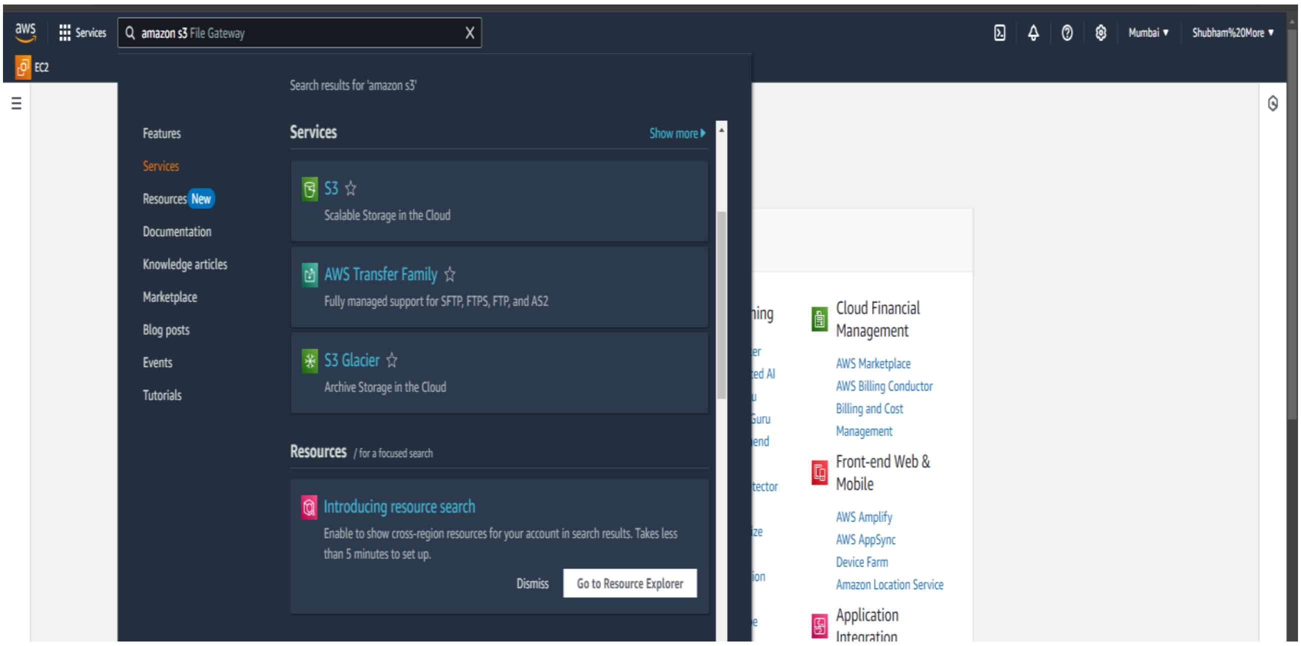
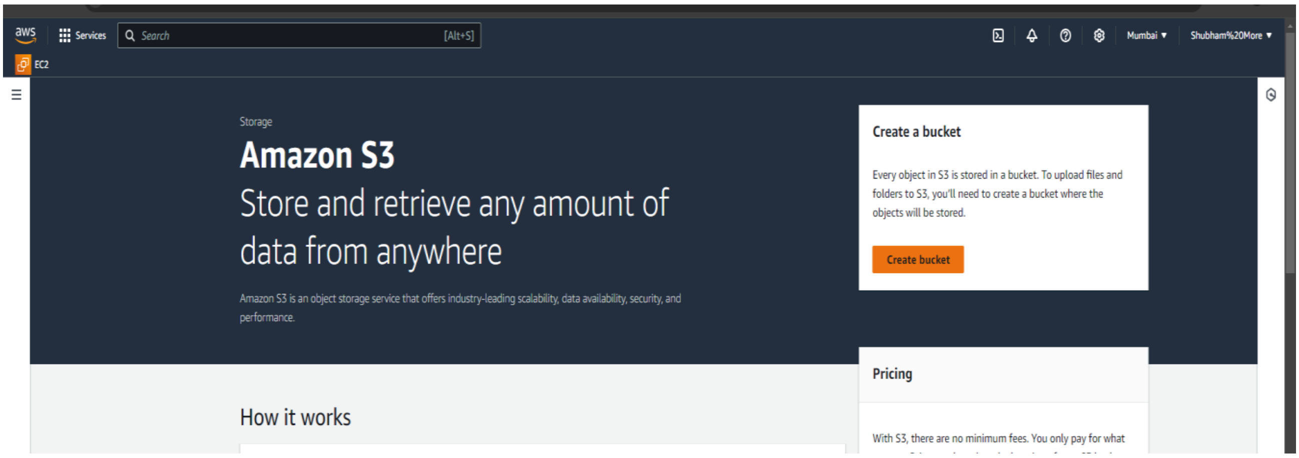
PRACTICAL - 6

Aim : Create a bucket for storing files using S3 in AWS (Simple Storage Service).

