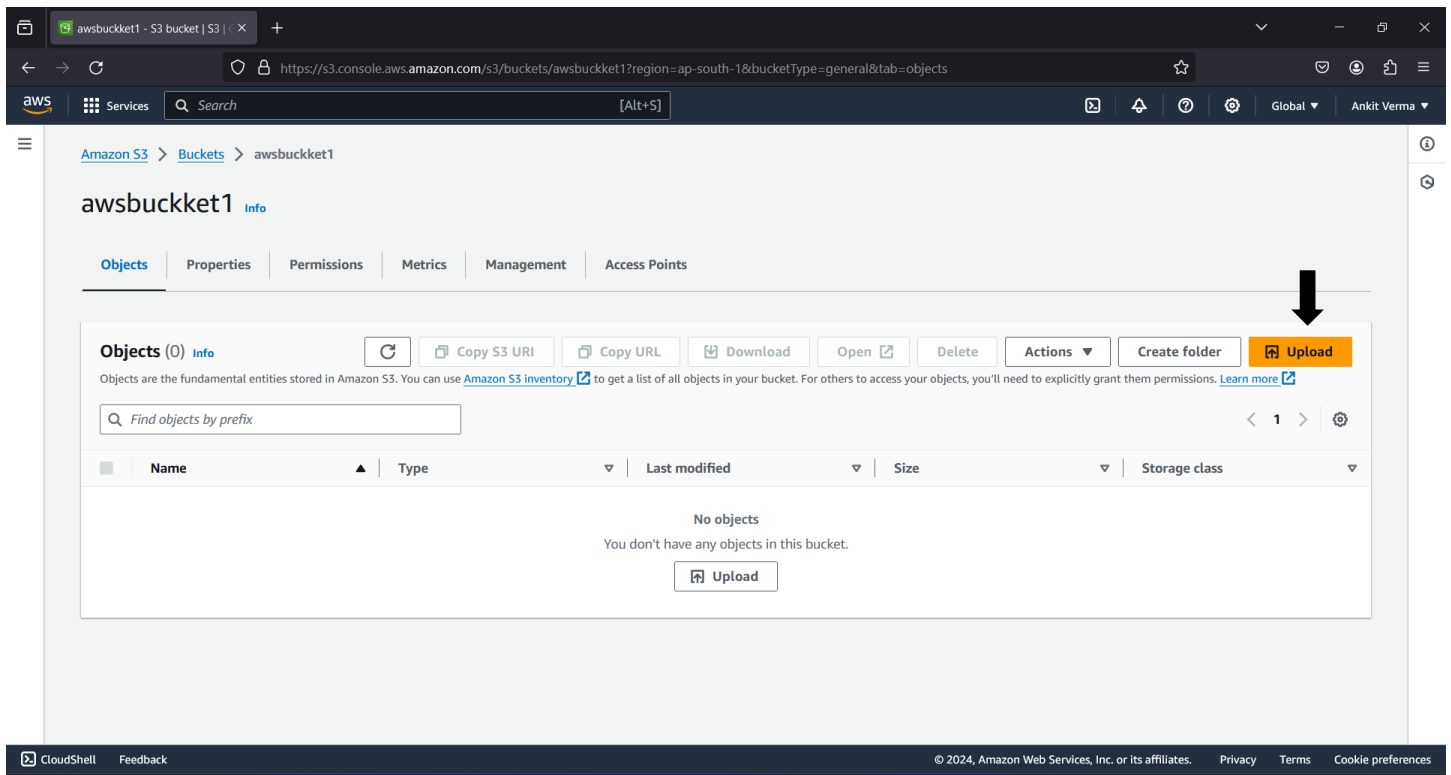
Step 5: Click on “Create Bucket”.



