

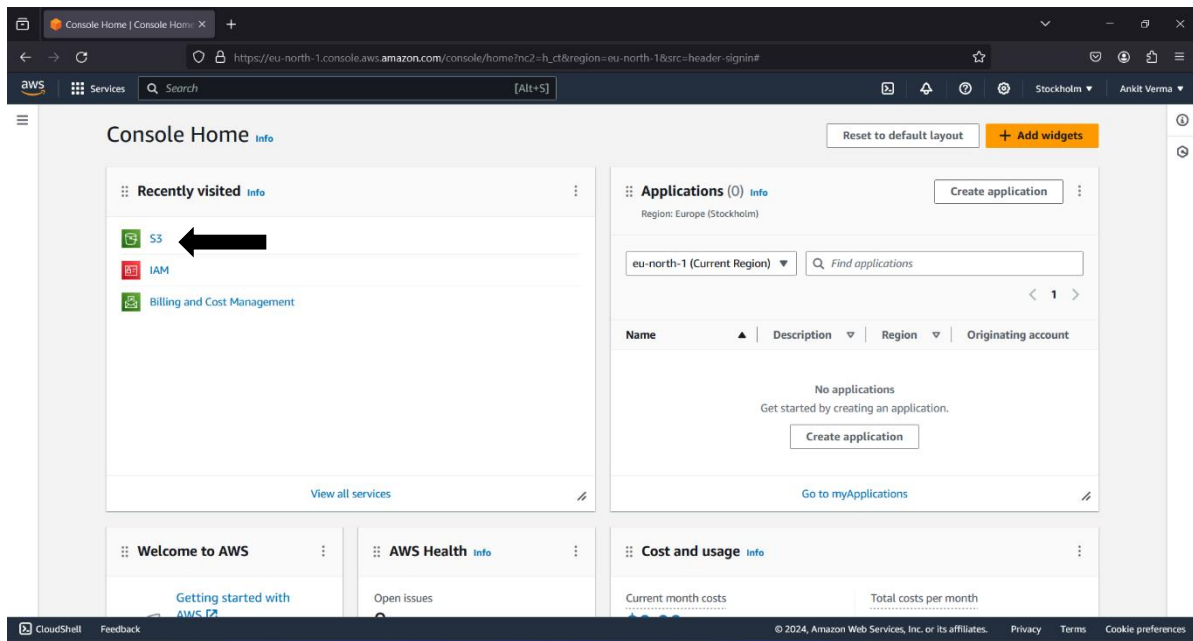
Assignment: 6

Problem Statement: Upload a static website on S3.

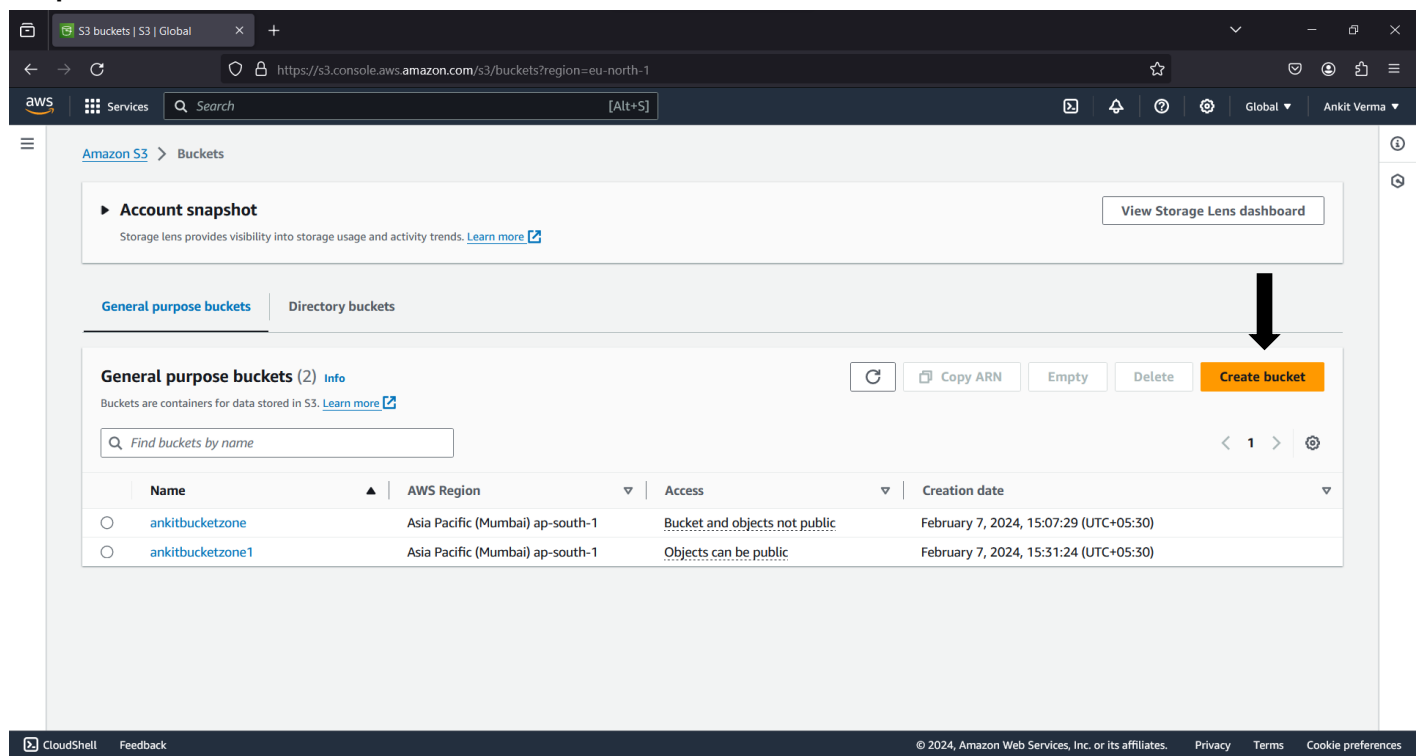
» The steps to upload the website:-

Step 1: Create 3 static website using HTML.

