



**Ganpat
University**

॥ विद्यया समाजोत्कर्षः ॥

**Institute of
Computer
Technology**

Name: Tushar Panchal

En.No: 21162101014

Sub: CCE(Cloud Computing Essentials)

Branch: CBA

Batch:71

-----PRACTICAL 05-----

Configure and set up S3 Bucket policy user-wise and role-wise for this organization.

Lab Overview:

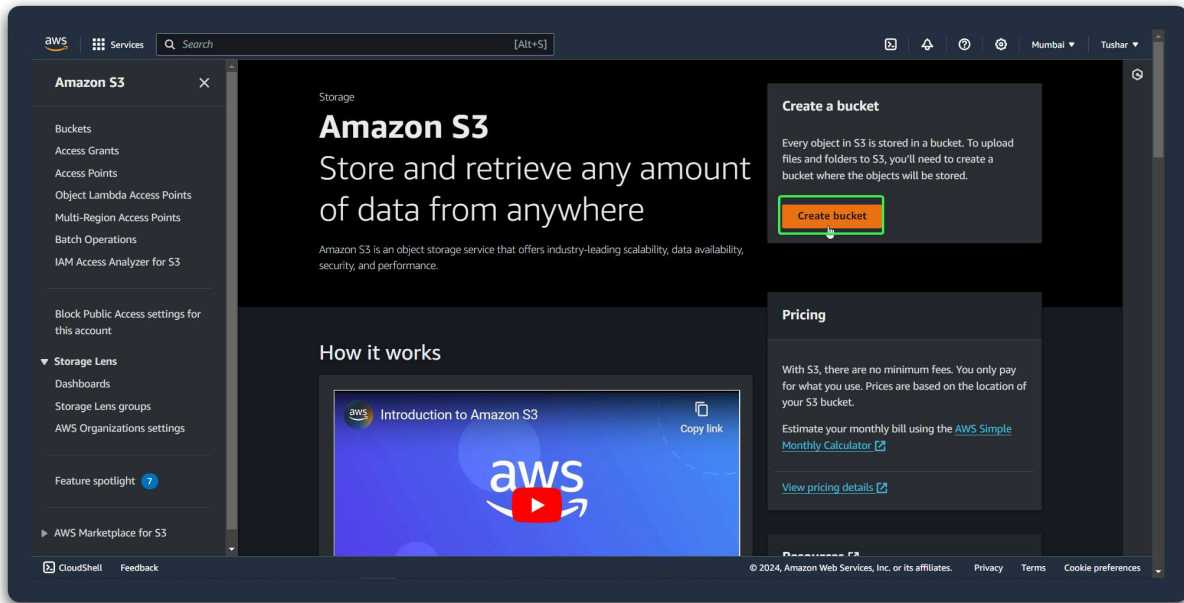
This lab focuses on Amazon S3 or Amazon Simple Storage Service offered by Amazon Web Services which provides object storage through a web service interface. Amazon S3 uses the same scalable storage infrastructure that Amazon.com uses to run its global e-commerce network. You are required to accomplish the following task based on the scenarios as shown in the figure:

Refer to the lab scenario attached herewith.

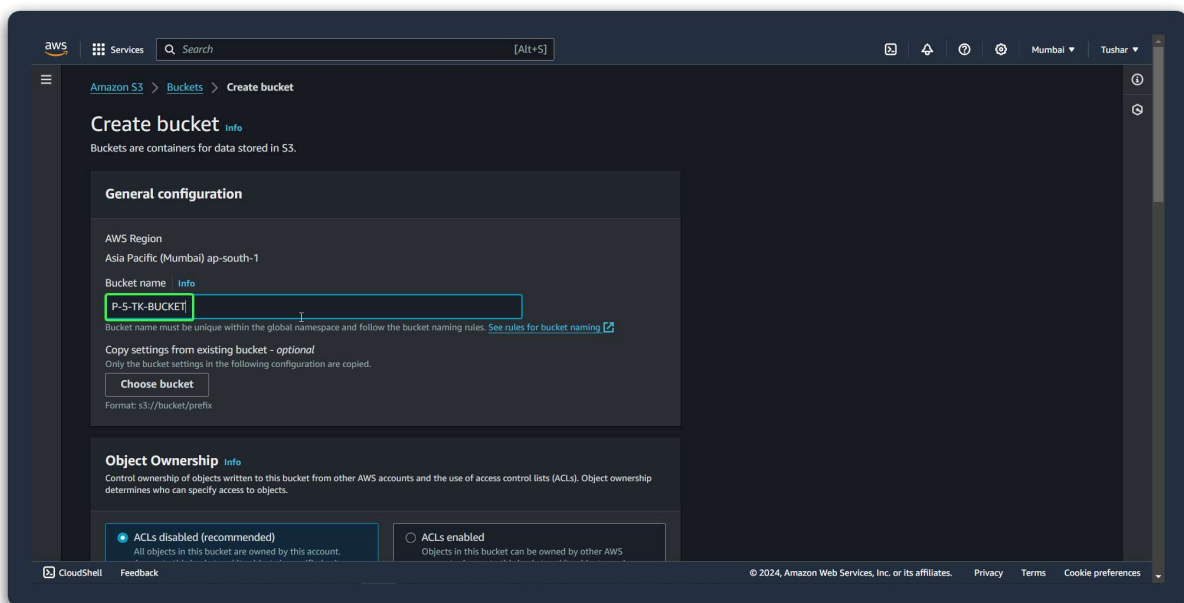
Tasks to be completed:

- 1. Create the S3 bucket**
- 2. Give the public access to S3 buckets**
- 3. Host static HTML site from S3 buckets**
- 4. Enable Versioning and test it**

