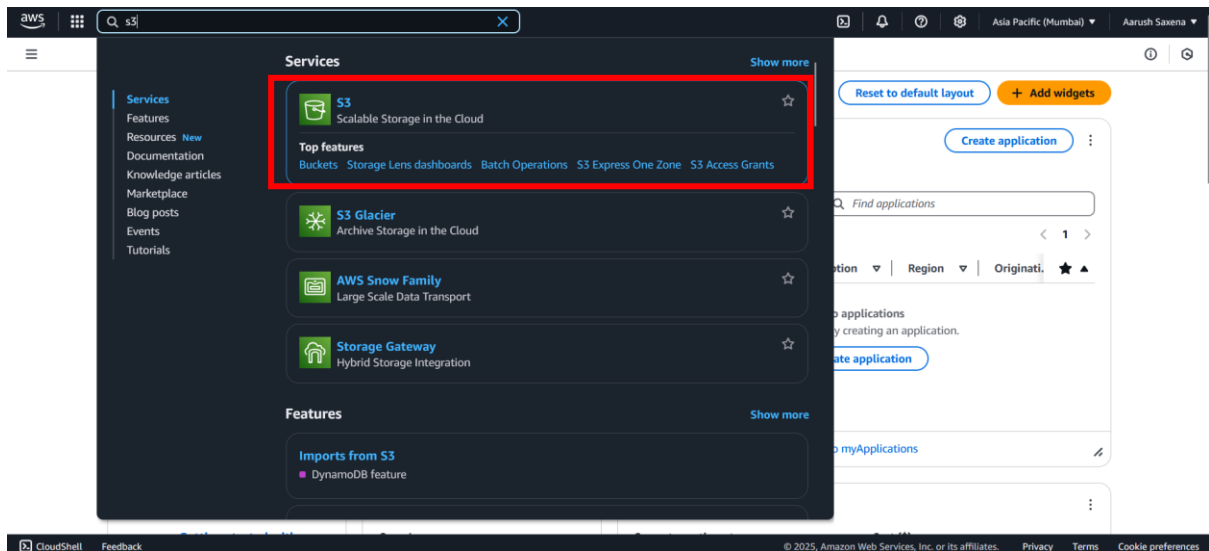
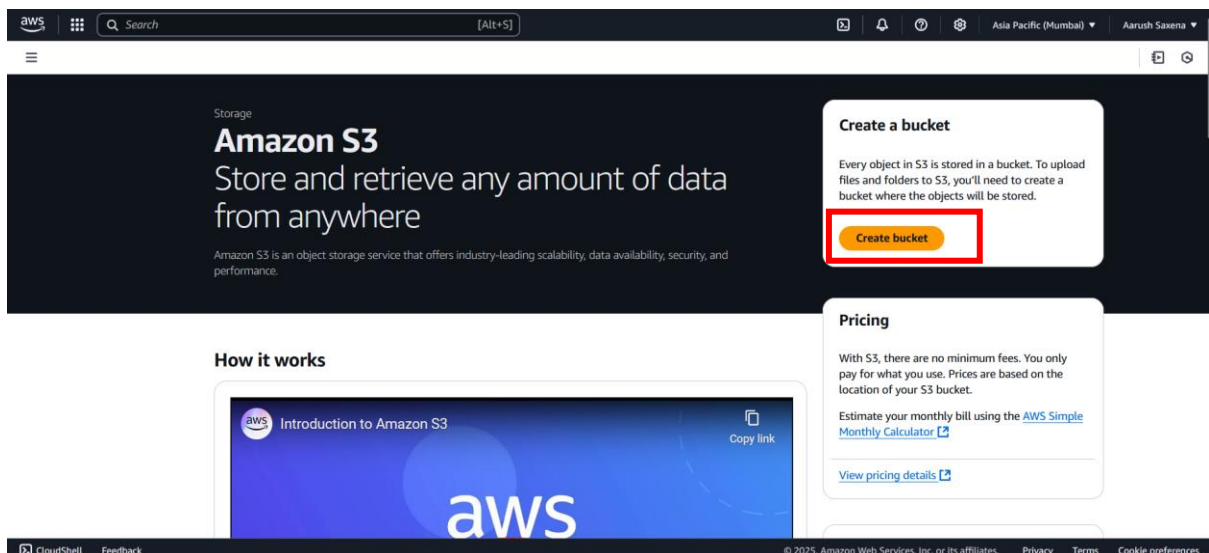


How to create Simple storage service bucket(S3) And Access it's Content Publicly

Step1: Log in to your aws account and through management console go to S3 by searching it on searchbar. As shown in image given below.



Step2: click on Create bucket.



Step3: After clicking on it you will see your console as shown in image given below from there given name to your S3 bucket as unique name which is not present globally. As first I specified it as “sample-bucket” and leave everything to default and clicked on create bucket and you will see it will give an error. So I changed the name of it and click on create bucket.

Create bucket info

Buckets are containers for data stored in S3.

General configuration

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

Bucket type info

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name info

sample-bucket

Bucket names must be unique within the specified region and follow the bucket naming rules. [Get links 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.

For giving block public access makes it super private which helps to access it's data by authorized users.

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 does not 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 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](#)

Bucket Versioning

☒ **Disable**

☐ **Enable**

Tags - optional (1)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key	Value - optional
name	bucketForSamplePurpose

[Add tag](#) [Remove](#)

Default encryption info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type info

☒ **Server-side encryption with Amazon S3 managed keys (SSE-S3)**
Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ **Server-side encryption with AWS Key Management Service keys (SSE-KMS)**
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#)