Step 2: Click on the “S3” button.



Step 3: Click on “Create Bucket”.



Step 4: 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 5: 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)**
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**

Turning off block all public access might result in this bucket and the objects within becoming public

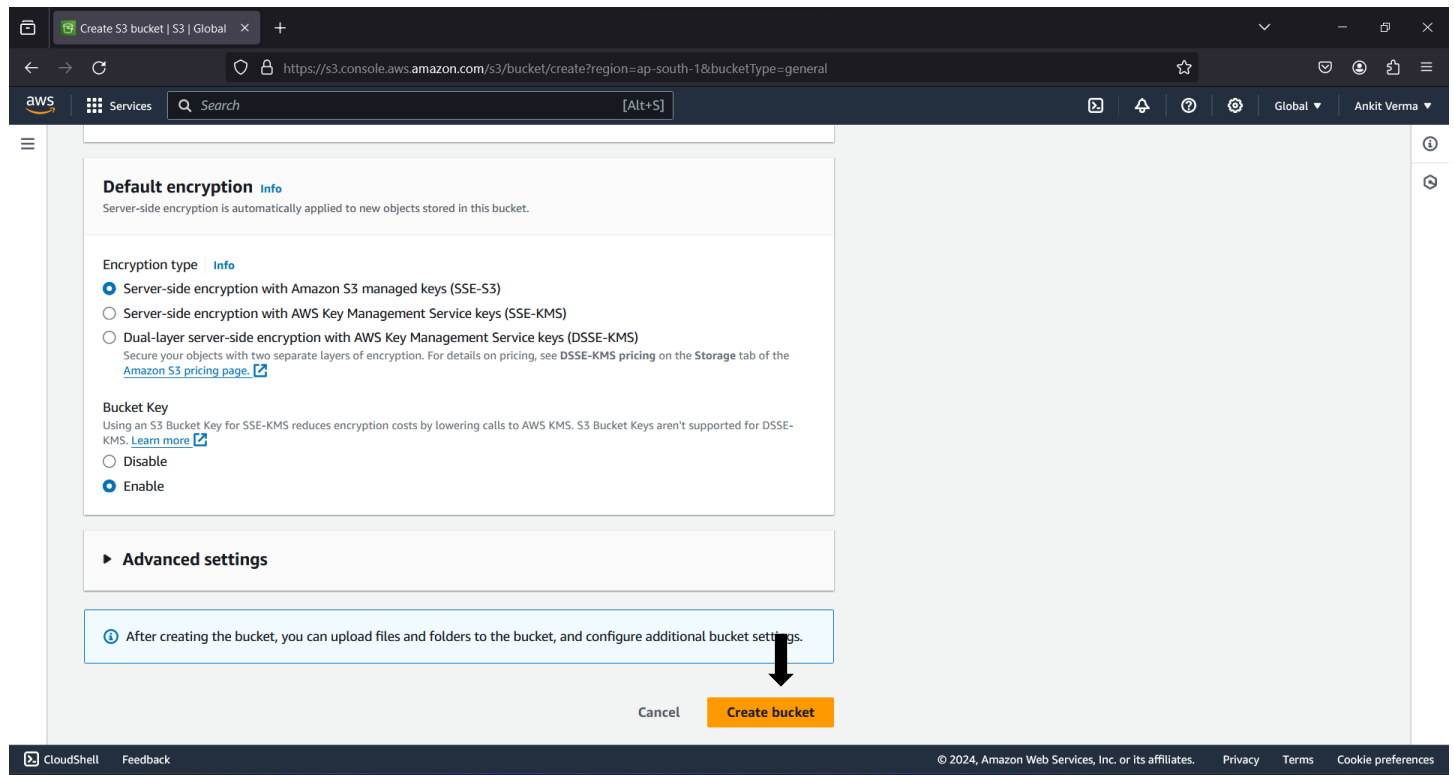
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