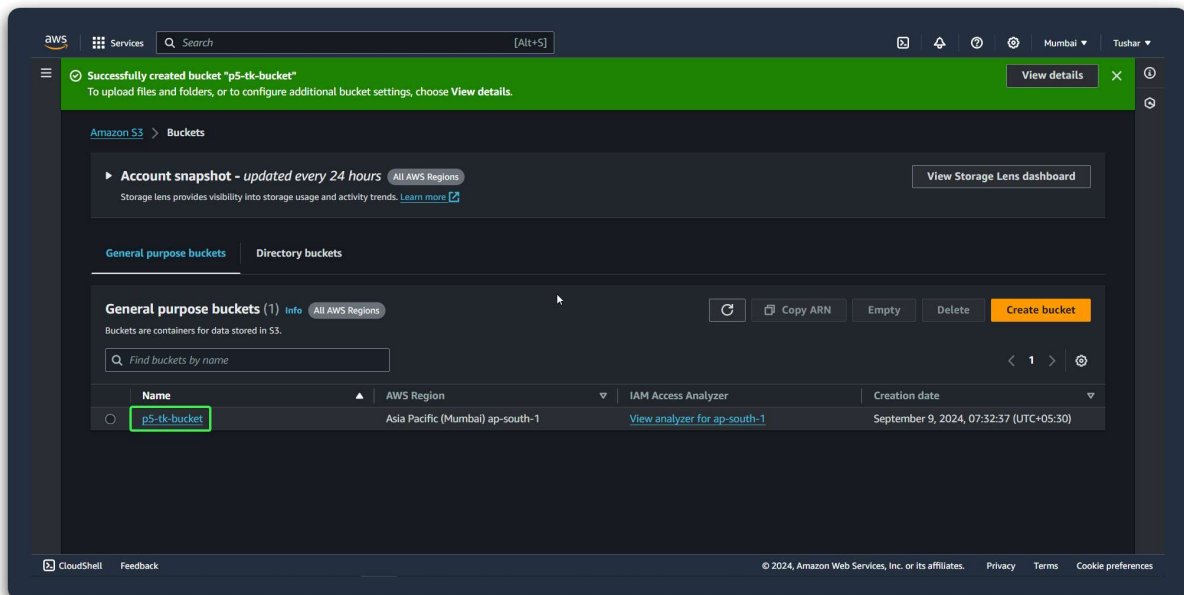
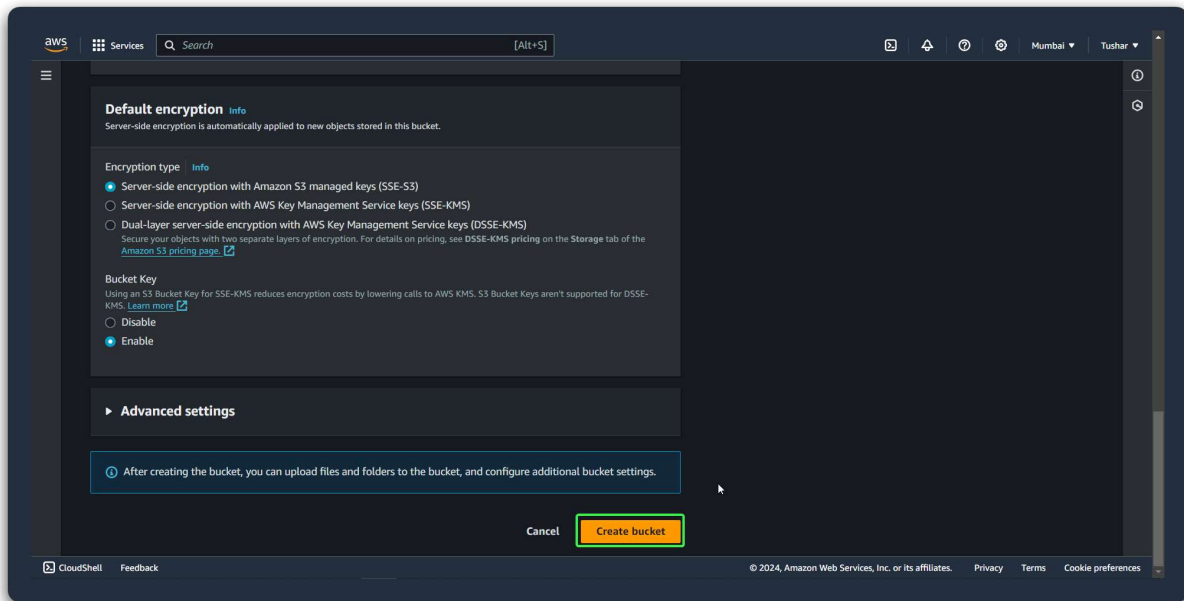
» First you have to create the Amazon S3 buckets.