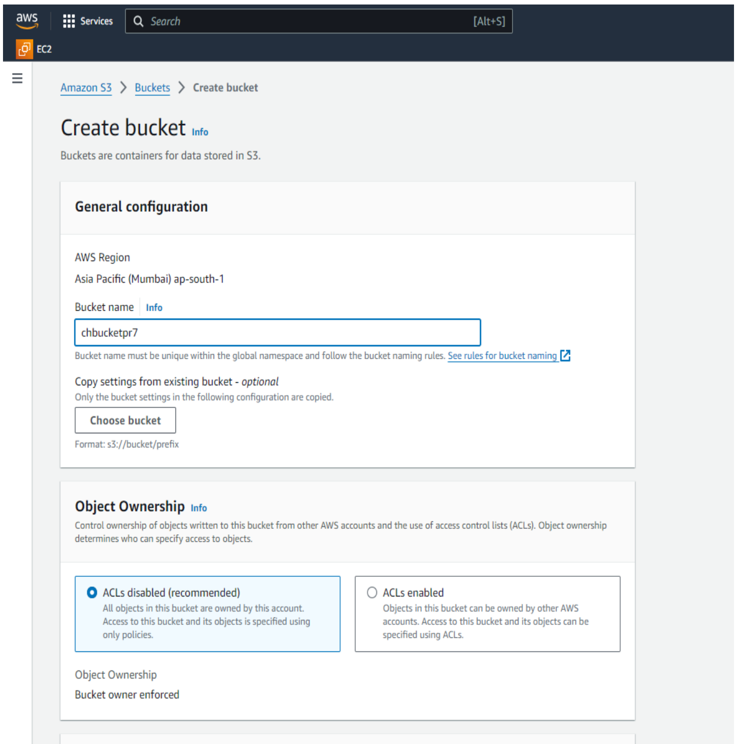
Step 1: In the first step go to services in AWS console and choose S3 service



Step 2: Click on Create bucket.


aws
Services
Search
[Alt+S]
Mumbai ▾
Shubham%20More ▾
EC2
Storage
Amazon S3
Store and retrieve any amount of data from anywhere
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.
Create a bucket
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.
Create bucket
Pricing
With S3, there are no minimum fees. You only pay for what
How it works

Step 3: Give bucket name and keep things as default 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 name Info

chbucketpr7

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.

Format: s3://bucket/prefix

Object Ownership Info

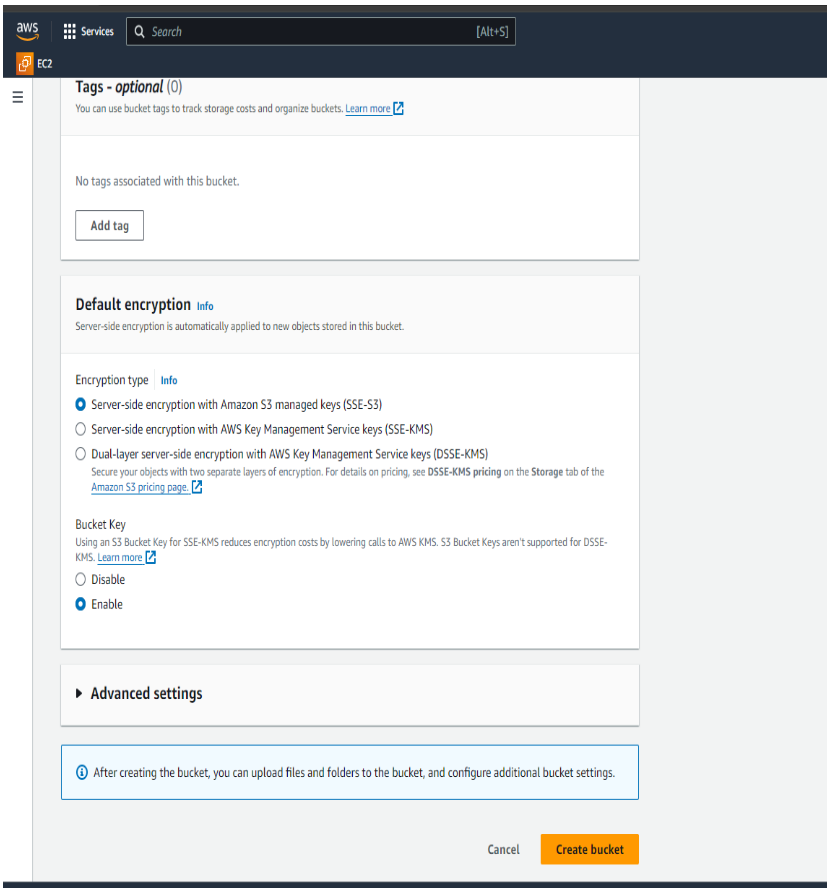
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● 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.