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

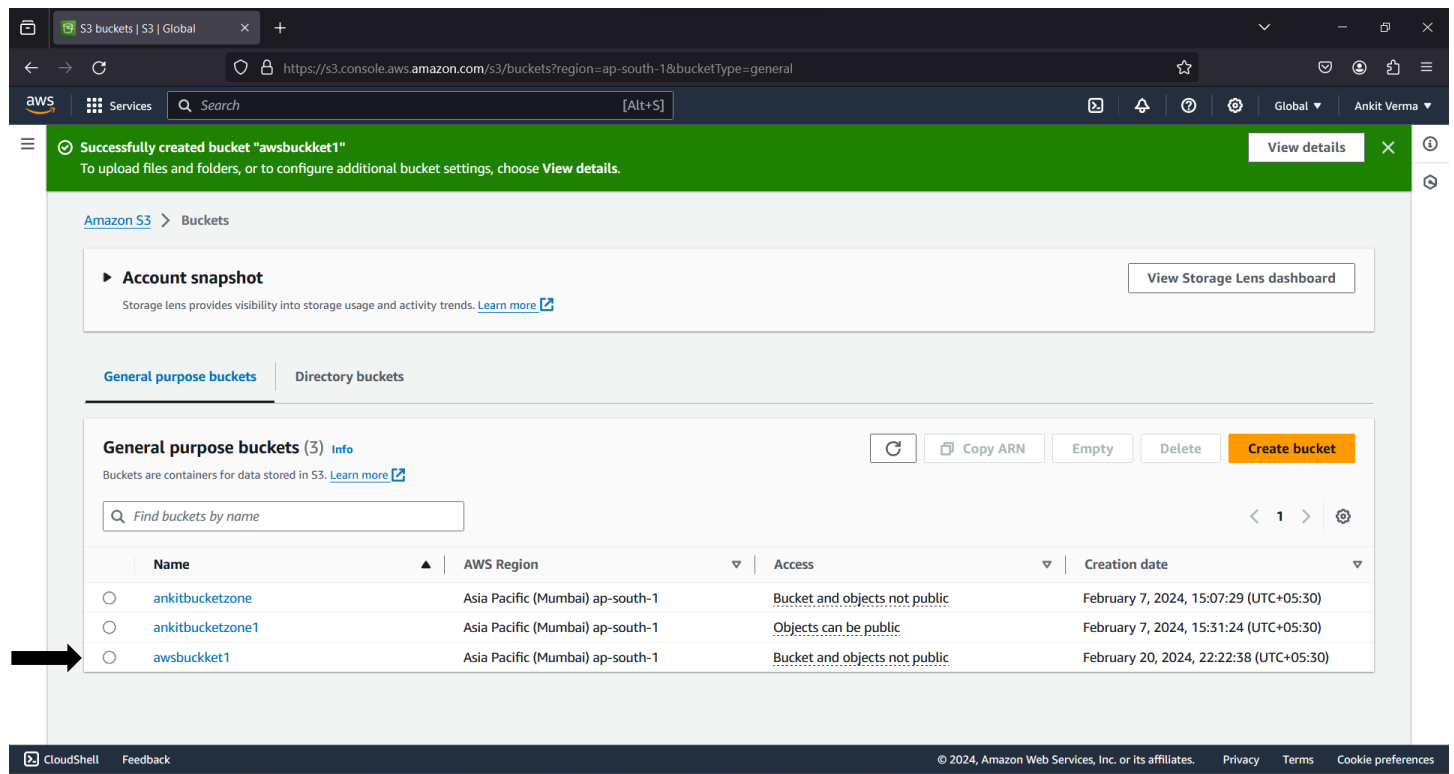
CloudShell Feedback

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

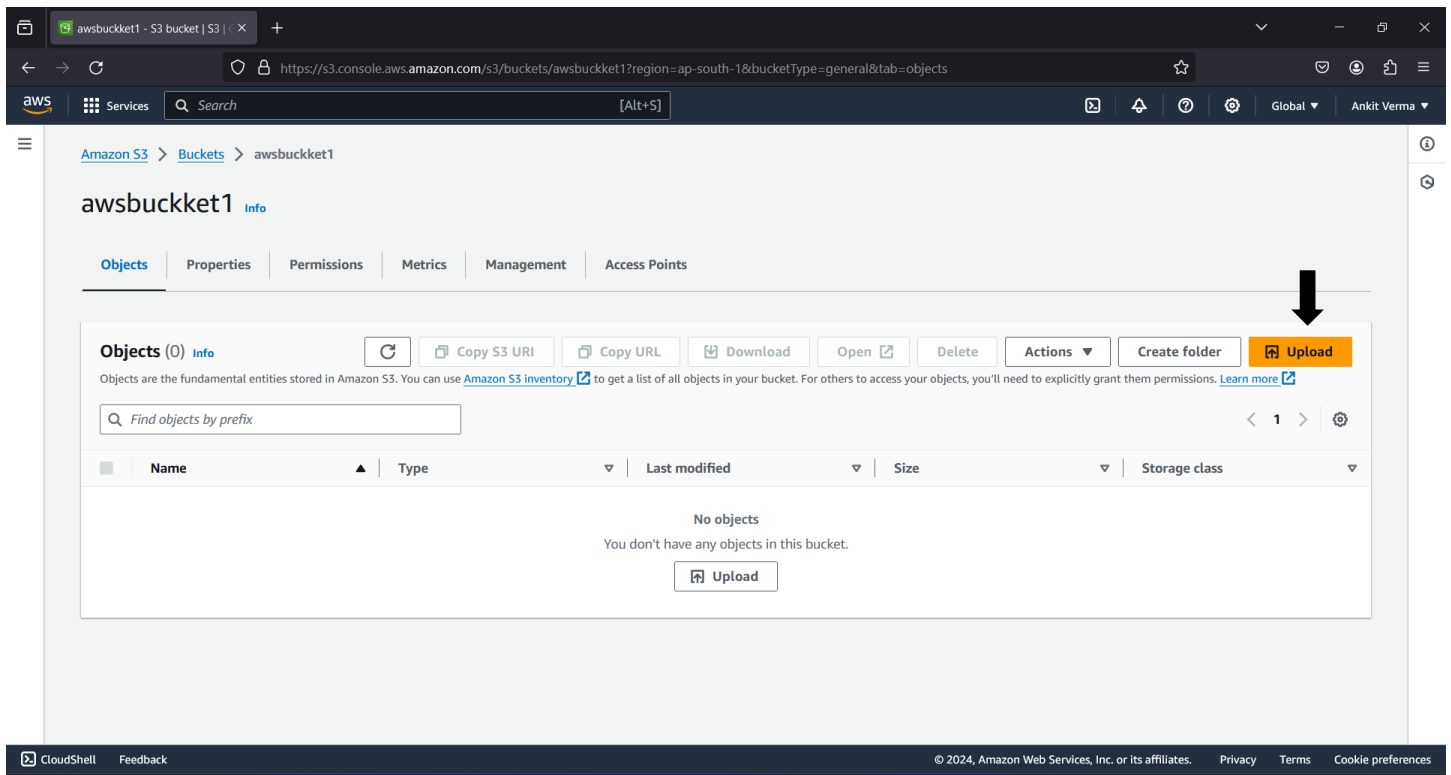
Step 6: Click on “Create Bucket”.