Give it a name and don't do other changes

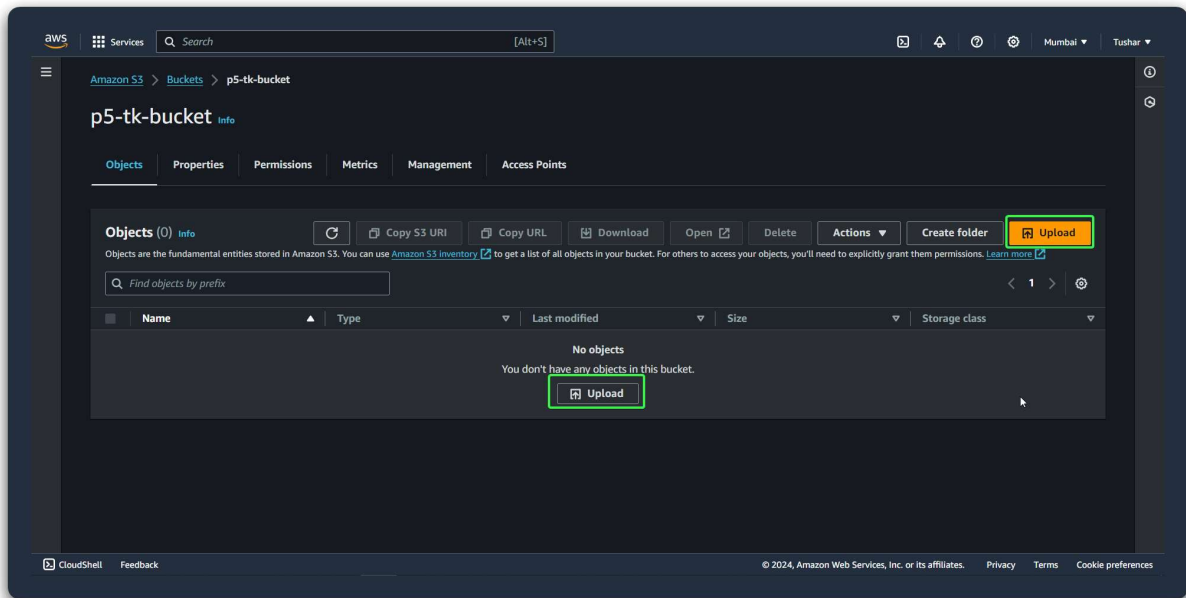


Create the bucket without making any changes



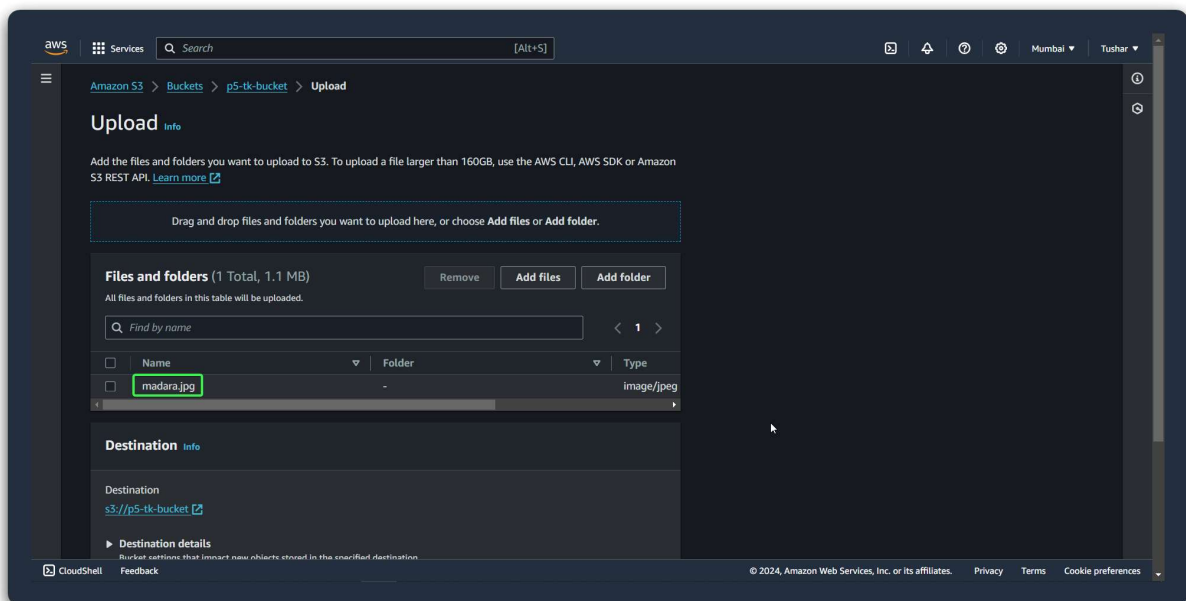
As you can see above our bucket has been created successfully.

Now upload an image or any file

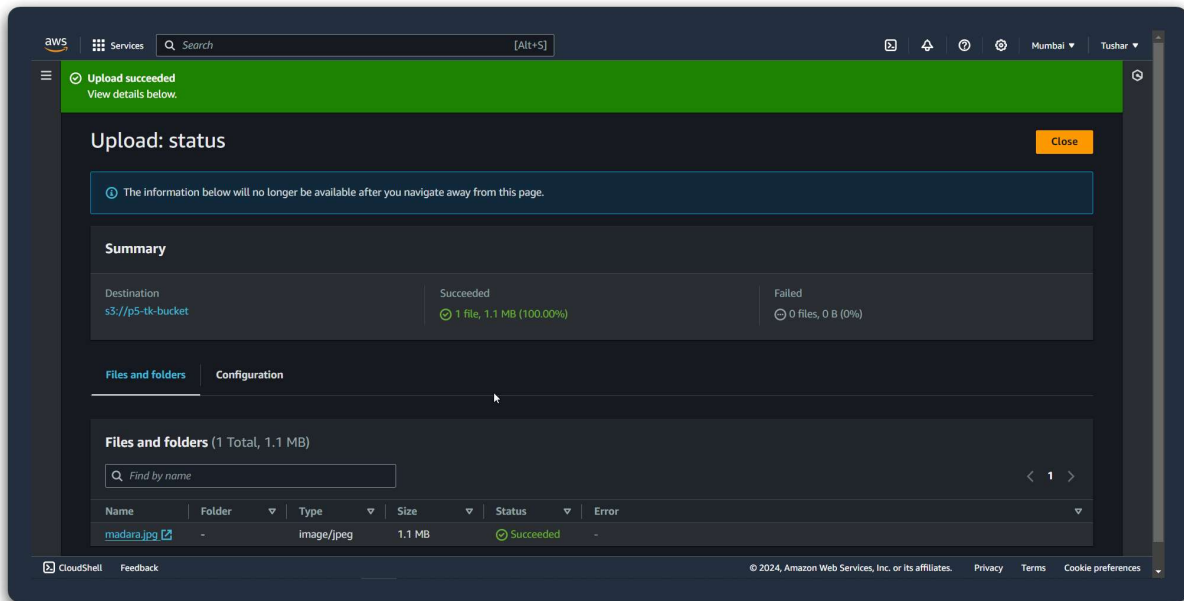


Here you have to upload any file you want

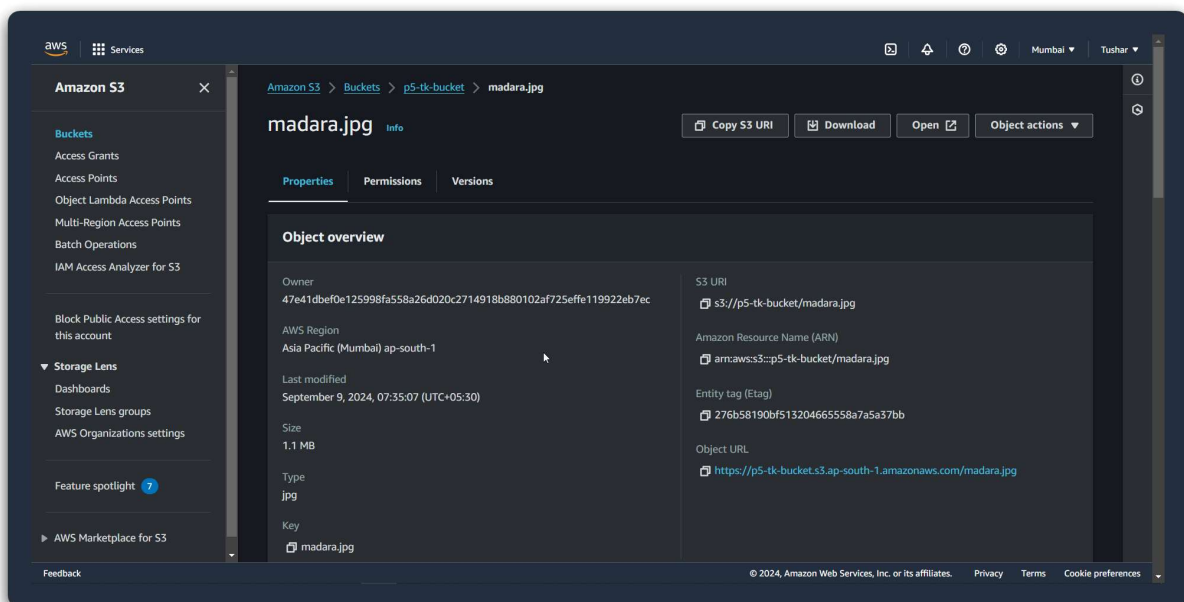
Here you can see I have uploaded the .png file



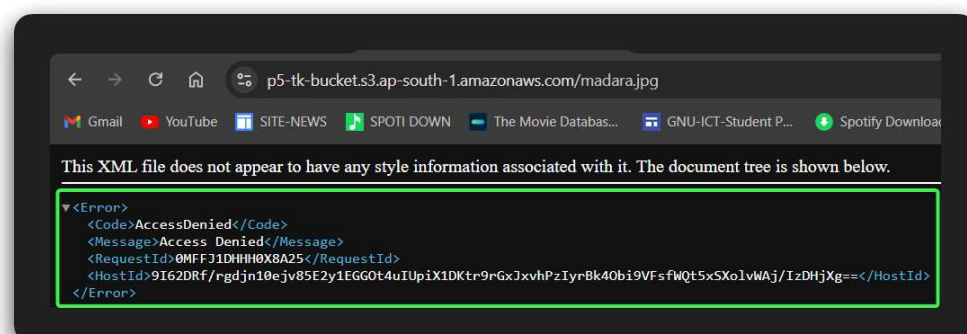
As you can see below file has been uploaded successfully