Object Ownership

Bucket owner enforced



Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

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)

○ 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

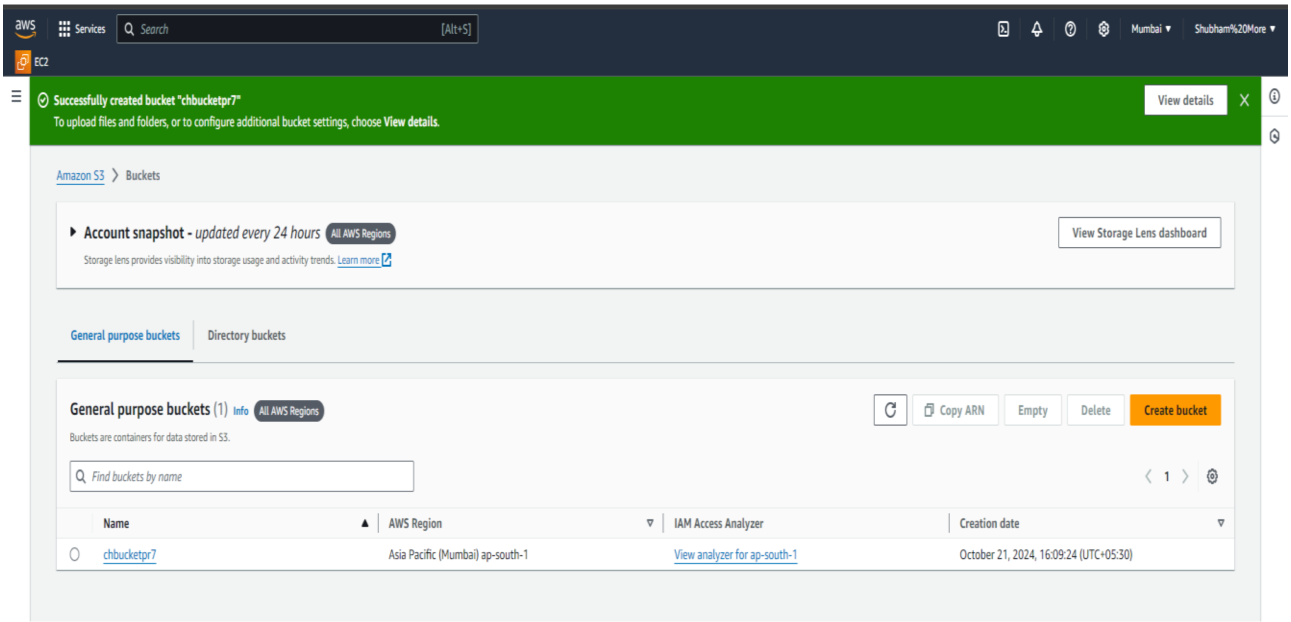
○ Disable

● Enable

▸ Advanced settings

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

Step 4: We successfully created bucket. Now click on bucket name.