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ **Disable**

☒ **Enable**

Advanced settings

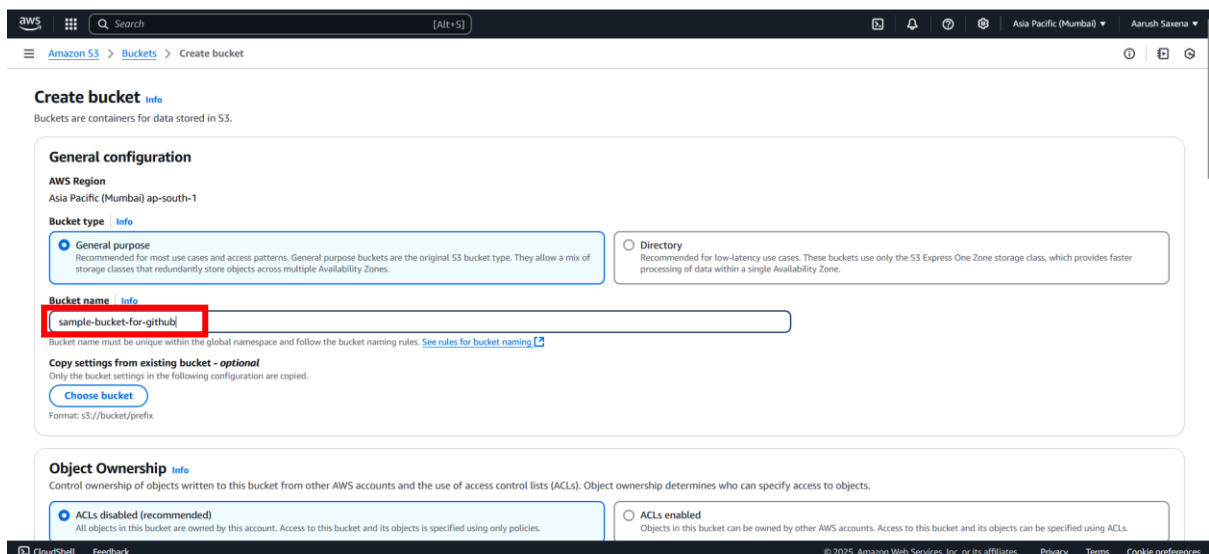
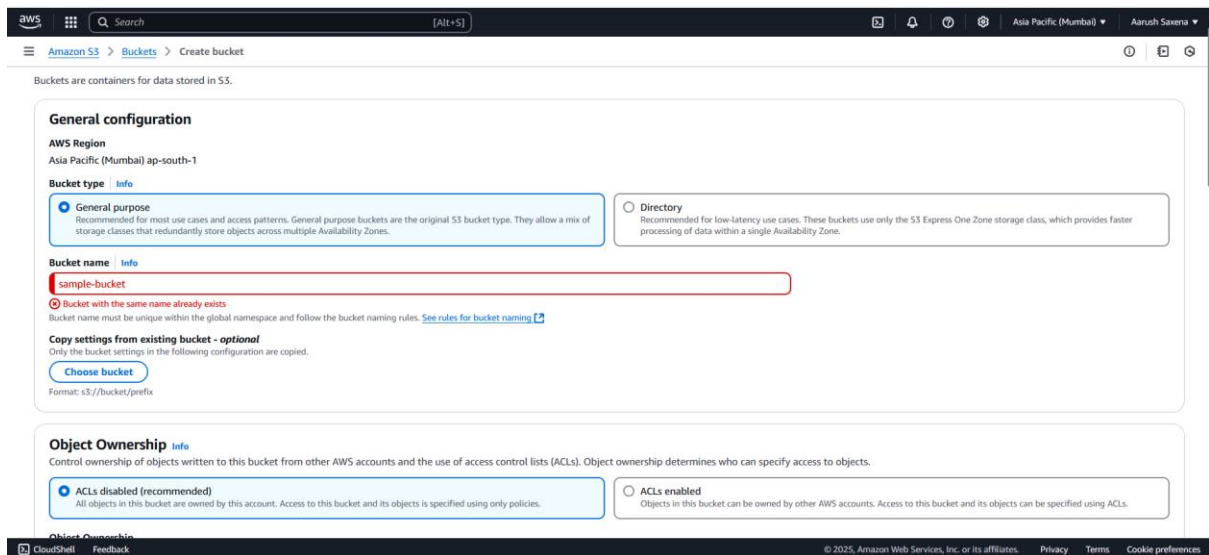
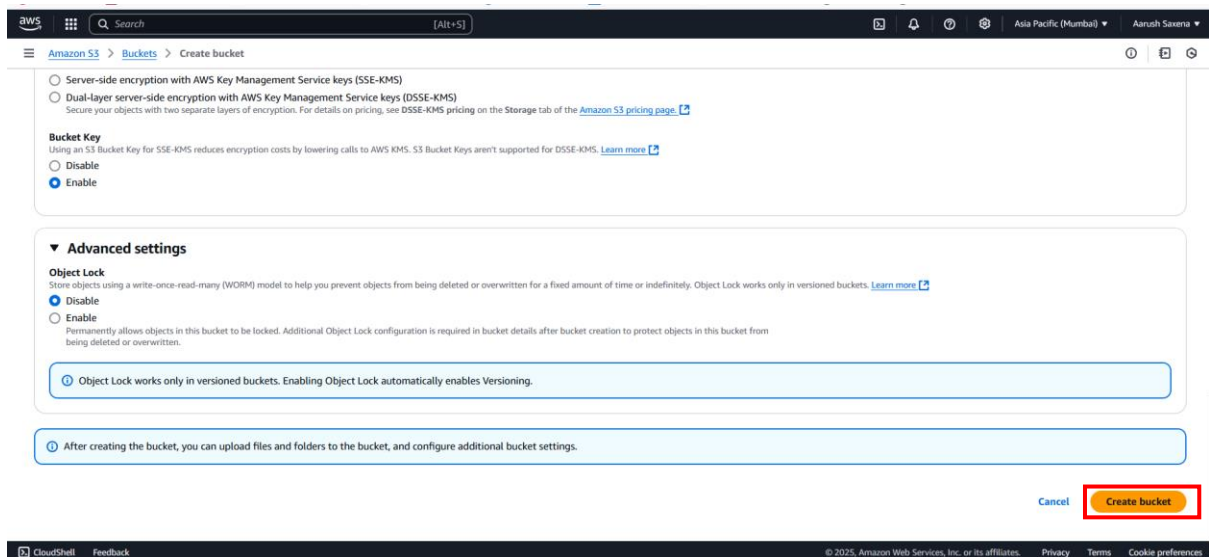
Object Lock
From objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

☒ **Disable**

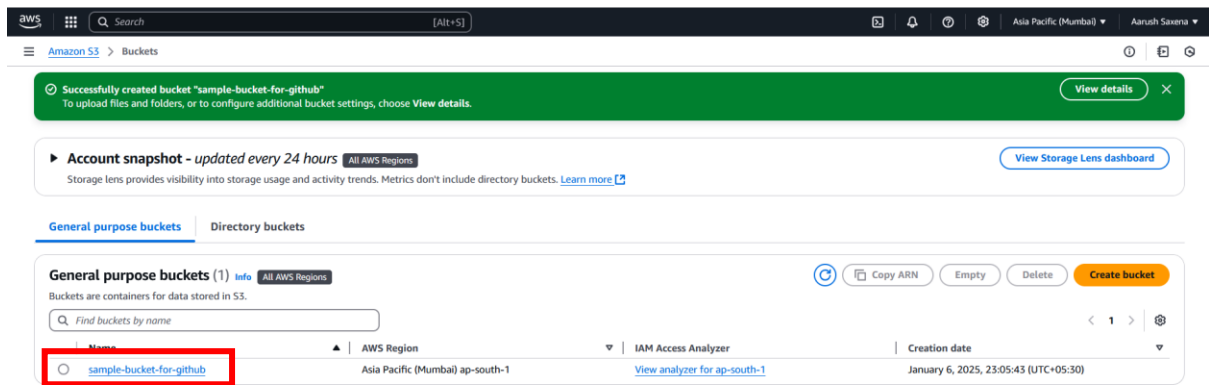
☐ **Enable**
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

☐ **Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.**

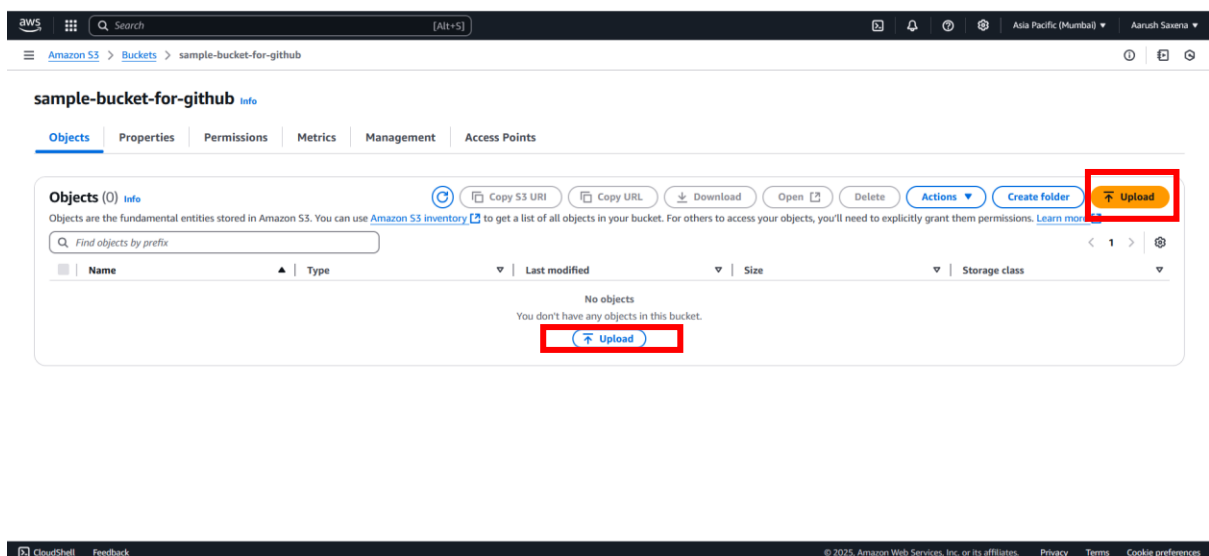
☐ **After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.**