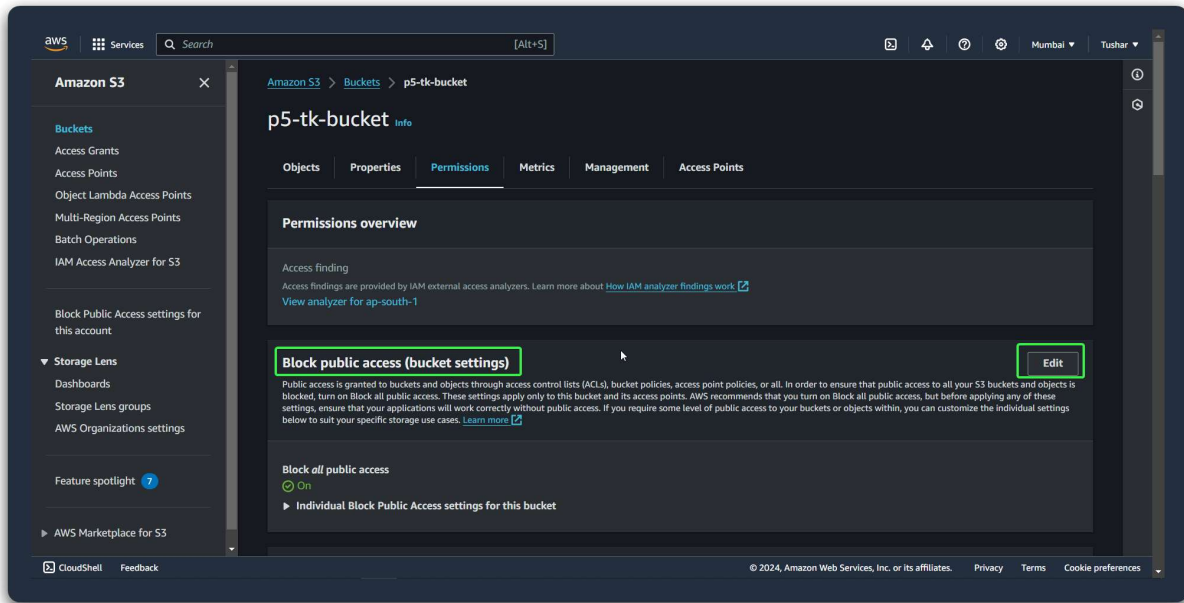
Here we can see the object url you can get the access of the image



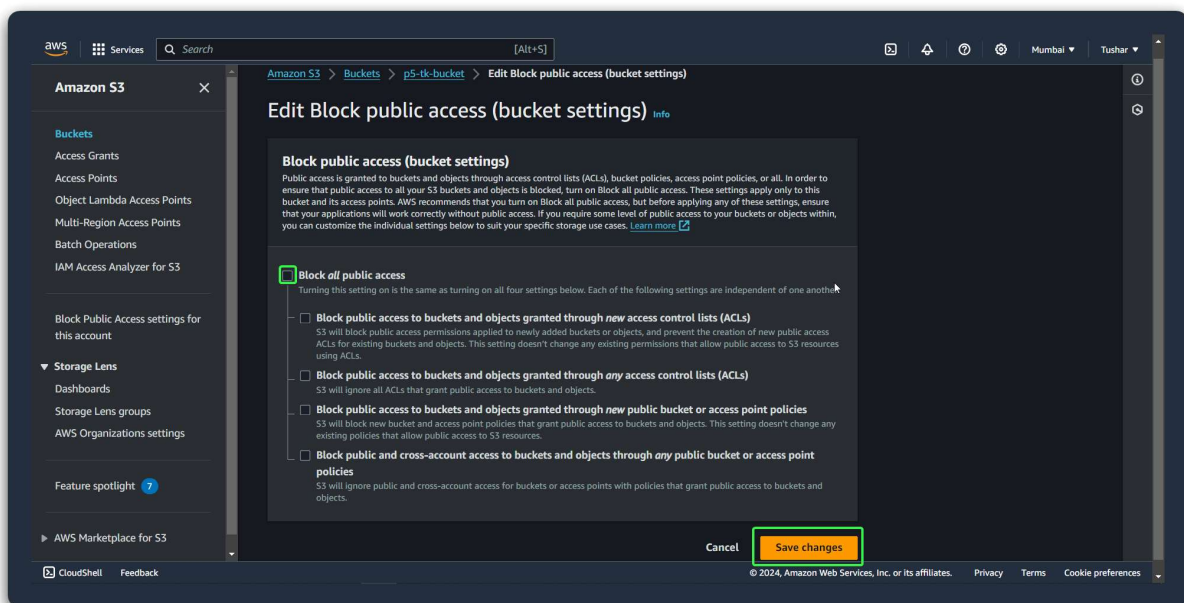
If you open the object URL Here you can see the access denied



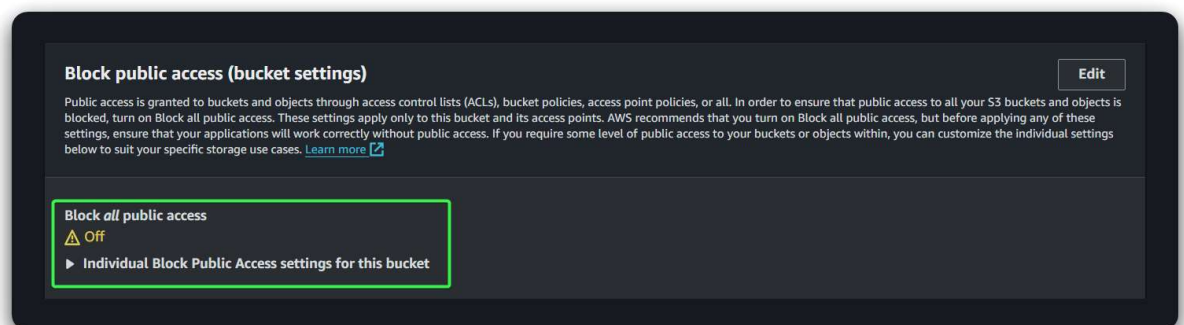
Now you have to turn off the Block the public access.