Successfully created bucket "chbucketpr7"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

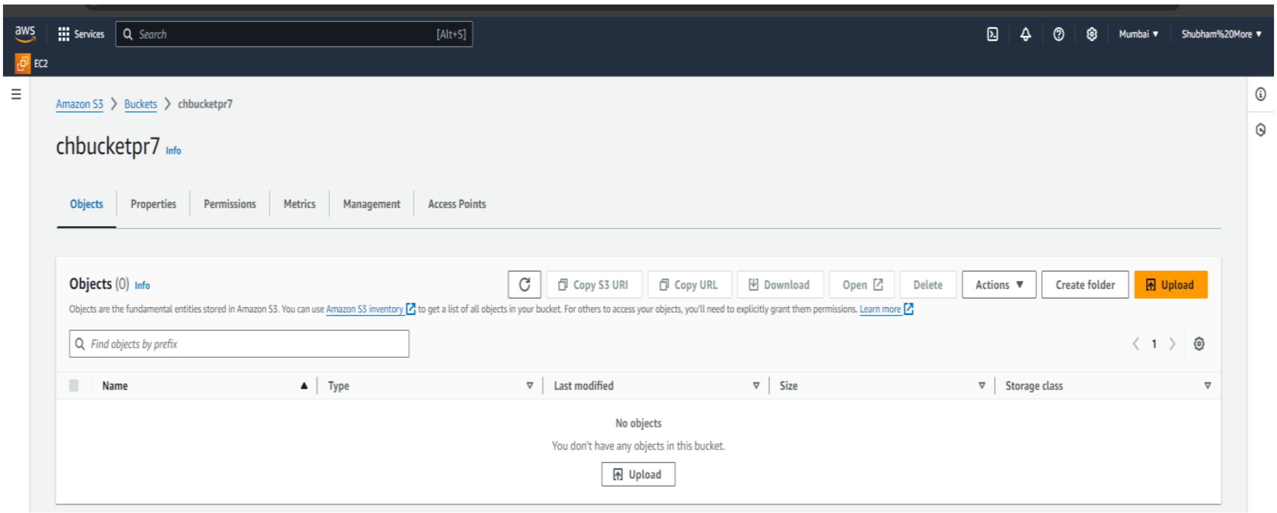
Amazon S3 › Buckets

Account snapshot - *updated every 24 hours* All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info All AWS Regions
Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	chbucketpr7	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	October 21, 2024, 16:09:24 (UTC+05:30)

Step 5: Then Click on Upload to upload any image.



Amazon S3 › Buckets › chbucketpr7

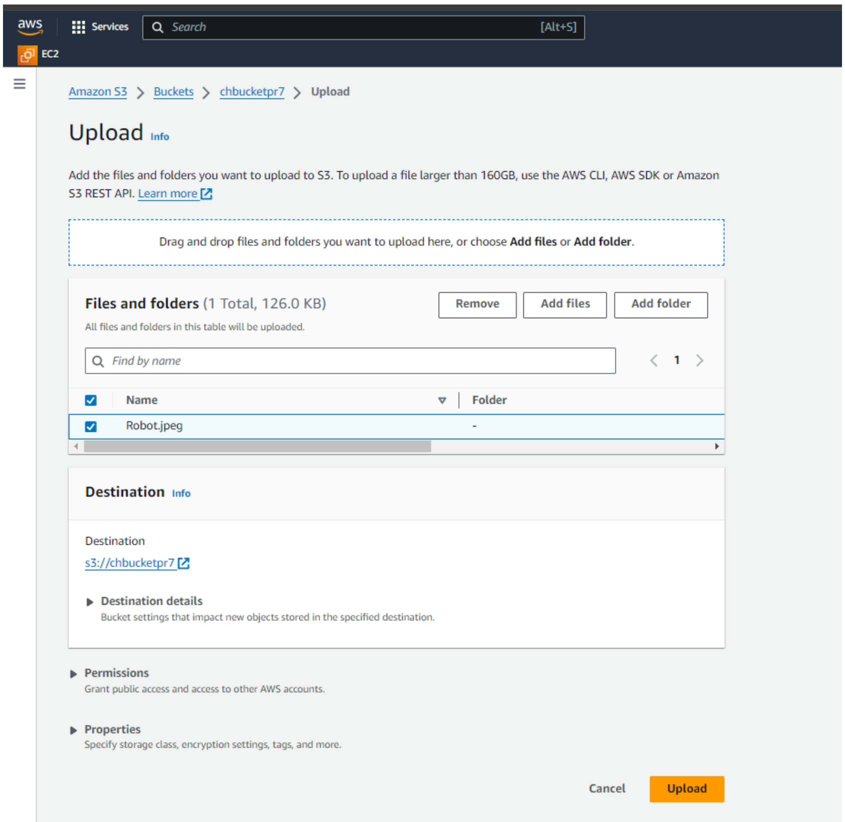
chbucketpr7 Info

Objects (0) Info
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class

No objects
You don't have any objects in this bucket.
Upload

Step 6: Select image and click on upload.



Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 126.0 KB)

All files and folders in this table will be uploaded.

☑	Name	Folder
☑	Robot.jpeg	-

Destination Info

Destination

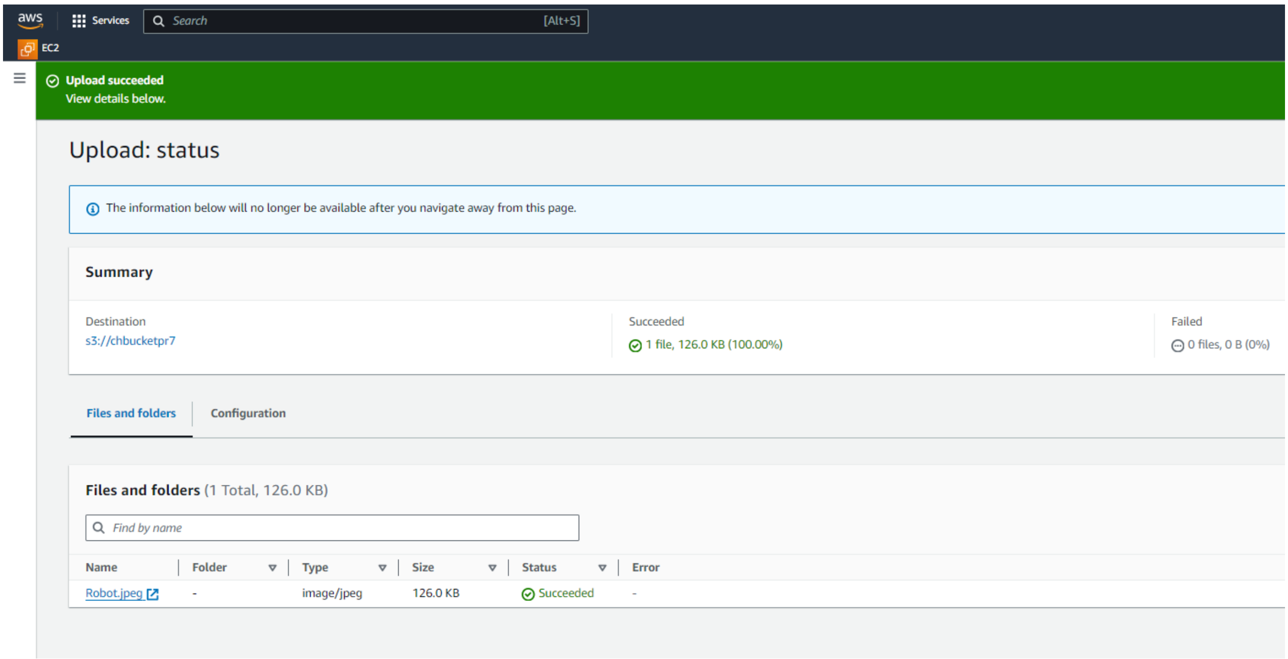
s3://chbucketpr7

▶ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

▶ **Permissions**
Grant public access and access to other AWS accounts.

▶ **Properties**
Specify storage class, encryption settings, tags, and more.

Step 7: Now we have successfully uploaded image file so, click on that image.



Upload succeeded
View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination
s3://chbucketpr7