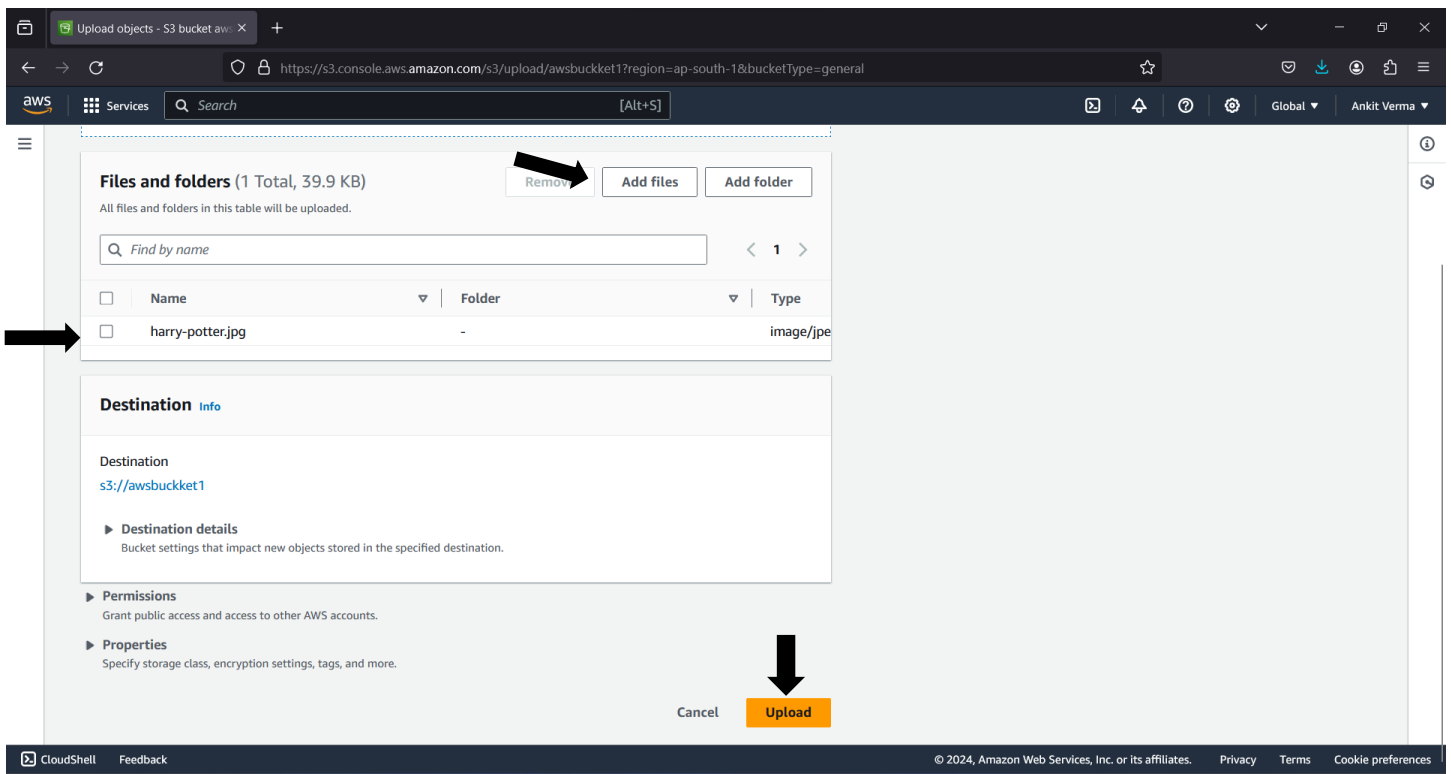
Step 6: The Bucket is created. Click on the bucket name.



Step 7: Click on the “Upload”.



Step 8: Click on “Add file” and add the files then click upload.



Step 9: The file has been uploaded successfully. Click on the file name.

The screenshot shows the AWS S3 console interface. At the top, a green banner indicates "Upload succeeded" with a link to "View details below." Below this, a light blue box contains a warning: "The information below will no longer be available after you navigate away from this page." The main content area is divided into two tabs: "Files and folders" (selected) and "Configuration". Under "Files and folders", it shows "Files and folders (1 Total, 39.9 KB)". A search bar labeled "Find by name" is present. Below the search bar is a table with columns: Name, Folder, Type, Size, Status, and Error. The table contains one entry: "harry-potter..." with a status of "Succeeded". A black arrow points to the file name "harry-potter...".