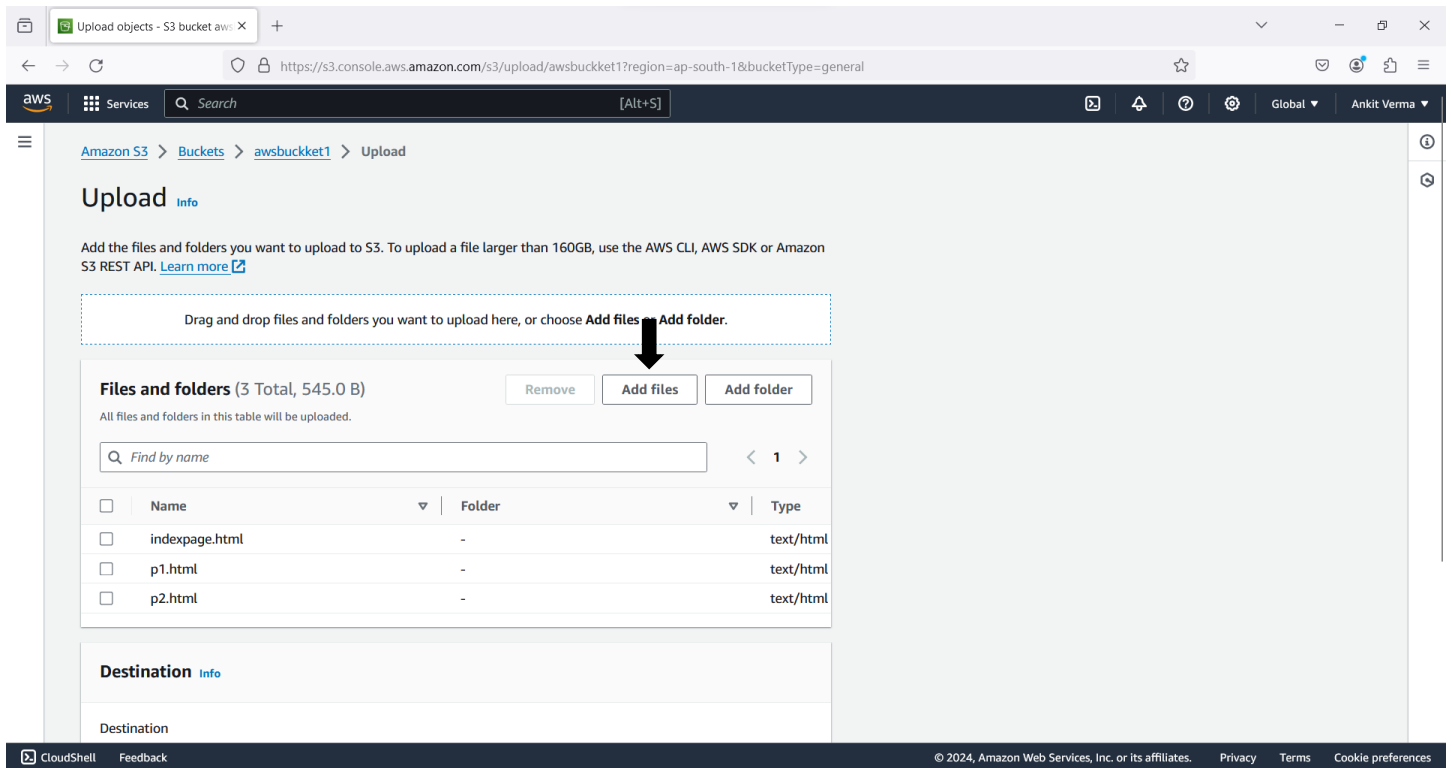
Step 7: The Bucket is created. Click on the bucket name.