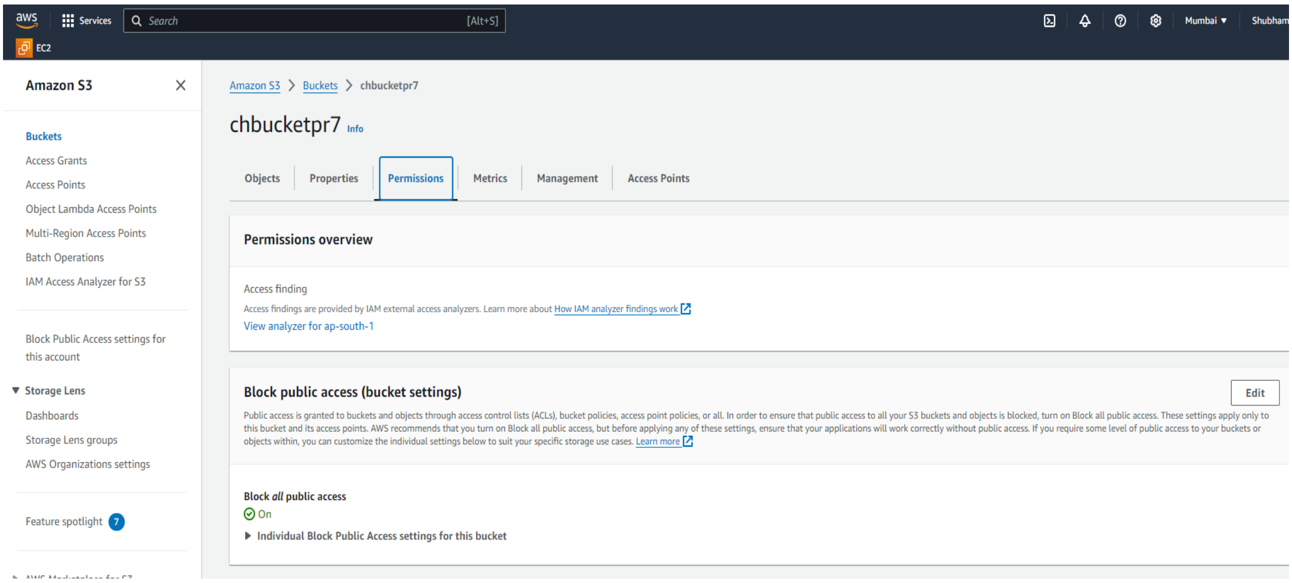
Succeeded
1 file, 126.0 KB (100.00%)

Failed
0 files, 0 B (0%)

Files and folders (1 Total, 126.0 KB)

Name	Folder	Type	Size	Status	Error
Robot.jpeg	-	image/jpeg	126.0 KB	Succeeded	-

Step 8: In this firstly we have to edit Block public access (bucket setting) so, click on edit.



chbucketpr7 Info

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work

View analyzer for ap-south-1

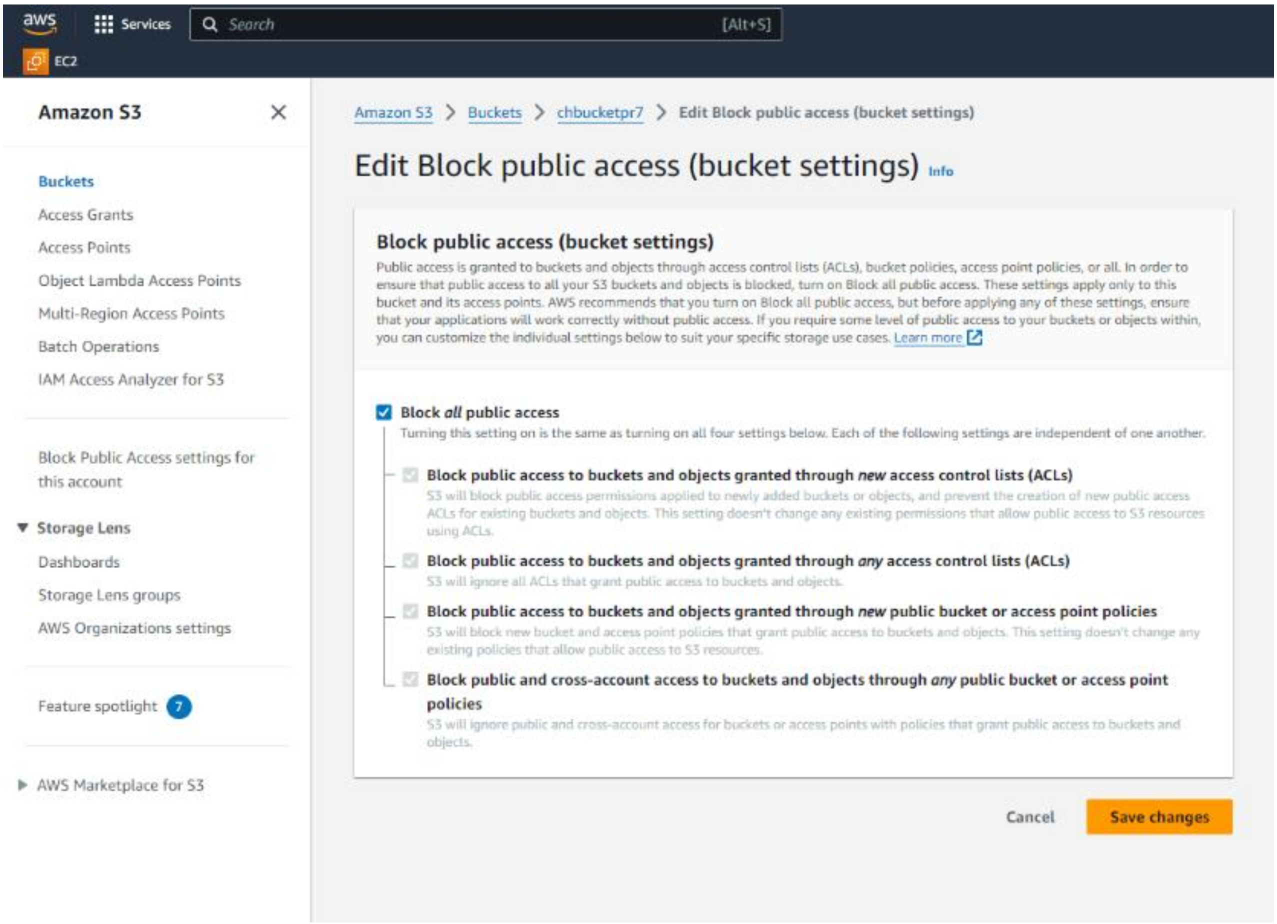
Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block *all* public access
✓ On