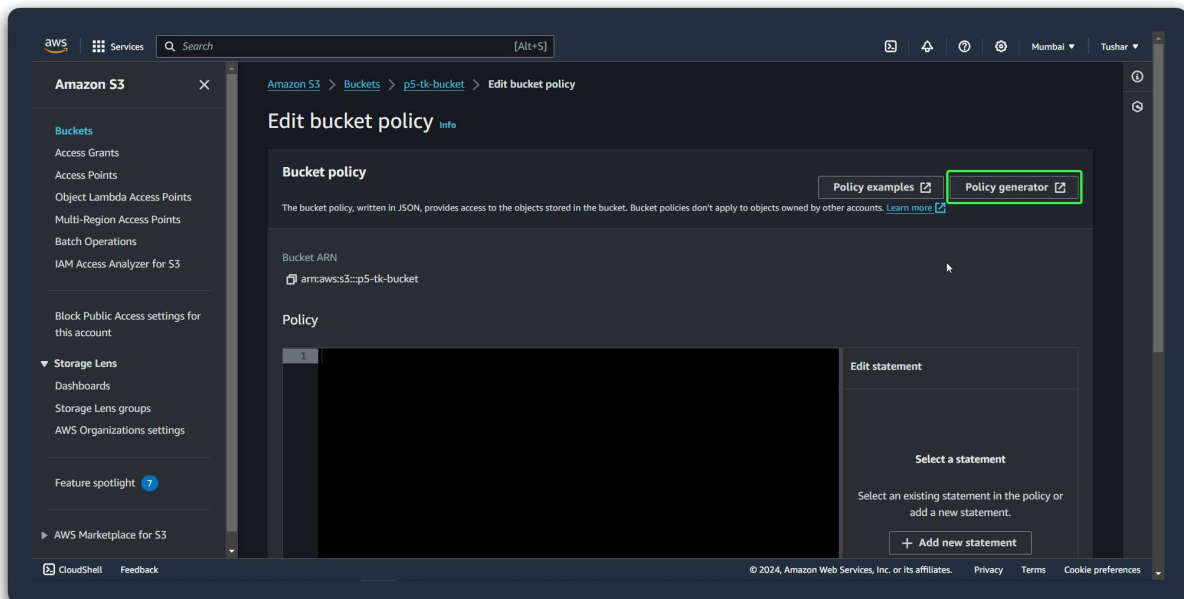
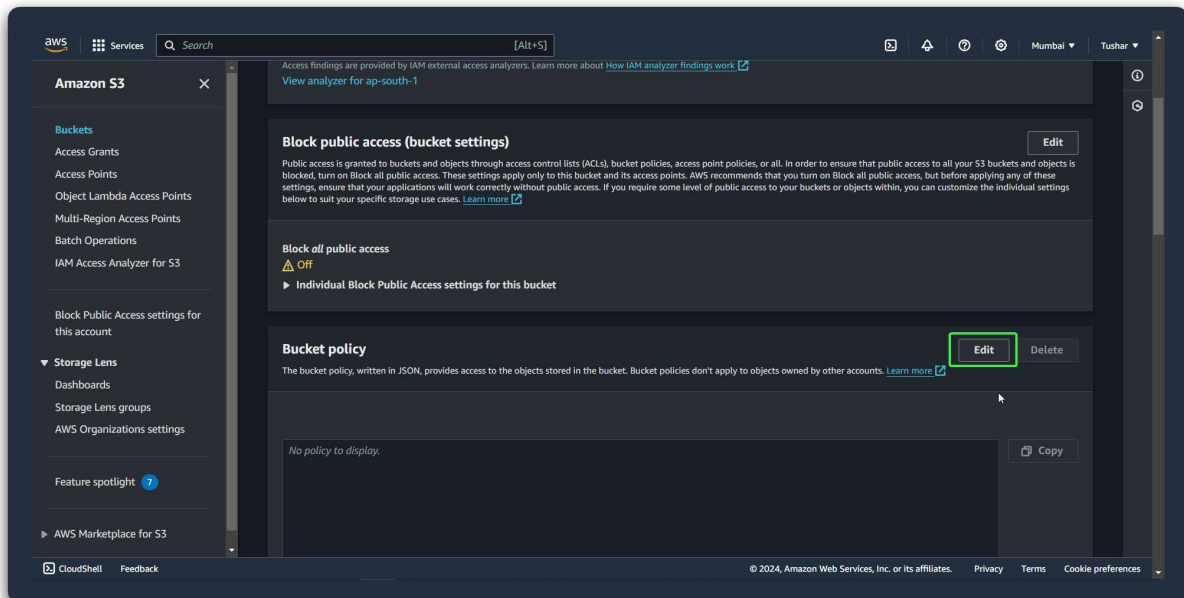
Turn off the block all public access and save the changes



Now as you can see here the block public access is off now



Now you have to generate the Bucket policy in edit you can get the Policy Generator



As below do the same but In principal gave the name * only

Step 1: Select Policy Type
A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)
A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3

☐ All Services ("*")

Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected ☐ All Actions ("*")

Amazon Resource Name (ARN) (BucketName)/\$ (KeyName).

☐ GetMetricsConfiguration
☐ GetMultiRegionAccessPoint
☐ GetMultiRegionAccessPointPolicy
☐ GetMultiRegionAccessPointPolicyStatus
☐ GetMultiRegionAccessPointRoutes
☒ **GetObject**
☐ GetObjectAcl
☐ GetObjectAttributes

1. You must enter a valid ARN.

Step 3: Generate Policy
A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.
Add one or more statements above to generate a policy.

Here select the action as get object and in ARN paste your bucket ARN and click on generate policy

Amazon S3 ☐ All Services ("*")

Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- ☐ All Actions ("*")

Amazon Resource Name (ARN)

ARN should follow the following format: `arn:aws:s3:::{BucketName}/{KeyName}`.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

You added the following statements. Click the button below to Generate a policy.

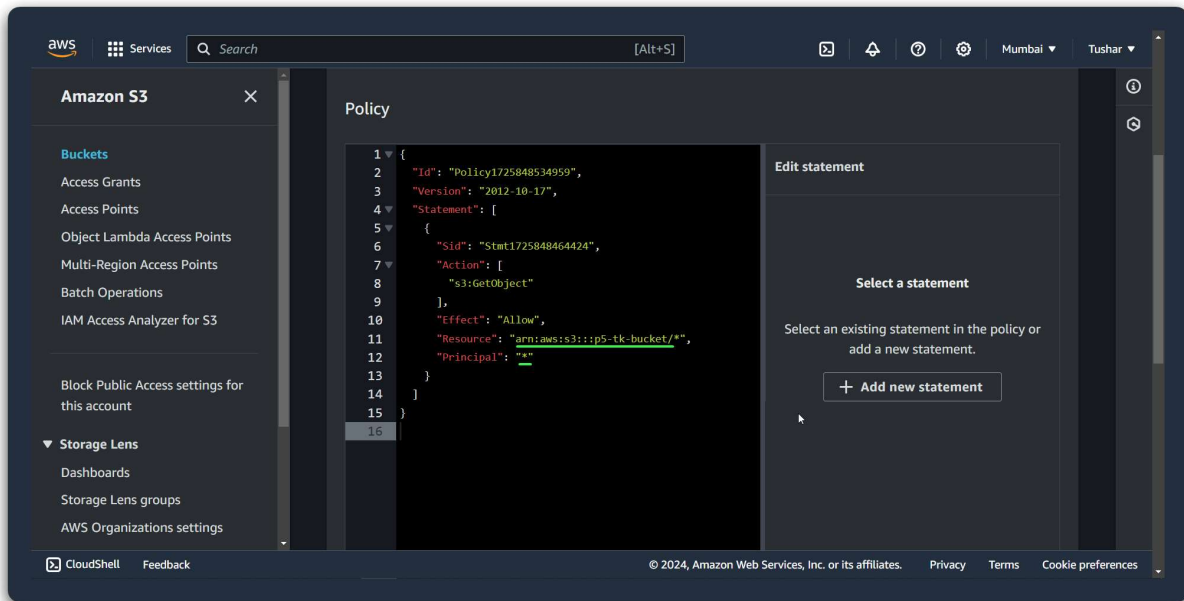
| Principal(s) | Effect | Action | Resource | Conditions |
|--------------|--------|--------------|---------------------------|------------|
| * * | Allow | s3:GetObject | arn:aws:s3:::p5-tk-bucket | None |

Step 3: Generate Policy
A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.