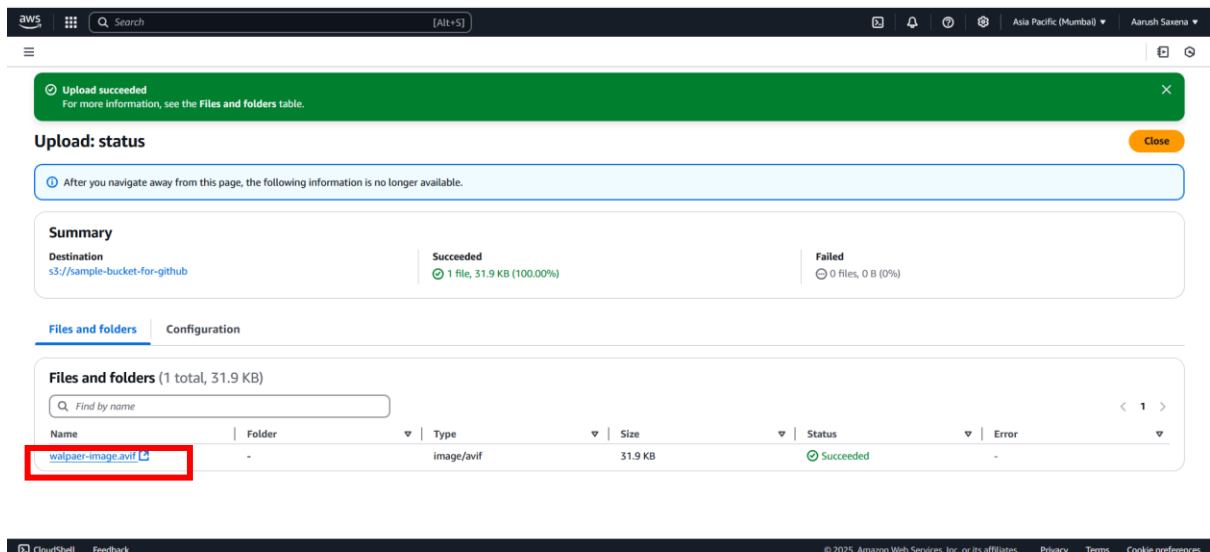
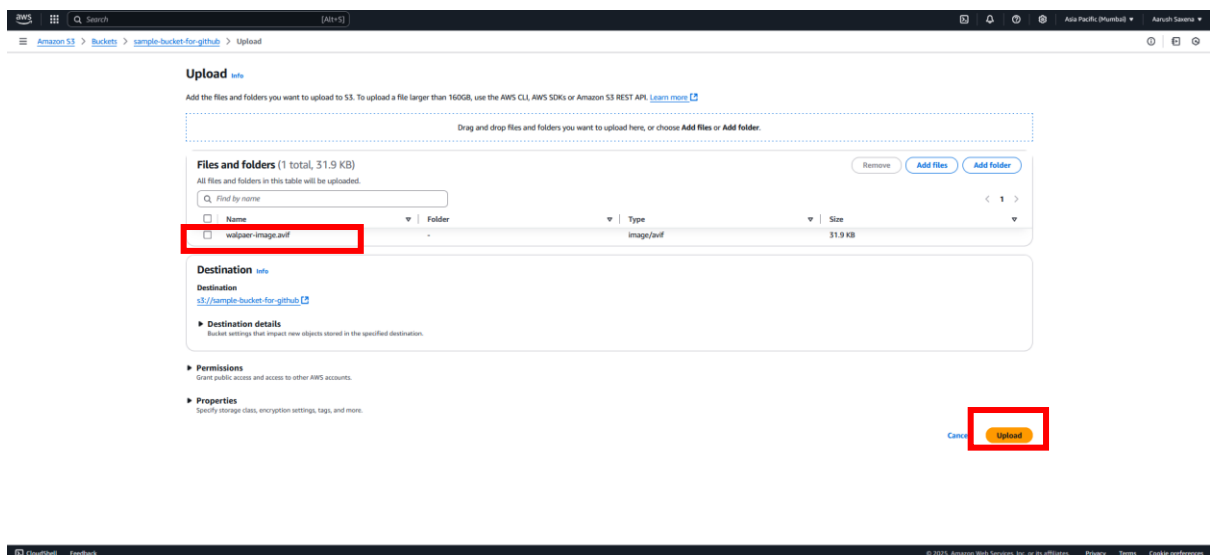
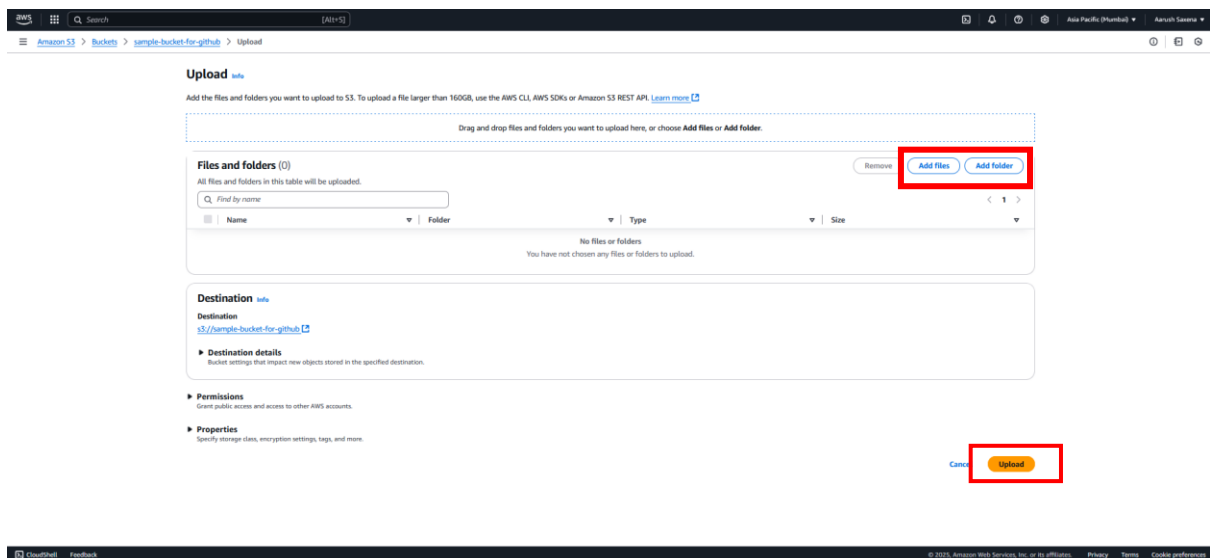
Step4: Now you can see your bucket has been created as shown in image given below. Now click on blue line link.