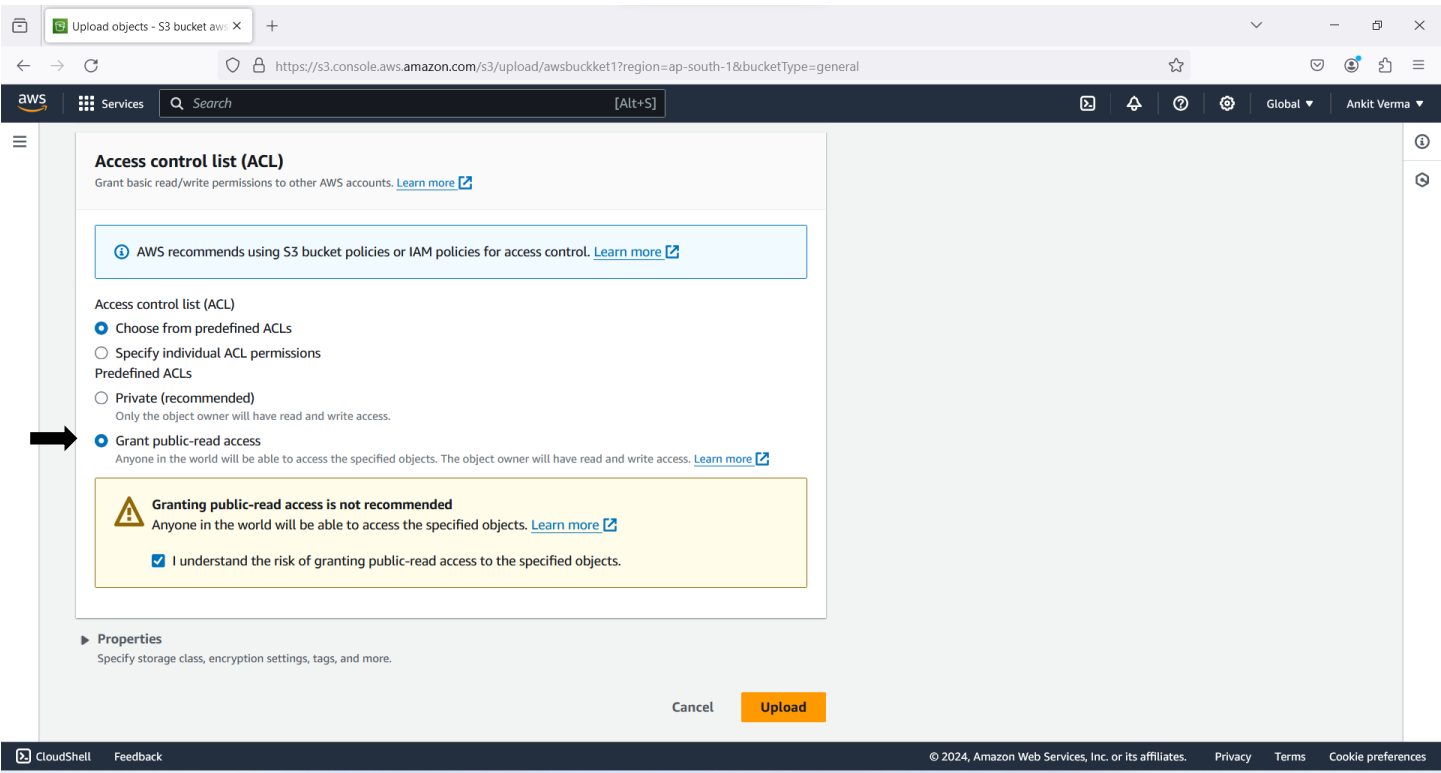
Step 8: Click on the “Upload”.



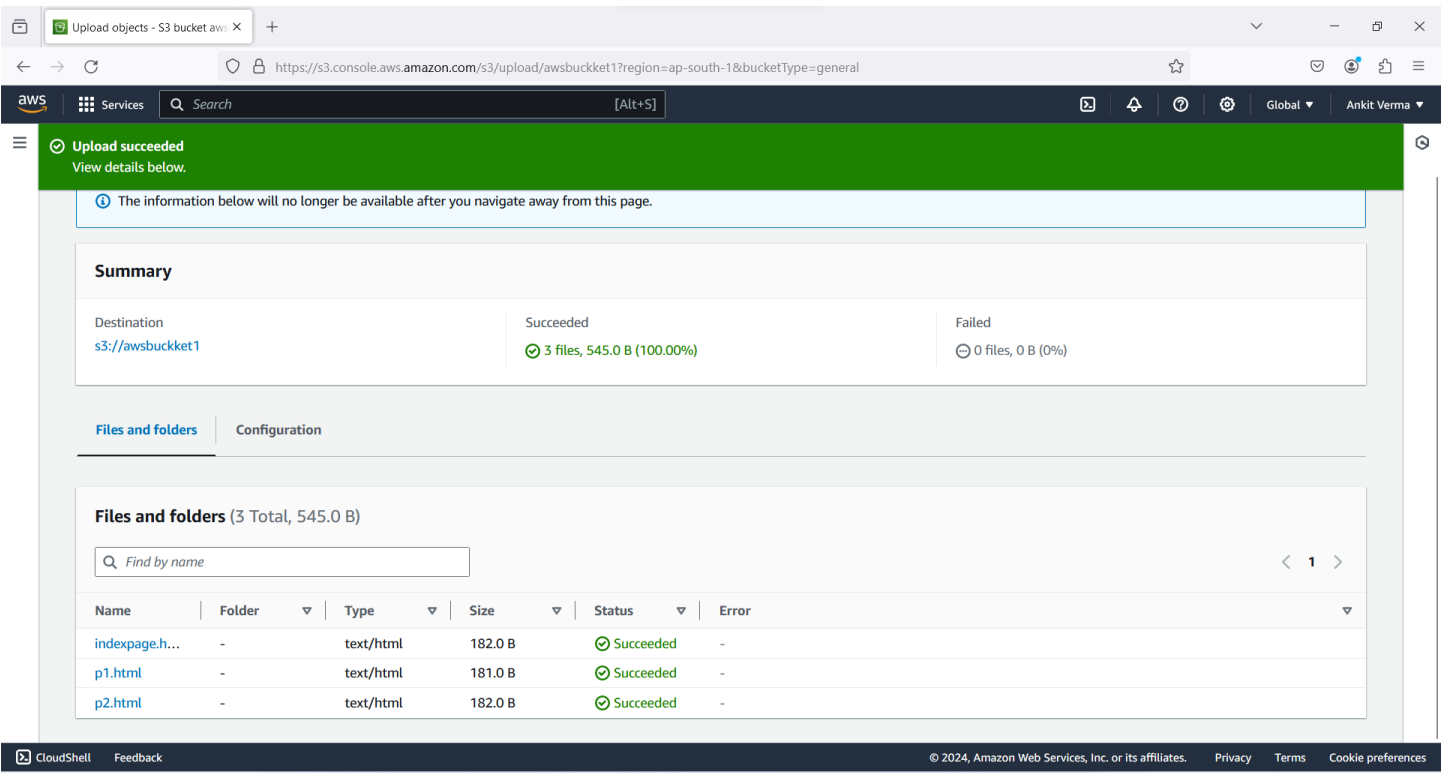
Step 9: Click on “Add file” and add the HTML files.