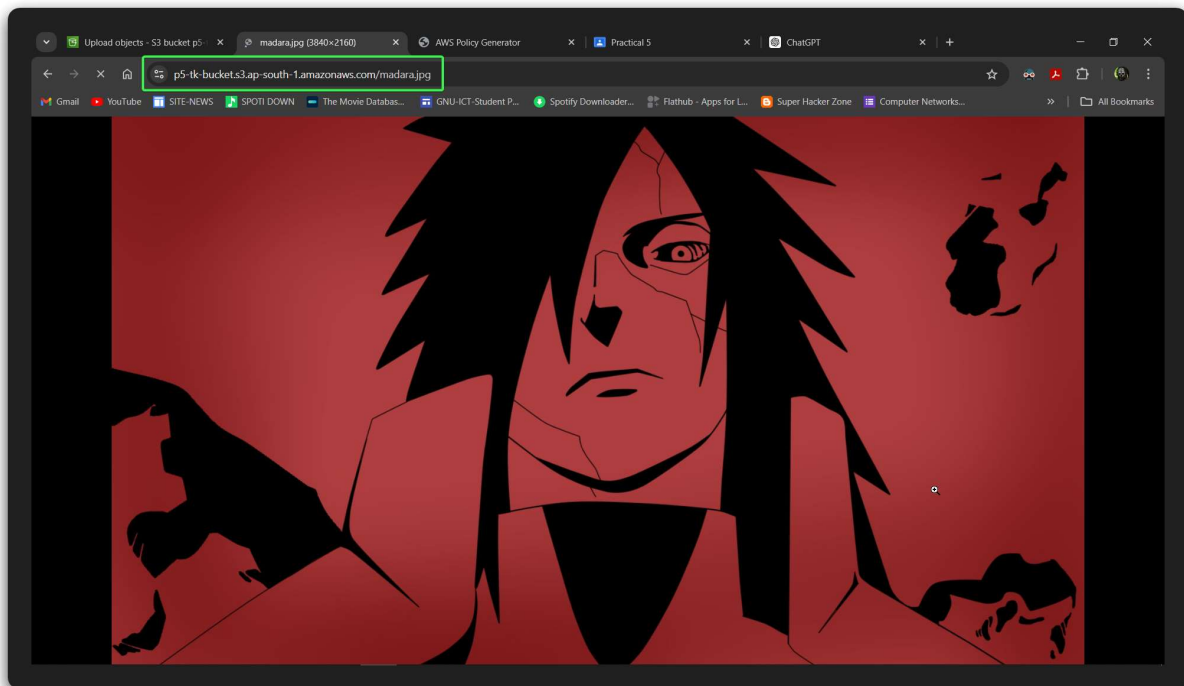
Generate Policy [Start Over](#)

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.
©2010, Amazon Web Services LLC or its affiliates. All rights reserved.
An **amazon.com** company

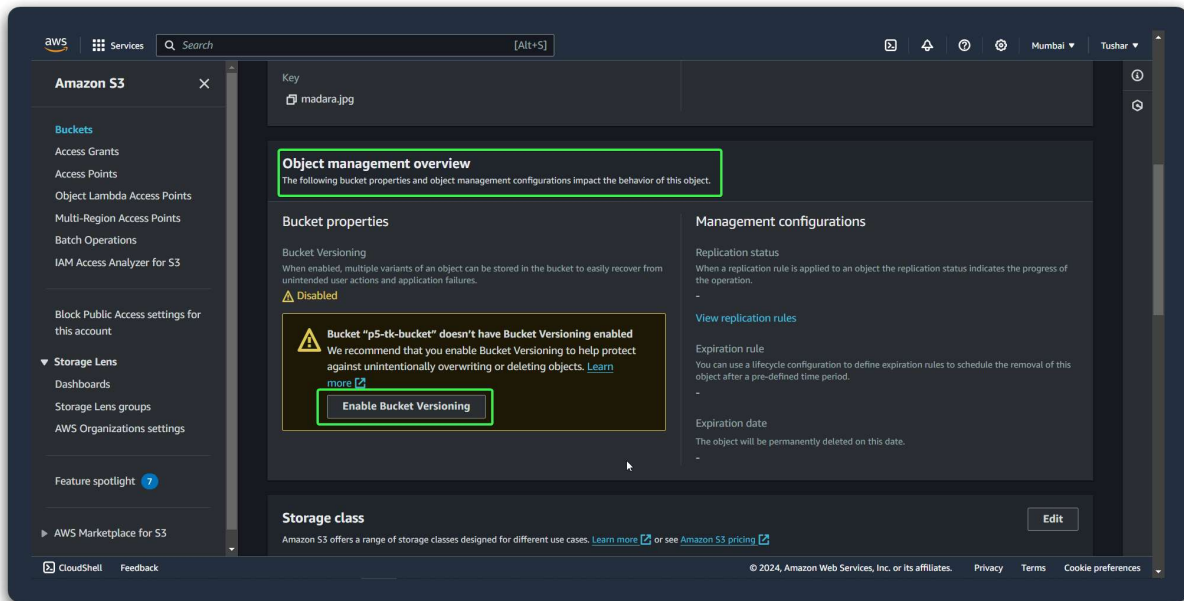
Here you can see we get this type of policy to paste it in bucket policy with changes in resources add **/* in the last of resources**