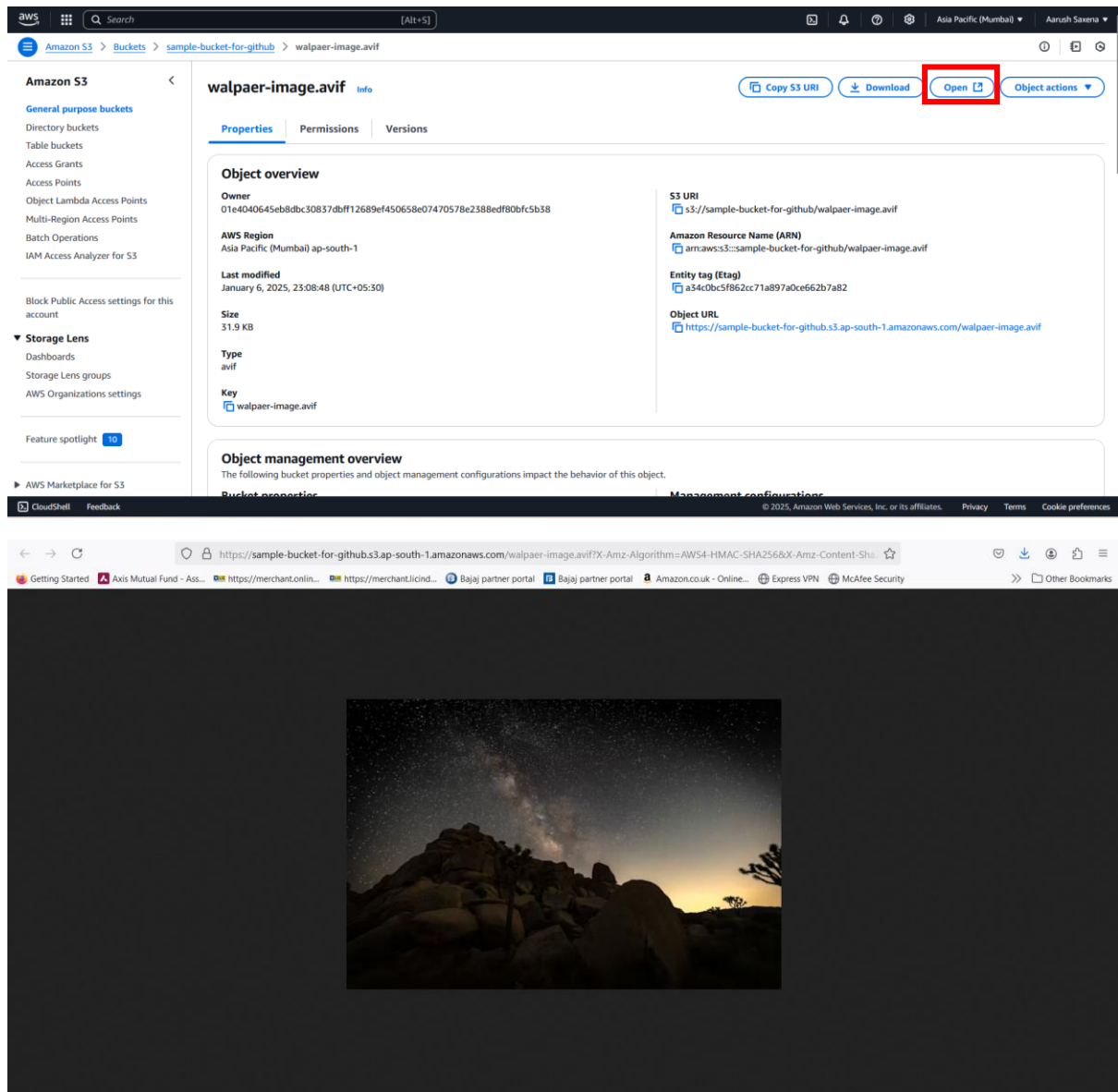
Step5: And you will see window as shown in image given below now to add files or folders to your bucket click on Upload. And you can perform drag and drop also.



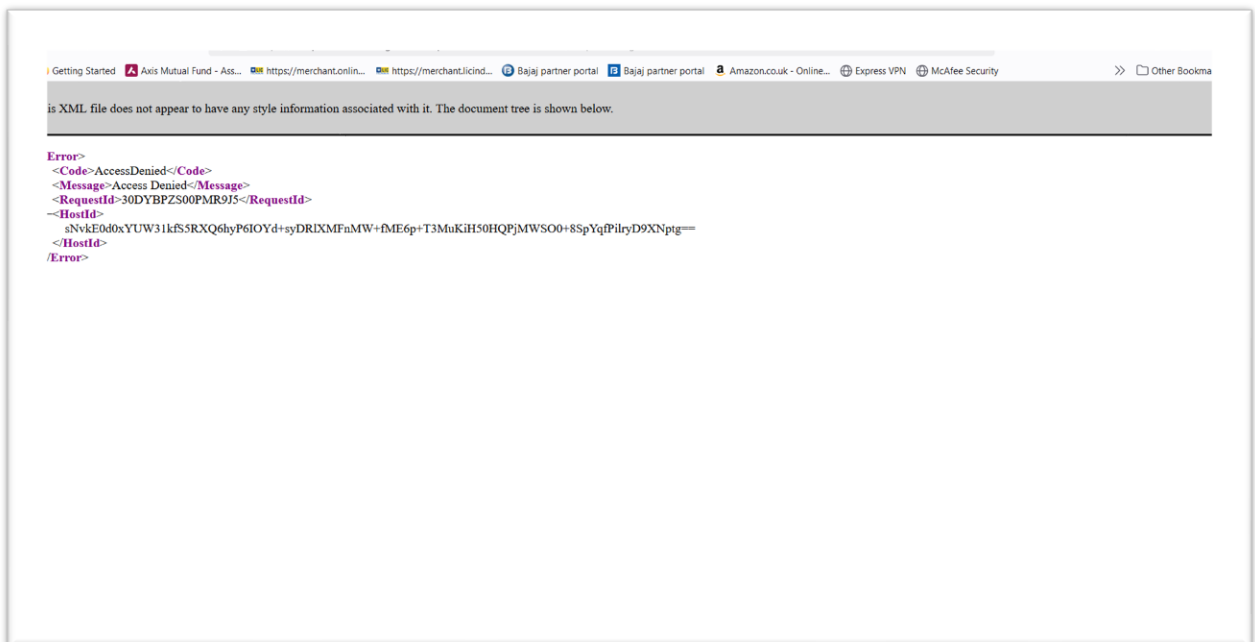
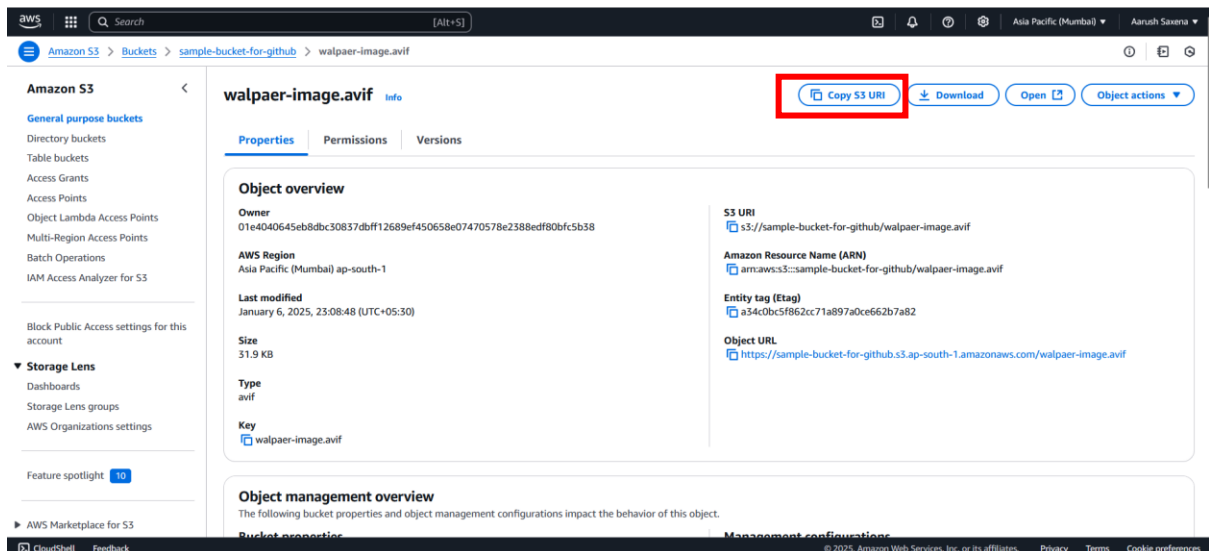
After clicking on it you will see window as shown in image given below from there click on add file or add folder or do drag and drop. After that click on upload.