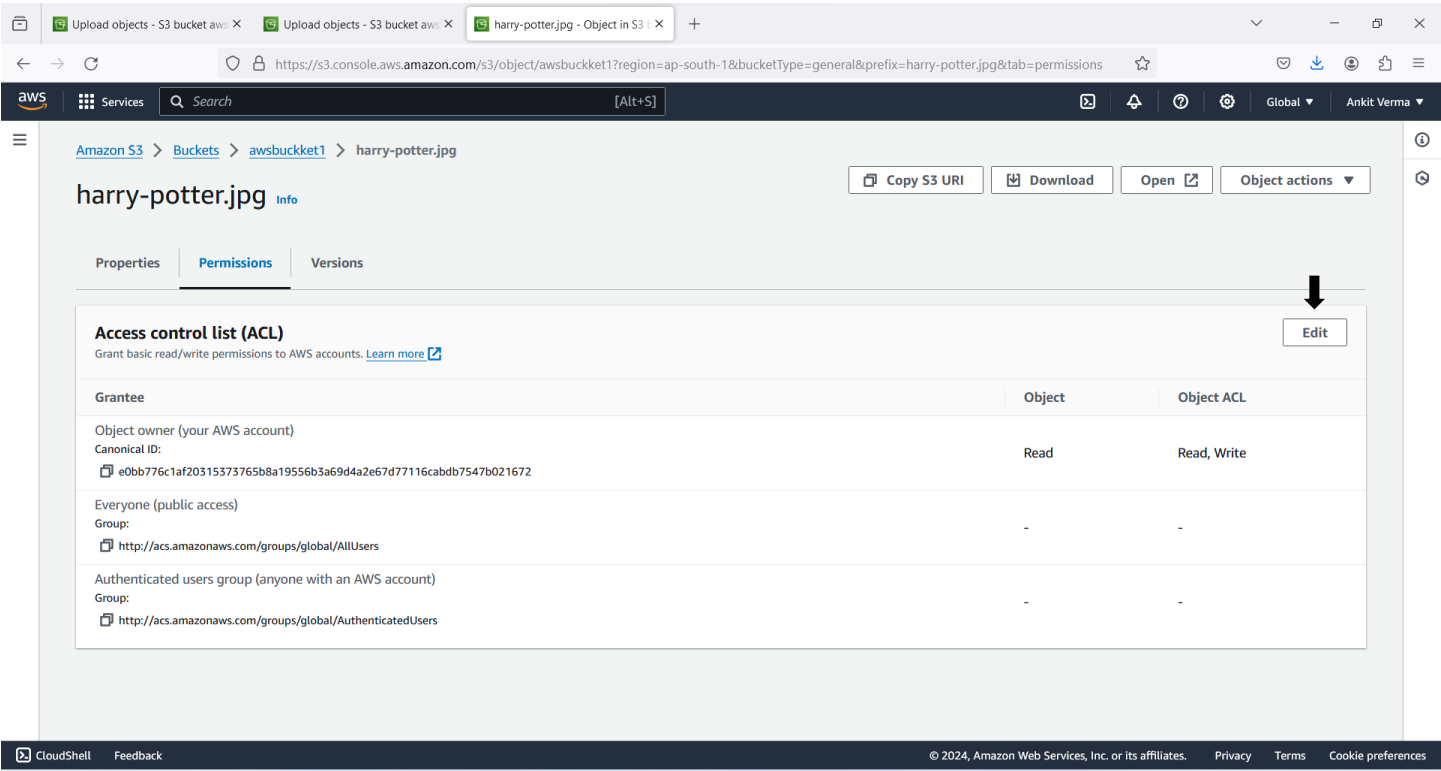
Name	Folder	Type	Size	Status	Error
harry-potter...	-	image/jpeg	39.9 KB	Succeeded	-

Step 10: Click on the "Permissions".