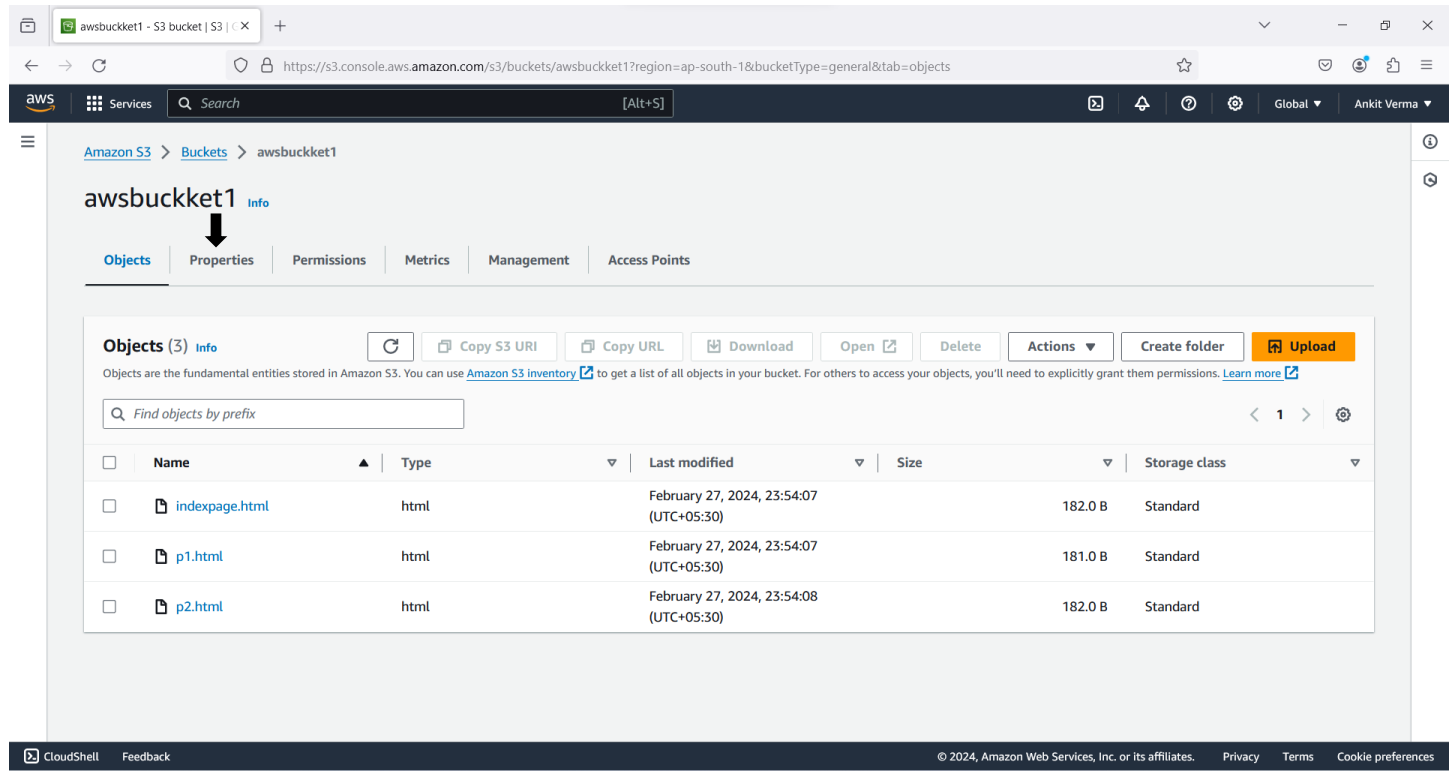
Step 10: Select Granting Public Read Access option. Click the “I understand” then click Upload.



Step 11: Files uploaded successfully.