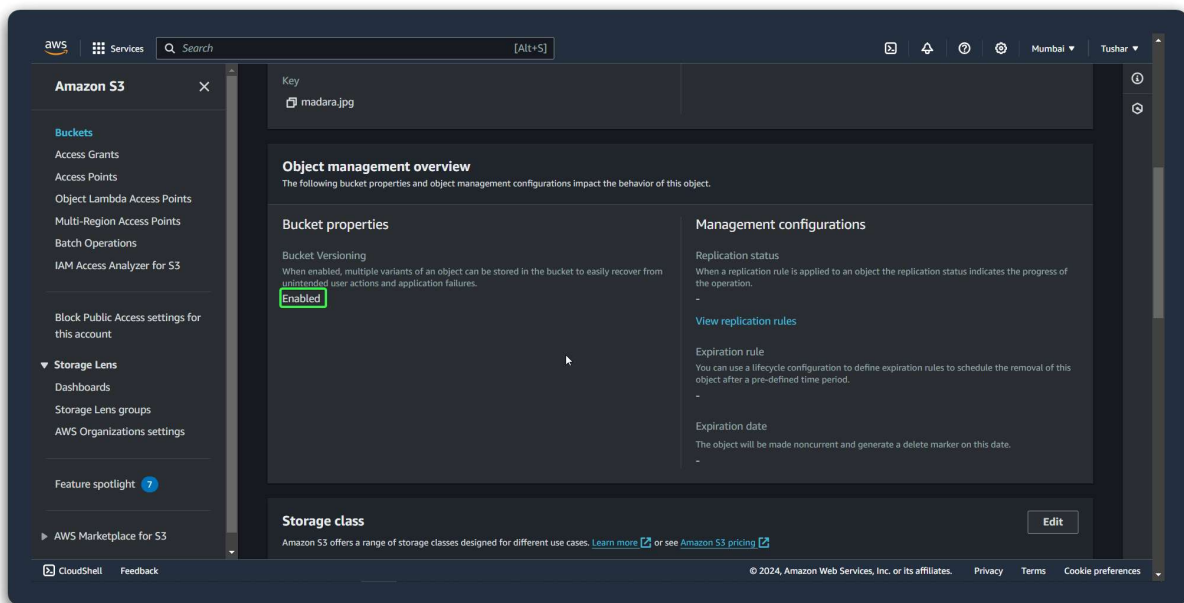
Now after making all the changes you can see the images is now seen



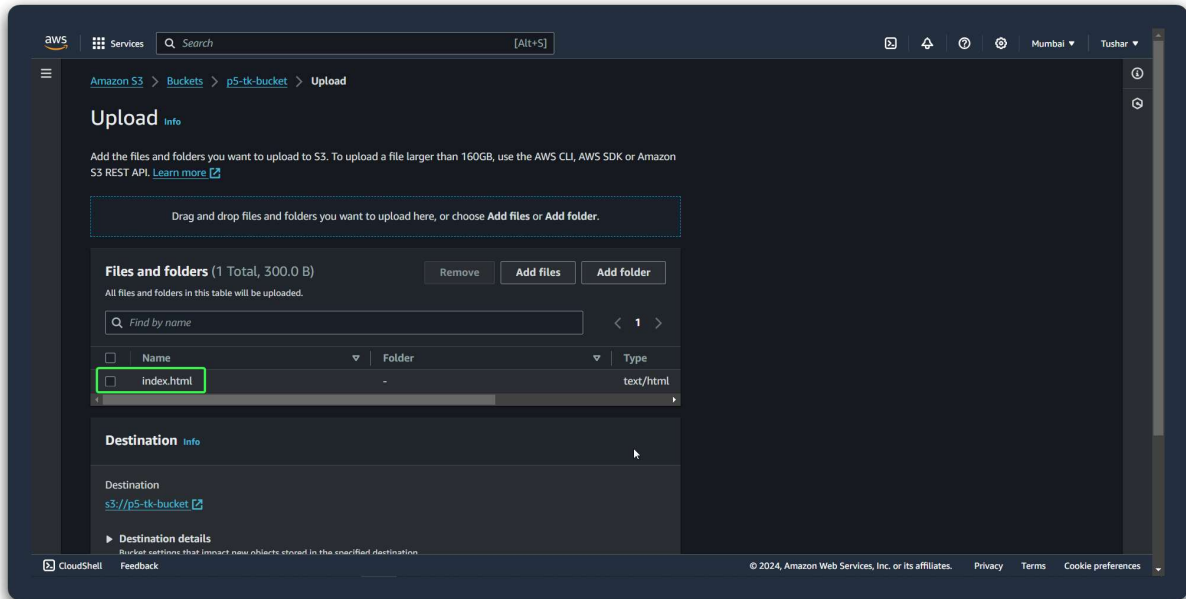
Now enable the Bucket versioning



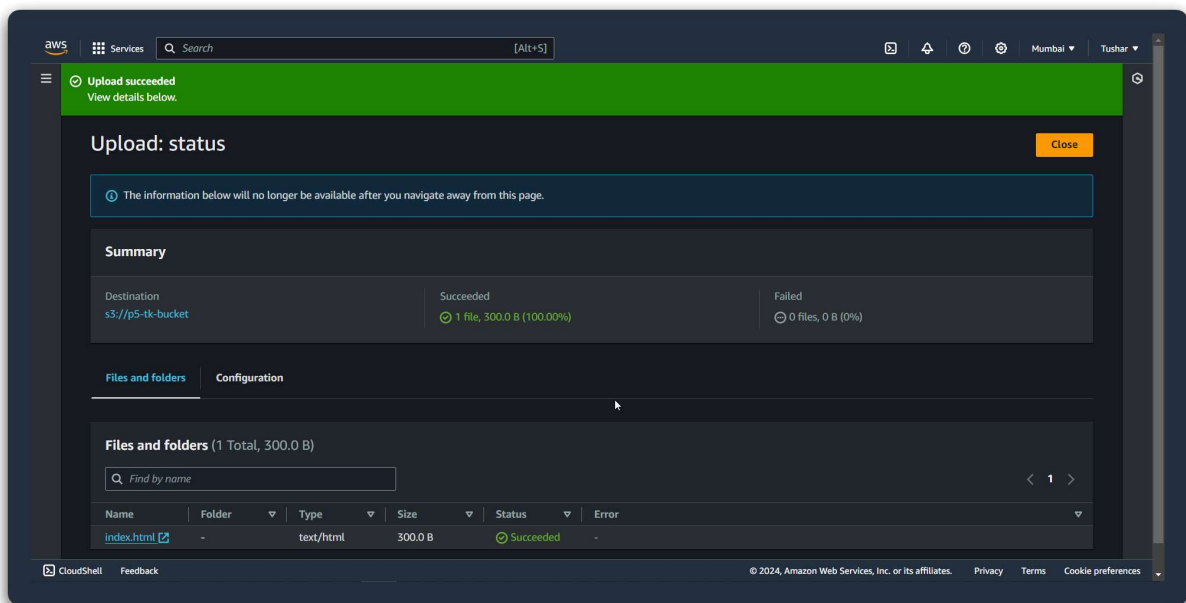
As you can see below Bucket Versioning is enabled