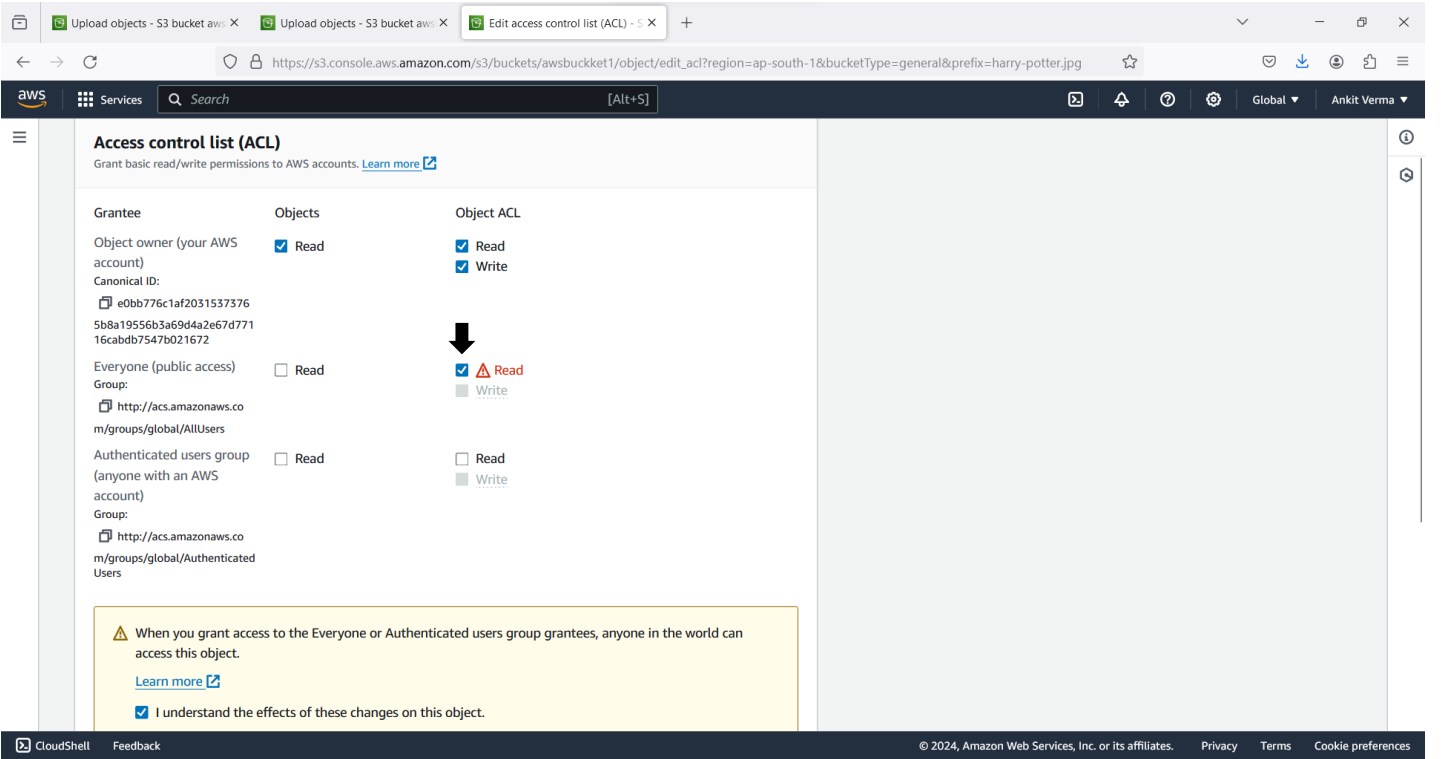
The screenshot shows the AWS S3 console interface for the object "harry-potter.jpg". The breadcrumb navigation is "Amazon S3 > Buckets > awsbucket1 > harry-potter.jpg". The object name "harry-potter.jpg" is displayed with an "Info" link. Below the name are three tabs: "Properties" (selected), "Permissions", and "Versions". A black arrow points to the "Permissions" tab. The "Object overview" section displays various metadata:

- Owner:** e0bb776c1af20315373765b8a19556b3a69d4a2e67d77116cabdb7547b021672
- AWS Region:** Asia Pacific (Mumbai) ap-south-1
- Last modified:** February 20, 2024, 23:48:06 (UTC+05:30)
- Size:** 39.9 KB
- Type:** jpg
- Key:** harry-potter.jpg
- S3 URI:** s3://awsbucket1/harry-potter.jpg
- Amazon Resource Name (ARN):** arn:aws:s3:::awsbucket1/harry-potter.jpg
- Entity tag (Etag):** b32a8bf00e220a49a603bed13cd40c1
- Object URL:** https://awsbucket1.s3.ap-south-1.amazonaws.com/harry-potter.jpg