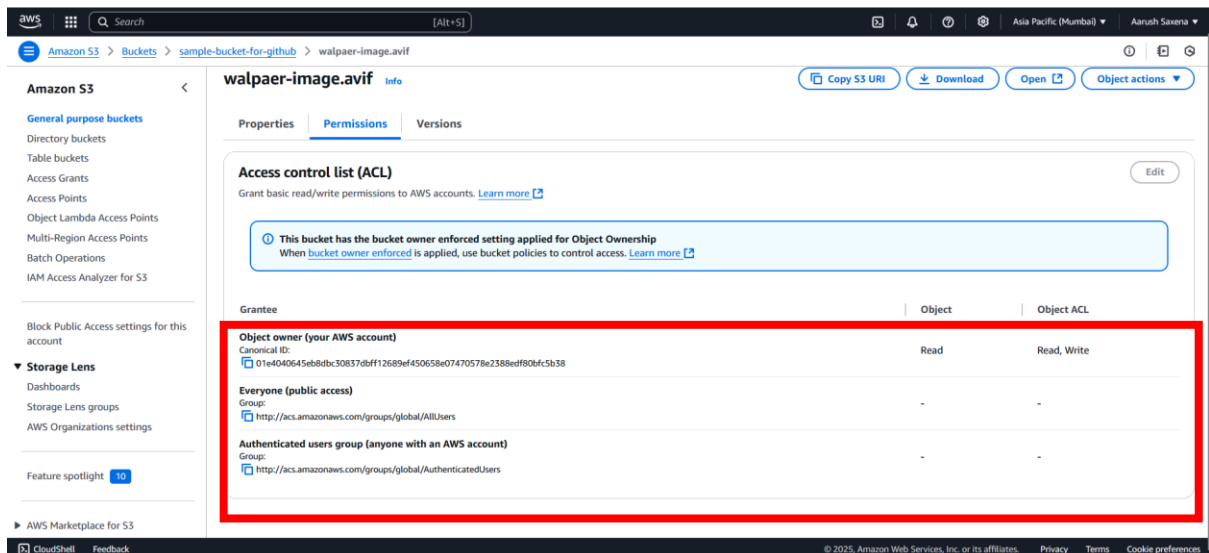
Step6: click on walpaer-image and you will see window as shown in image given below. And from there click on open button and you will see your uploaded file content.



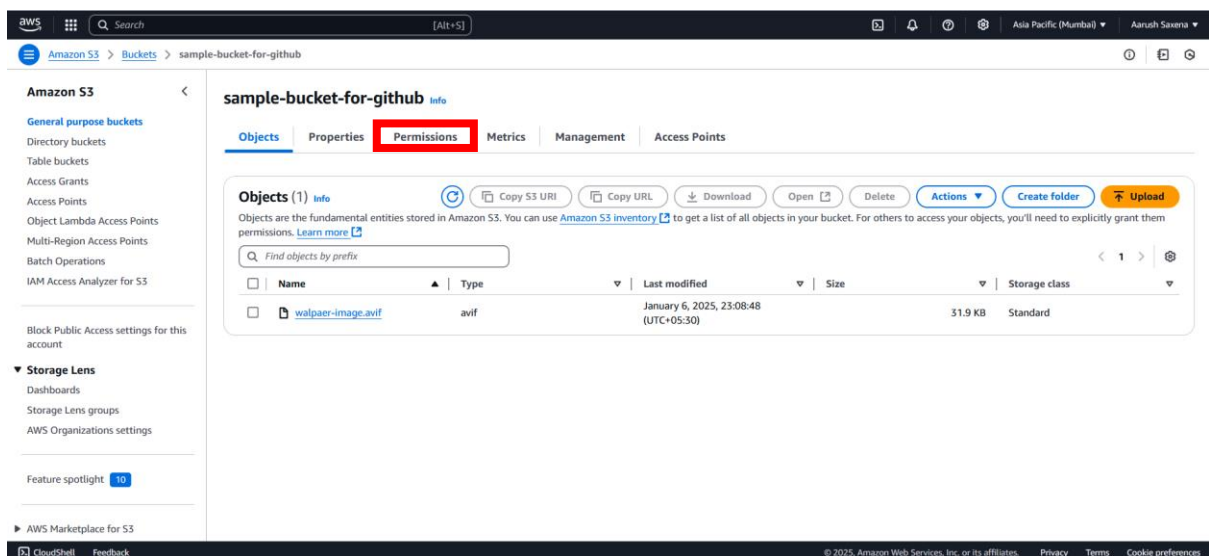
But If you try to access your data through S3 URI you will get an error as shown in image given below to overcome that follow Step7.



Step7: Now Go back to walper-image-avif file or folder and click on Permission option as shown in image given below and you will see the permission of files.

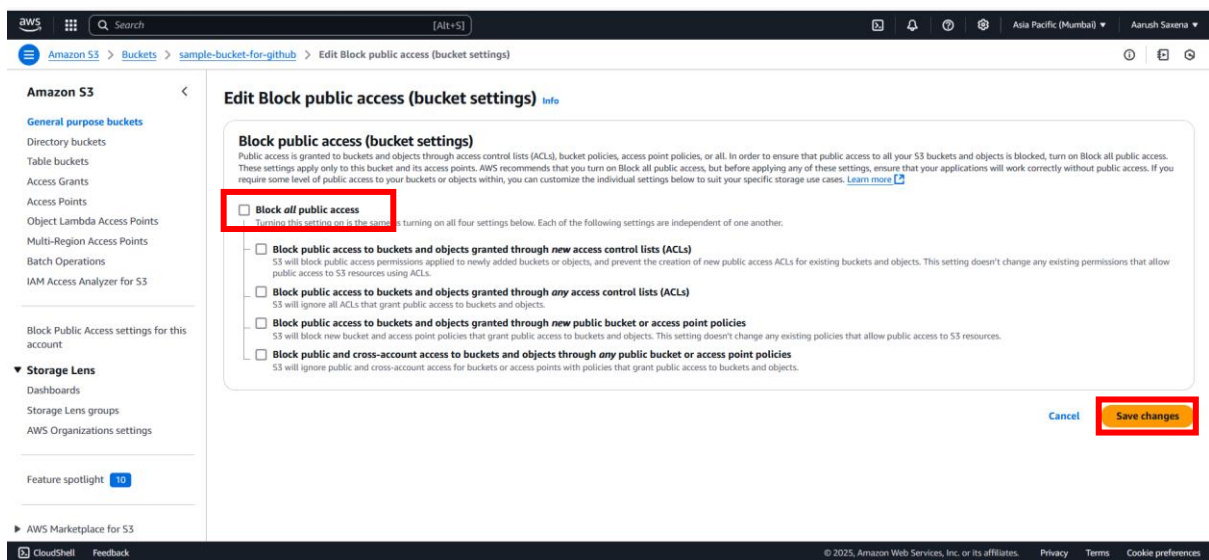
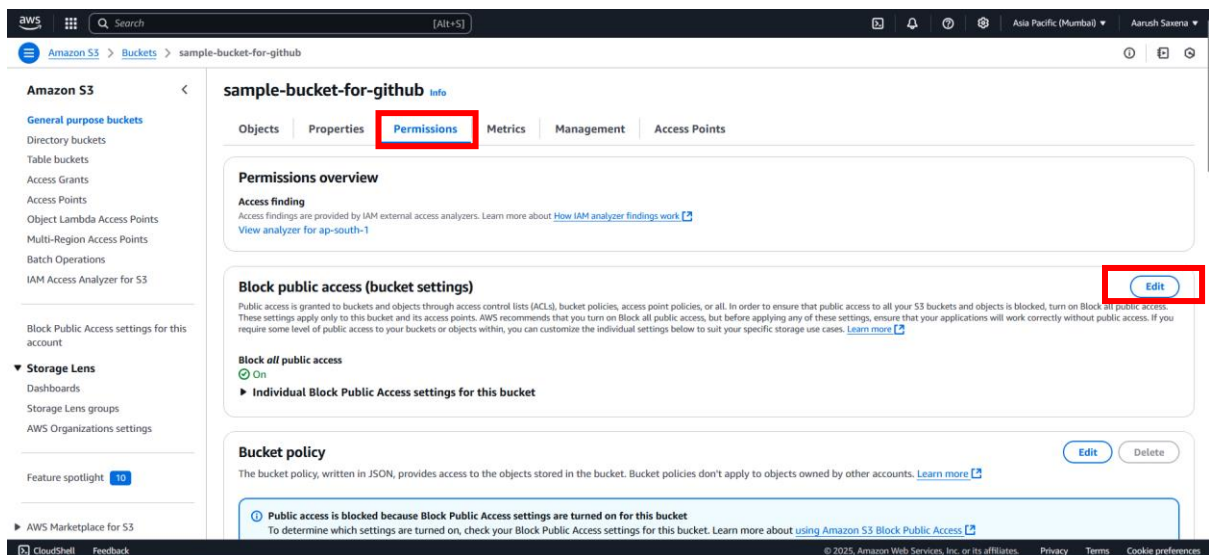