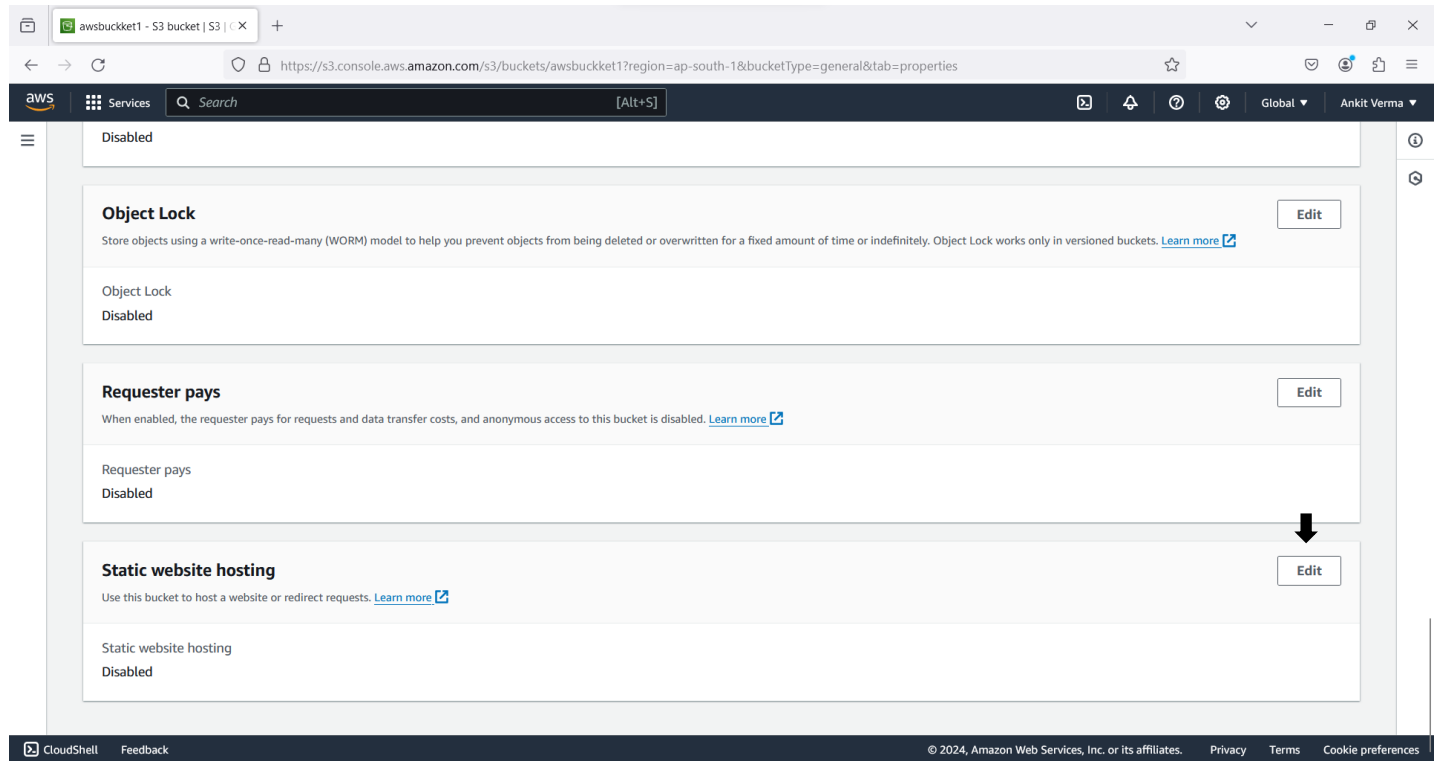
Step 12: From the bucket go to the Properties.



The screenshot shows the AWS S3 console interface. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > awsbucket1'. The main heading is 'awsbucket1' with an 'Info' link. Below this, there are tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is currently selected, showing a list of objects in the bucket. Above the list are buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A search bar is present with the placeholder text 'Find objects by prefix'. The table below lists three objects: 'indexpage.html', 'p1.html', and 'p2.html', each with details on its type, last modified date, size, and storage class.

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	indexpage.html	html	February 27, 2024, 23:54:07 (UTC+05:30)	182.0 B	Standard
<input type="checkbox"/>	p1.html	html	February 27, 2024, 23:54:07 (UTC+05:30)	181.0 B	Standard
<input type="checkbox"/>	p2.html	html	February 27, 2024, 23:54:08 (UTC+05:30)	182.0 B	Standard

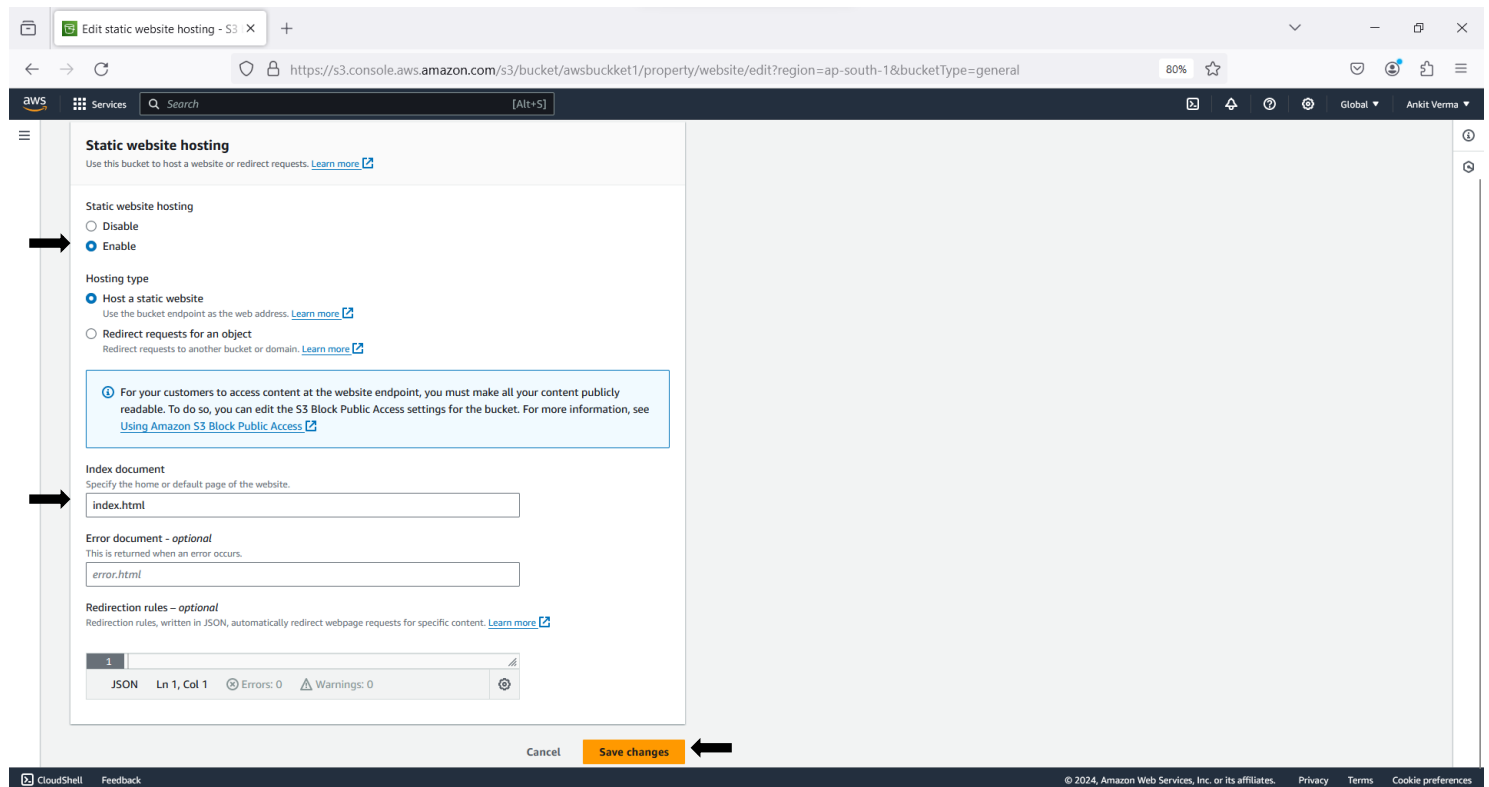
STEP 13- In Static Website Hosting, click on 'Edit'.