▶ Individual Block Public Access settings for this bucket

Step 9 : Uncheck the dialogue box (Block all public access)


aws
Services
Search
[Alt+S]
EC2
Amazon S3
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 7
▶ AWS Marketplace for S3
Amazon S3 > Buckets > chbucketpr7 > Edit Block public access (bucket settings)
Cancel
Save changes

Edit Block public access (bucket settings) Info

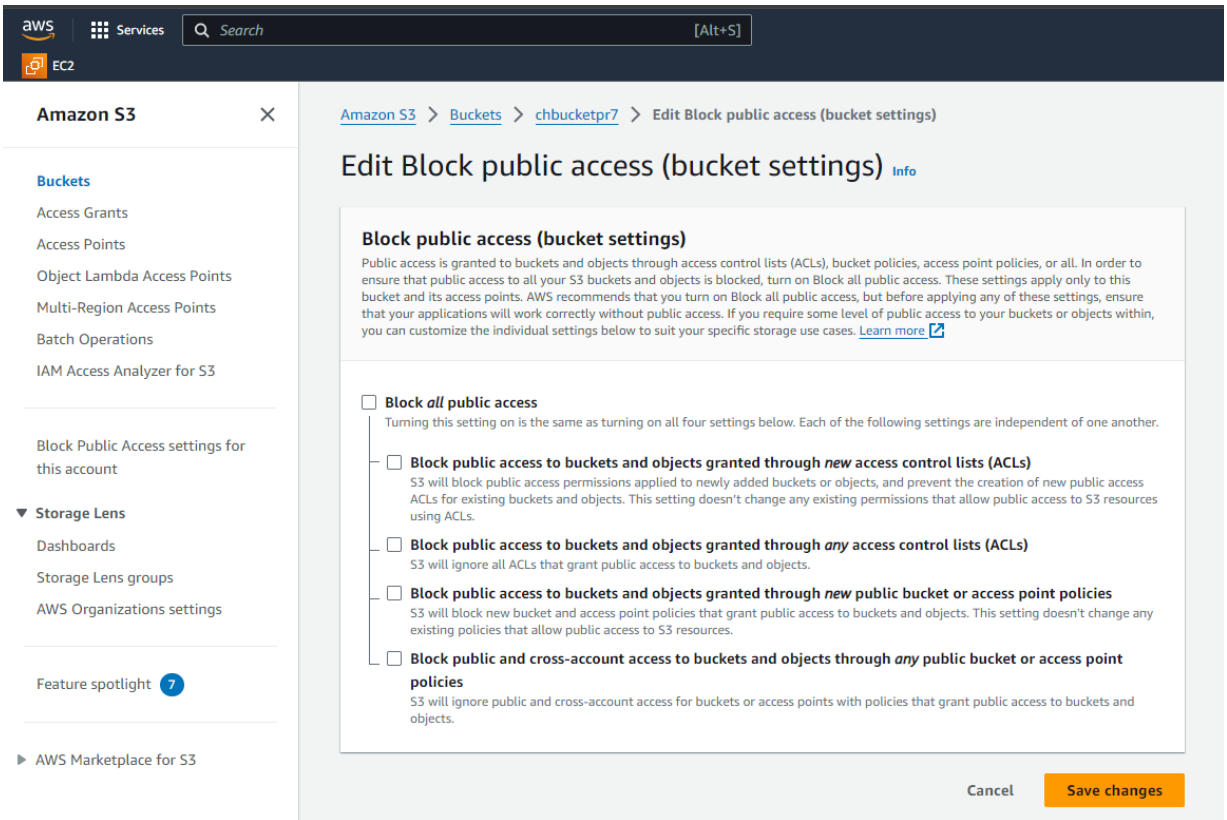
Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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.