Step8: Now go come to this window as shown in image given below or under your bucket where you store your file and click on permissions option.

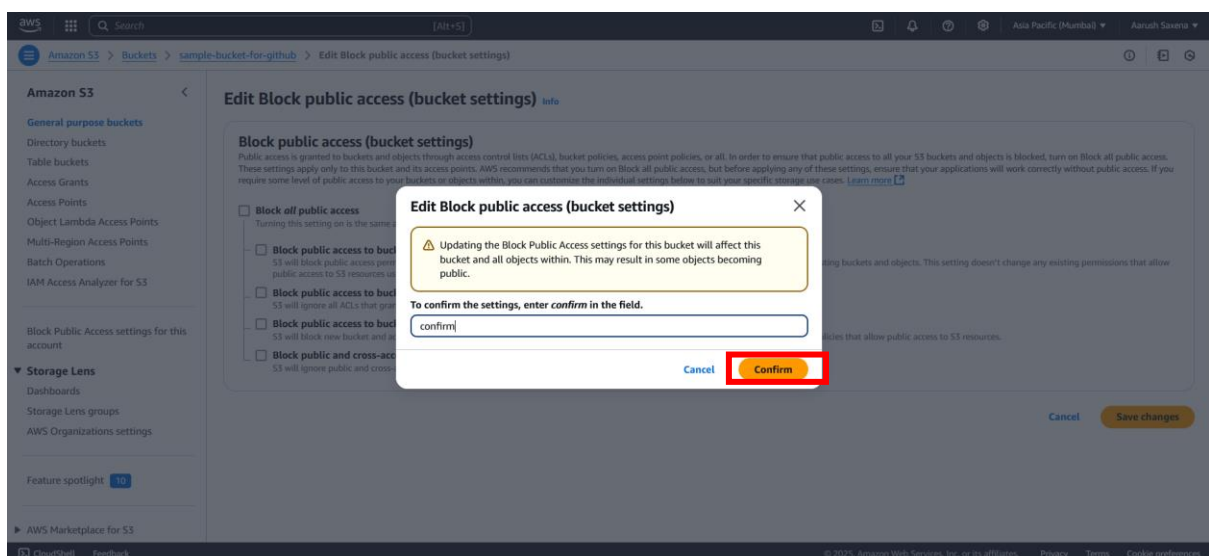


After clicking on permissions click on block public access edit button and uncheck the block public access permission.

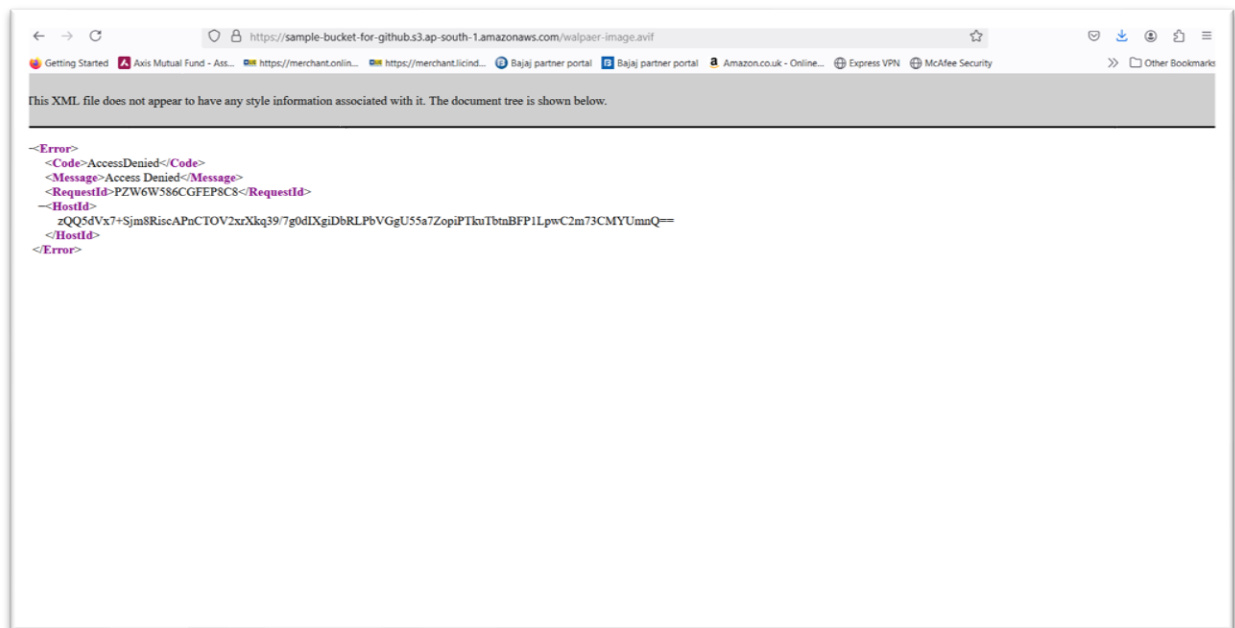
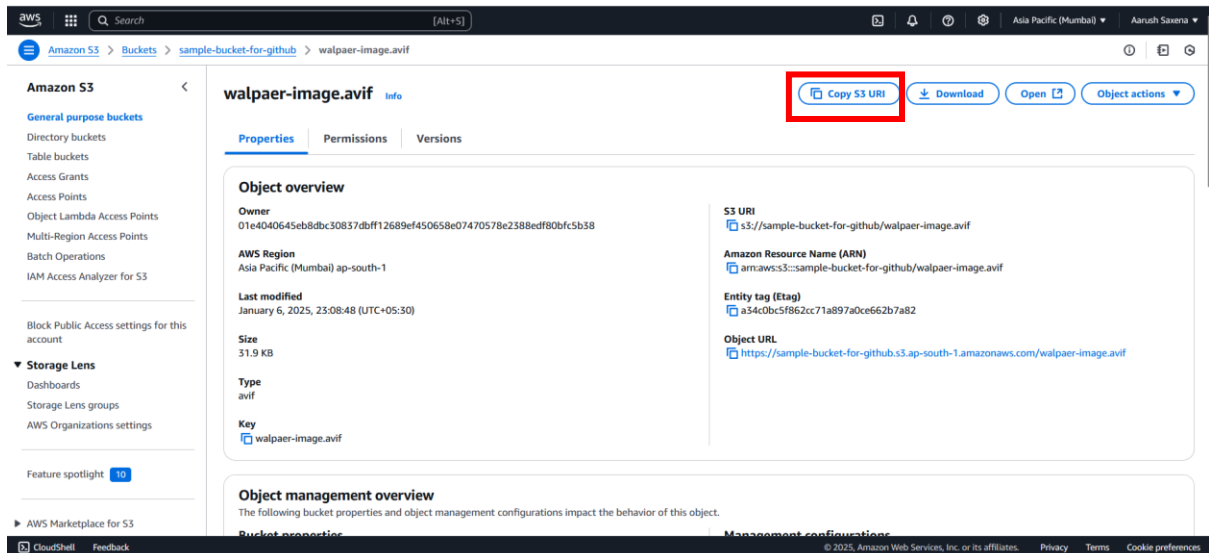
As shown in image given below.