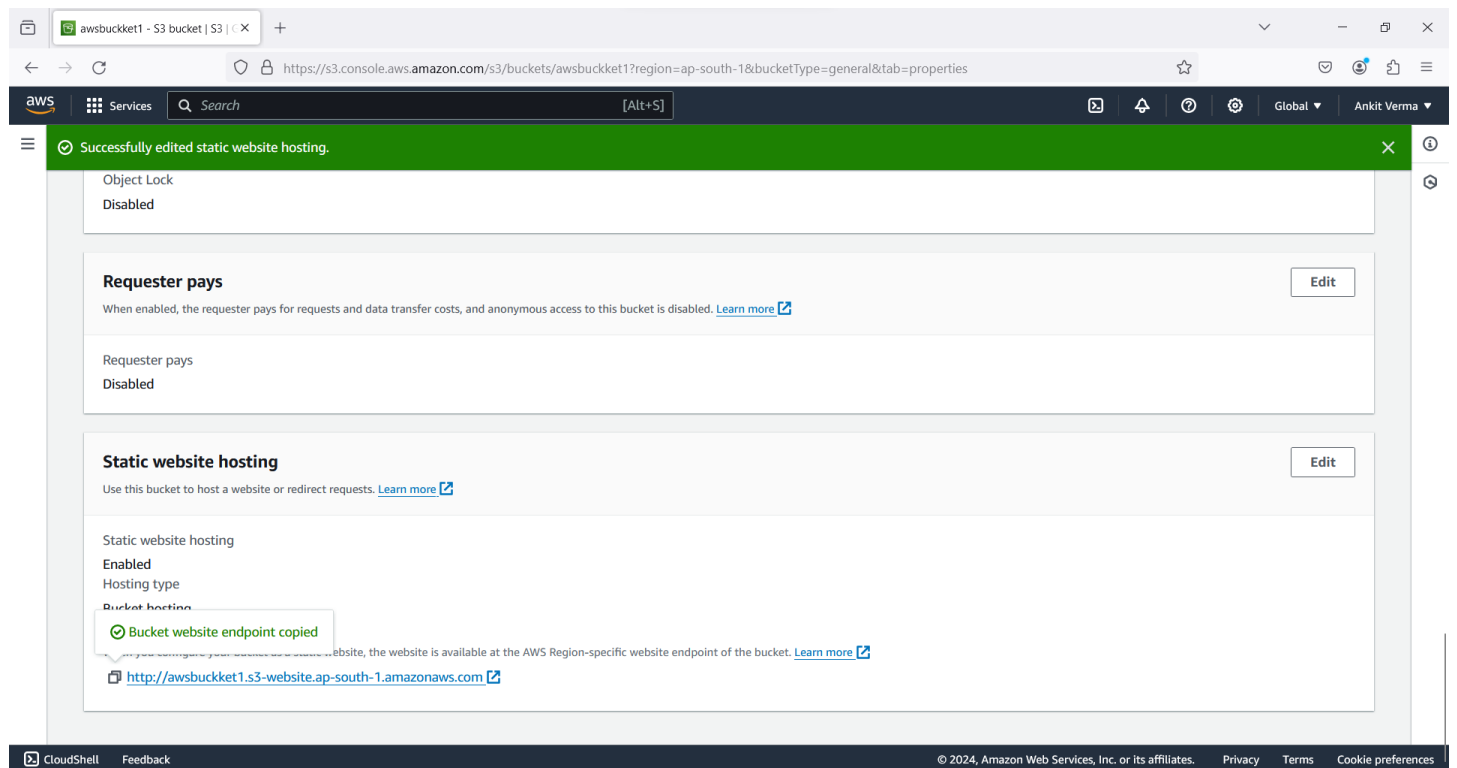
The screenshot shows the 'Properties' tab for the 'awsbucket1' bucket. The 'Static website hosting' section is highlighted with a black arrow pointing to the 'Edit' button. The 'Object Lock' and 'Requester pays' sections are also visible, each with an 'Edit' button. The 'Static website hosting' section is currently disabled.

Static website hosting
Disabled

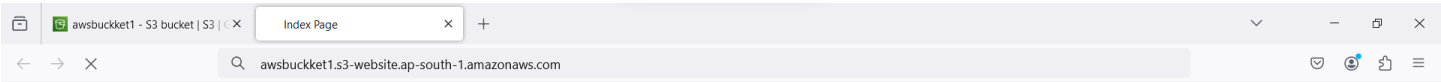
STEP 14- Select Enable. Give the name of the index file “index.html” & save changes.



STEP 15- From Static Website Hosting copy the url.



STEP 16- Open a new window and paste the url.



Services

[Services](#)

About

[About](#)