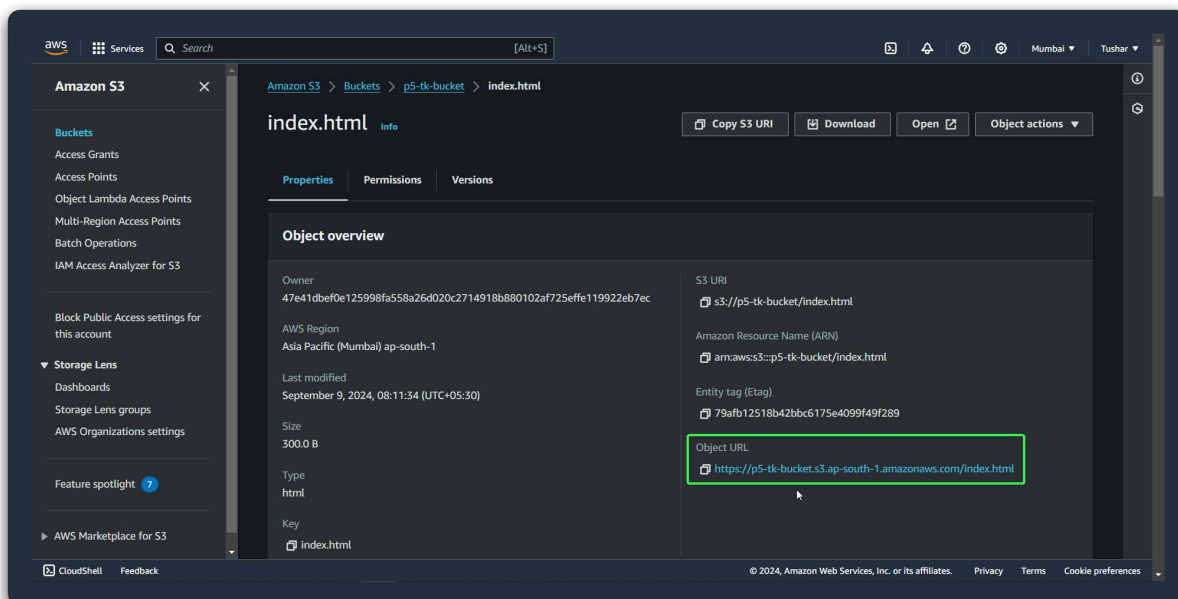
Now you have to upload the index.html



As you can see the index.html is uploaded



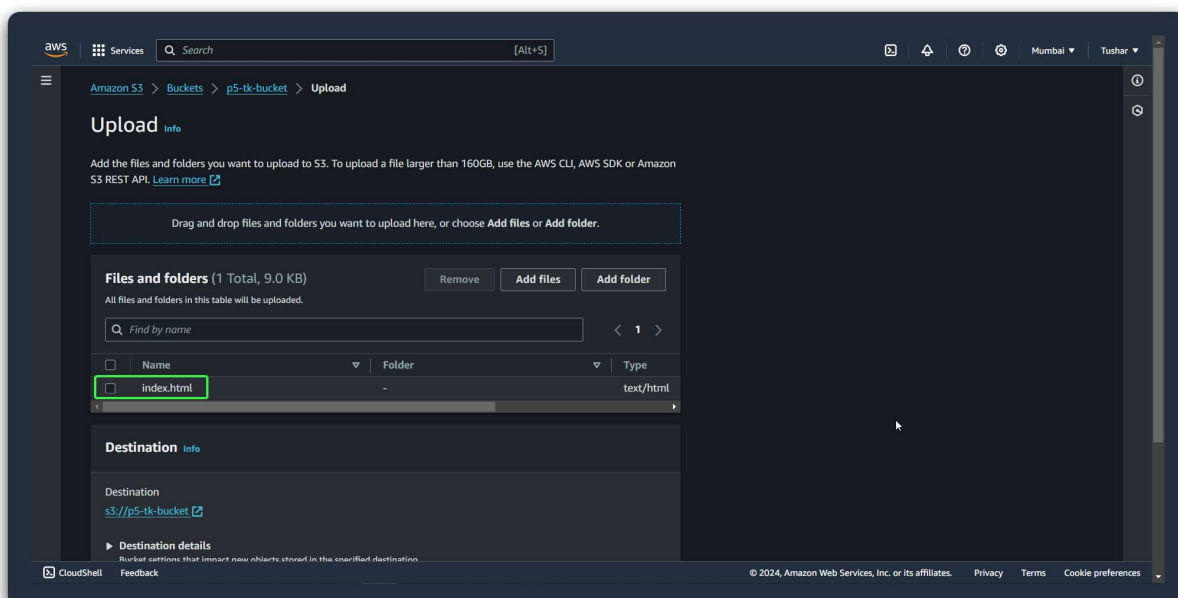
Get access to the index.html from the object url



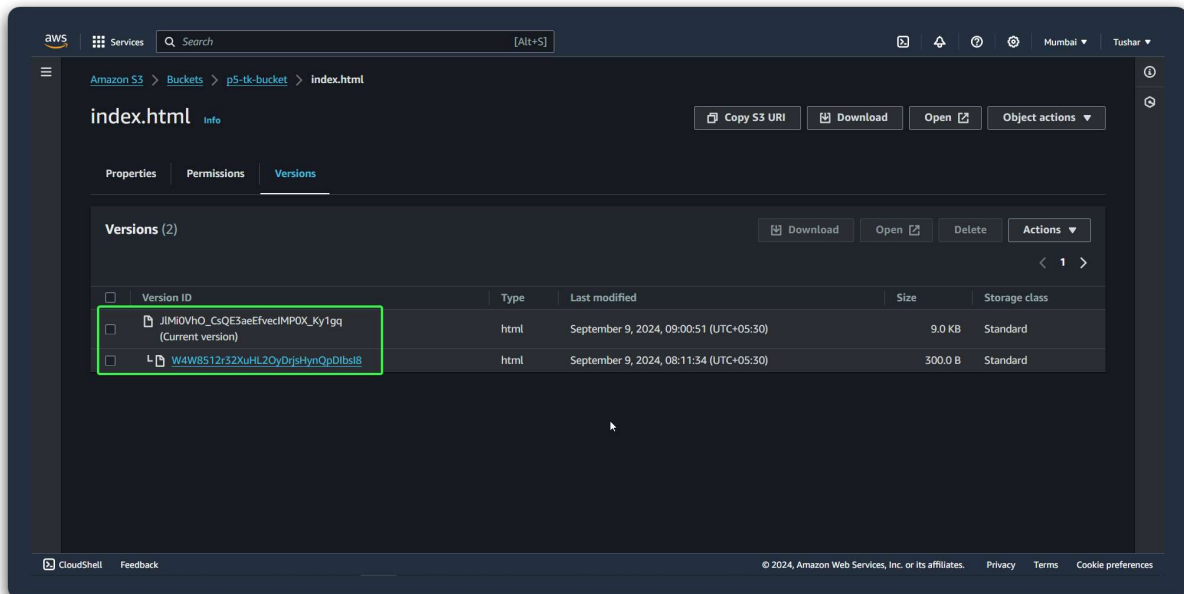
You can see the index.html Output.



Now make some changes in the html file and upload it again with the same name.



As we have enabled the versioning you can see the index.html have the version you can access both the index.html file



Here is the changed HTML file Output