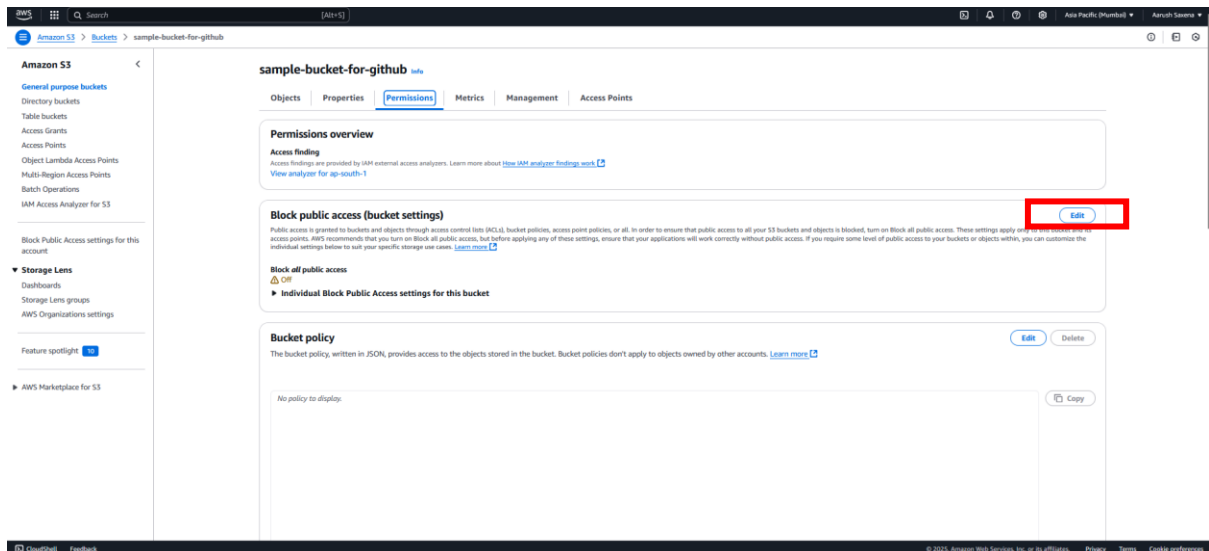
After clicking on save changes a pop will appear as shown in image given below and type confirm to it and click to confirm button.



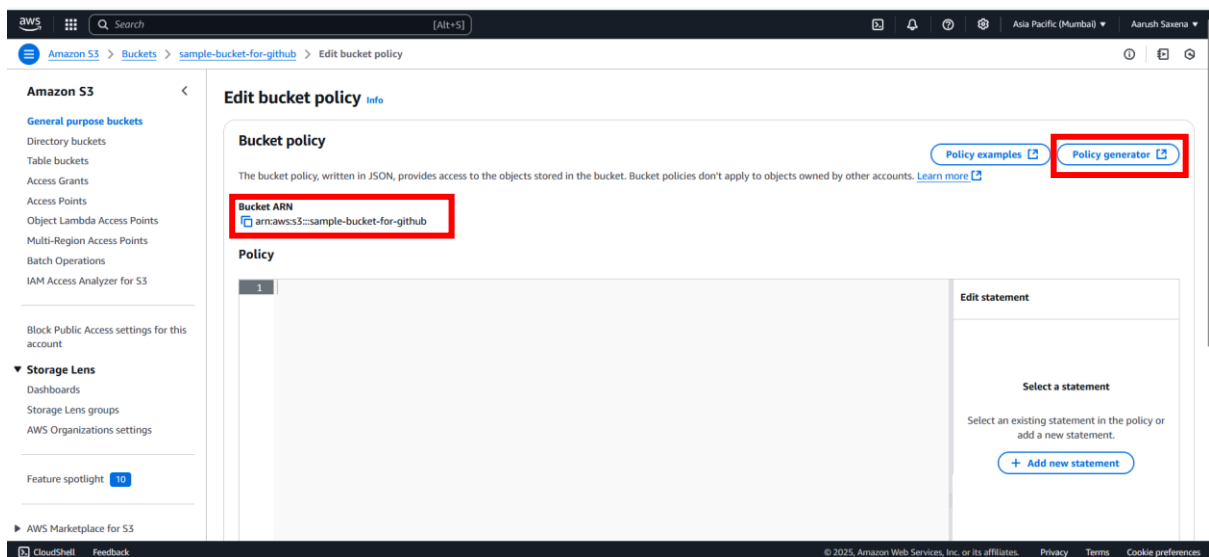
Now if you go back to your file and try to copy S3 URI and paste it to tab and try to access it again go get an error to remove that error follow Step9.



Step9: Go back permission options and click on bucket policy edit button as shown in image given below.




After that if you know how to type policy you can simple write it but right now we are going to generate policy button and remember to copy bucket arn



Now you will see a window as shown in image given below from the drop down click on S3 bucket, on principle placeholder type * (asteric) which tells to provide permission for all, after that on actions click on get object dropdown so that we can access data of Bucket publicly after that paste ARN which we copied and click on Add statement button. It will create policy by clicking on generate policy copy that and follow Step10.

← → ↺ https://awspolicygen.s3.amazonaws.com/policygen.html

Getting Started Axis Mutual Fund - Ass... https://merchant.onlin... https://merchant.licind... Bajaj partner portal Bajaj partner portal Amazon.co.uk - Online... Express VPN McAfee Security >> Other Bookmark



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

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 SQS Queue 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 SQS ☐ 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:sqs:$(Region):$(Account):$(QueueName)`.
Use a comma to separate multiple values.



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

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 SQS Queue Policy
SQS Queue Policy
S3 Bucket Policy
VPC Endpoint Policy
IAM Policy
SNS Topic 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 SQS ☐ 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:sqs:$(Region):$(Account):$(QueueName)`.
Use a comma to separate multiple values.

Permissions

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::sample-bucket-for-github	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.

©2019, Amazon Web Services LLC or its affiliates. All rights reserved.

An amazon.com company

AWS ServiceAmazon S3

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

Actions

-- Select Actions --

All Actions (*)

Amazon Resource Name (ARN)

You added the

Principal(s)

* *

Step 3: C

A policy is a c

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor. Changes made below will not be reflected in the policy generator tool.

```
{
  "Id": "Policy1736185830128",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stat1736185812277",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3::sample-bucket-for-github",
      "Principal": "*"
    }
  ]
}
```

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.