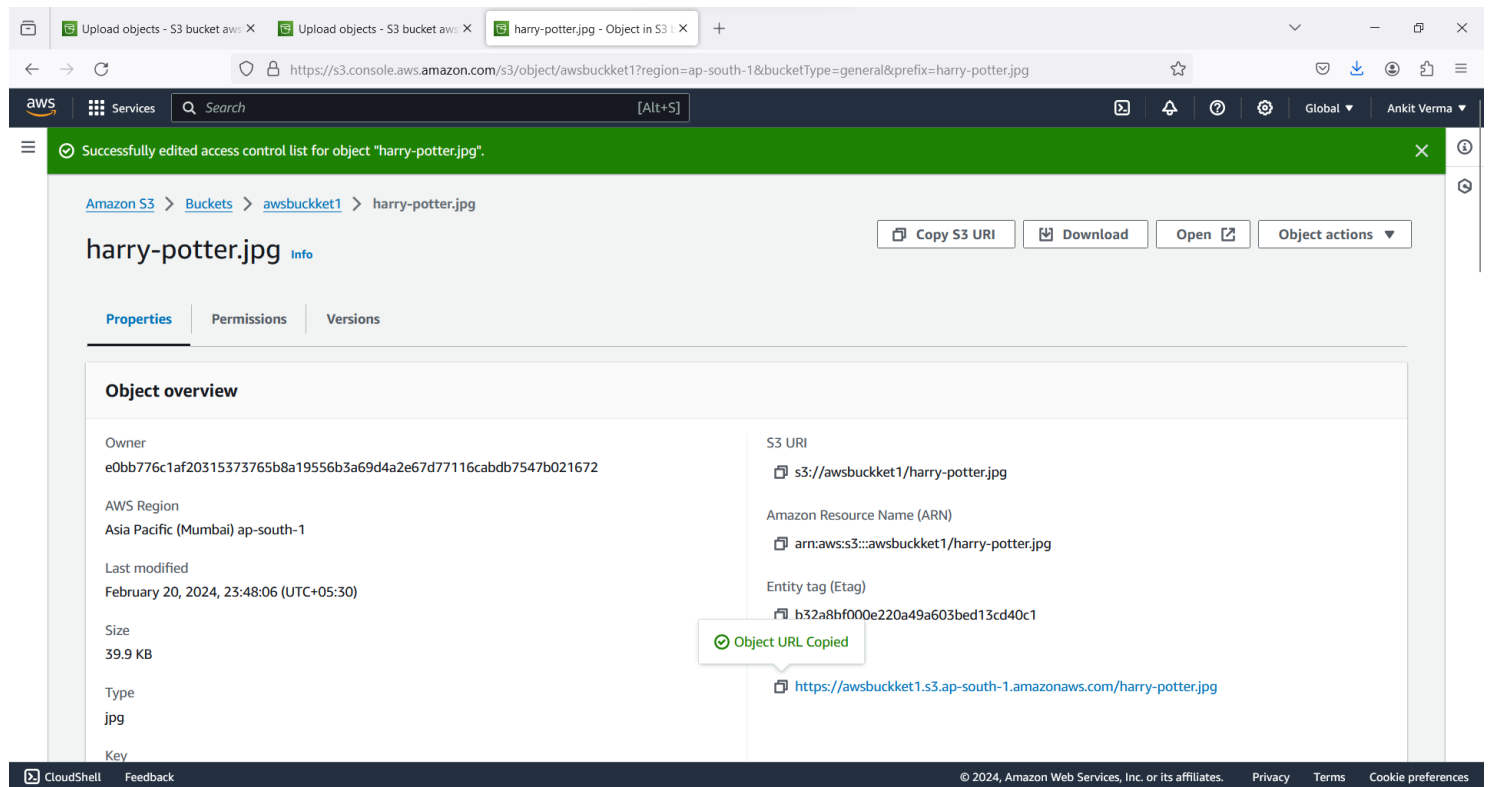
Step 11: Click on the “Edit”.



STEP 12- Give the “Read” permissions.



STEP 13- Click on “Save Changes” & Copy the “Object URL”.



STEP 14- Open a new browser window and paste the URL.