©2019, Amazon Web Services LLC or its affiliates. All rights reserved.

An amazon.com company

Close

Amazon S3

General purpose buckets

Directory buckets

Table buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Bucket ARN

arn:aws:s3::sample-bucket-for-github

Policy

```
1 {
2   "Id": "Policy1736185830128",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stat1736185812277",
7       "Action": [
8         "s3:GetObject"
9       ],
10      "Effect": "Allow",
11      "Resource": "arn:aws:s3::sample-bucket-for-github",
12      "Principal": "*"
13    }
14  ]
15 }
```

Add new statement

JSON Ln 15, Col 1

Security 0 Errors 0 Warnings 0 Suggestions 0

Preview external access

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

Add new statement

Cancel

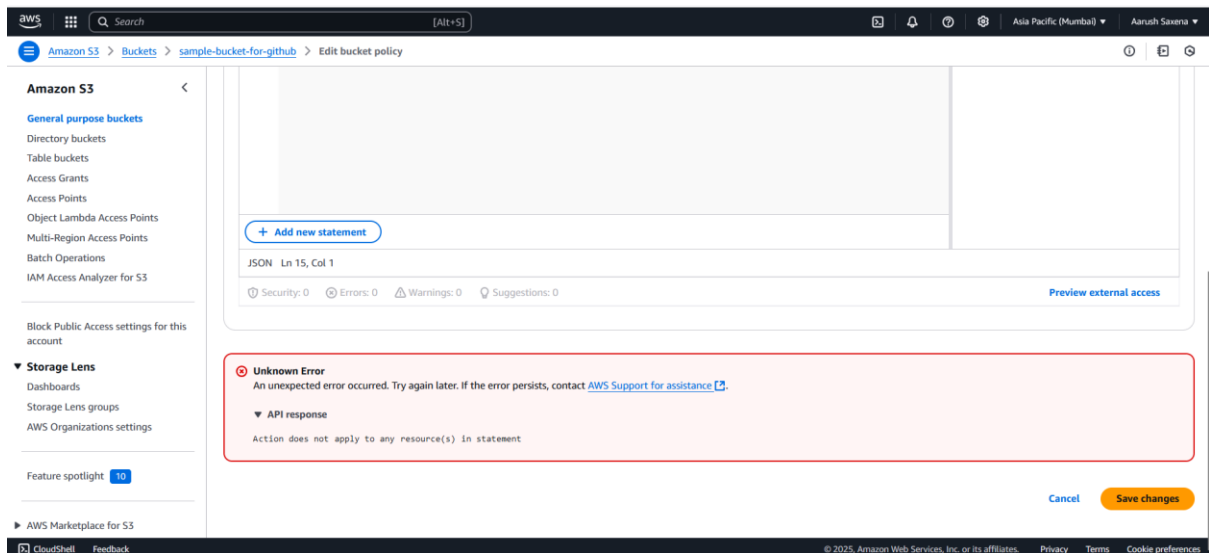
Save changes

CloudWatch

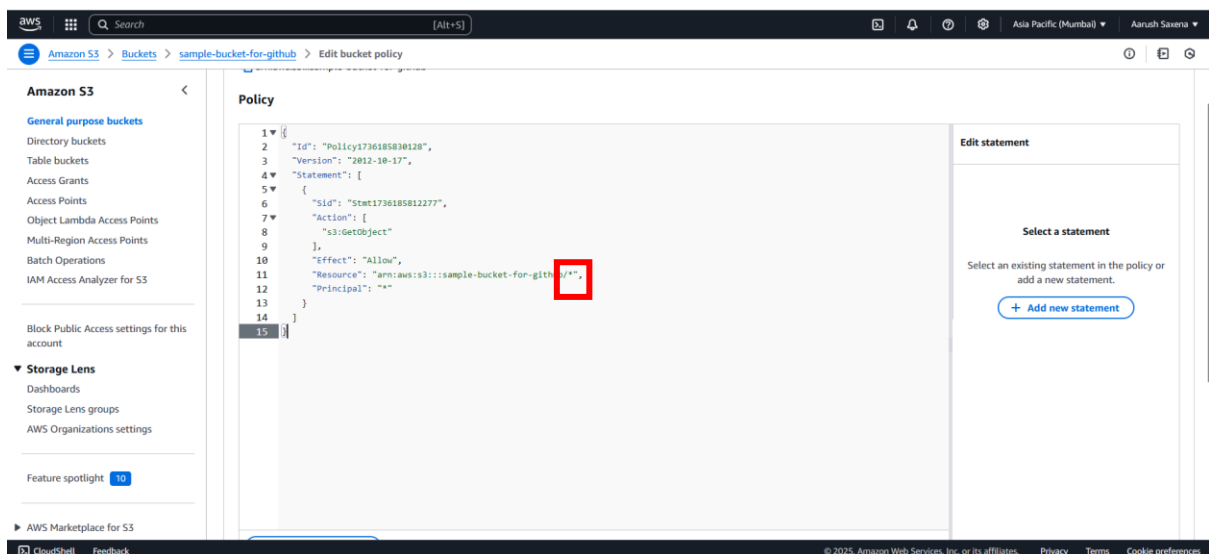
Feedback

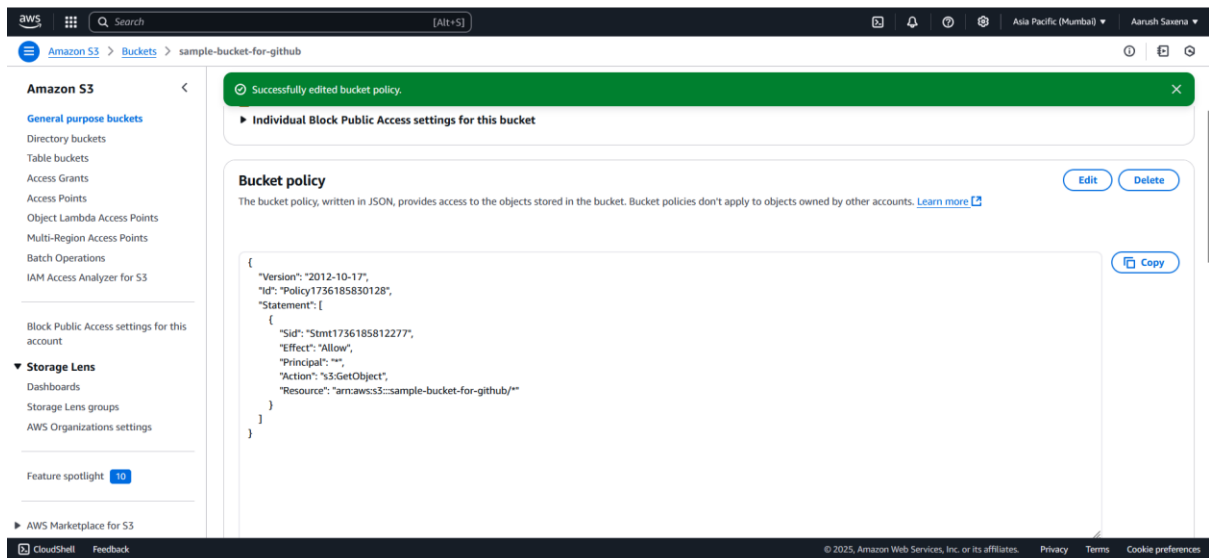
© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Contact us

Step10: Now if you click on save changes it will give an error because if do not specify on which object it have to provide permissions so we will applied on all by “*”.



/* to provide all s3 object and click on save changes





And if you try to copy S3 URI and paste it to tab it will show your content as shown in image given below.