Step 10: Uncheck all dialogue boxes and click on save changes.


aws
Services
Search
[Alt+S]
EC2
Amazon S3
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 7
AWS Marketplace for S3
Amazon S3 > Buckets > chbucketpr7 > Edit Block public access (bucket settings)
Info
Cancel
Save changes

Edit Block public access (bucket settings)

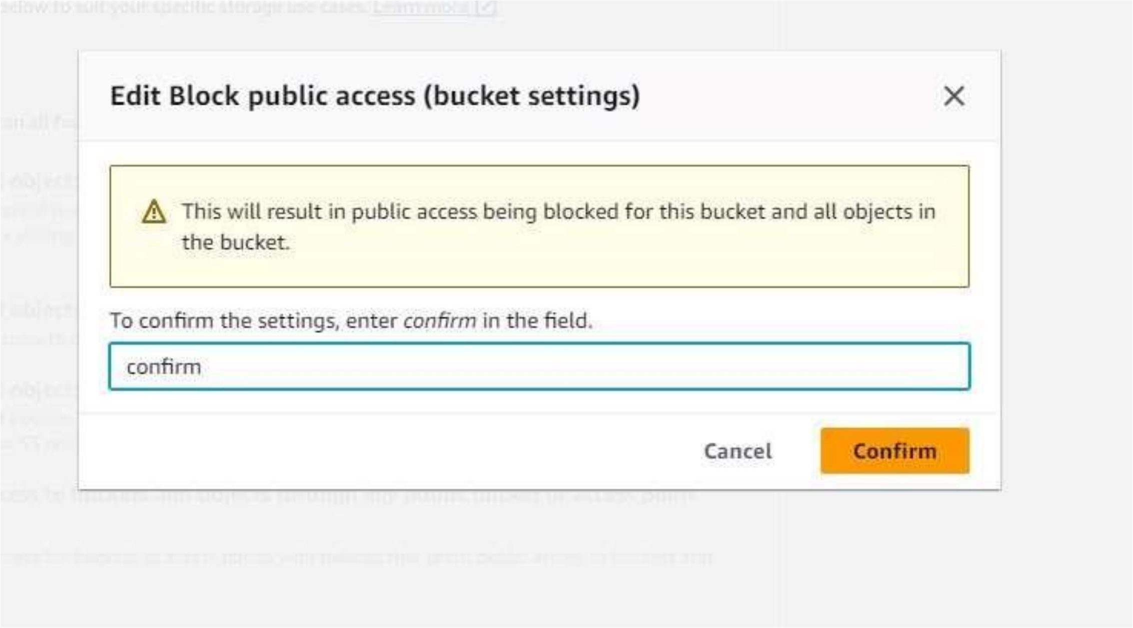
Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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.

Step 11: Type confirm in field given and click on confirm.



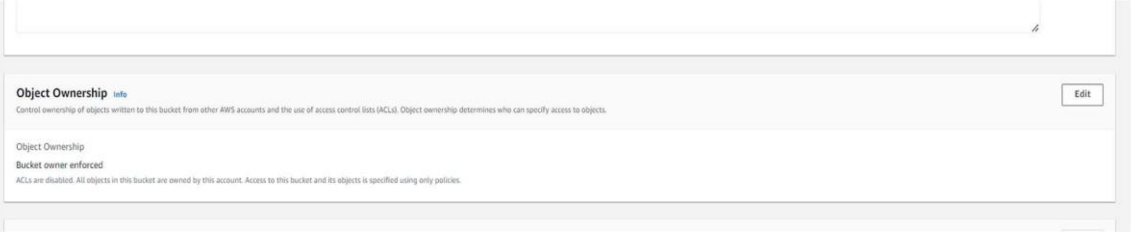
Edit Block public access (bucket settings)

⚠ This will result in public access being blocked for this bucket and all objects in the bucket.

To confirm the settings, enter *confirm* in the field.

confirm

Step 12: Now go to buckets the permissions and edit Object ownership



Object Ownership

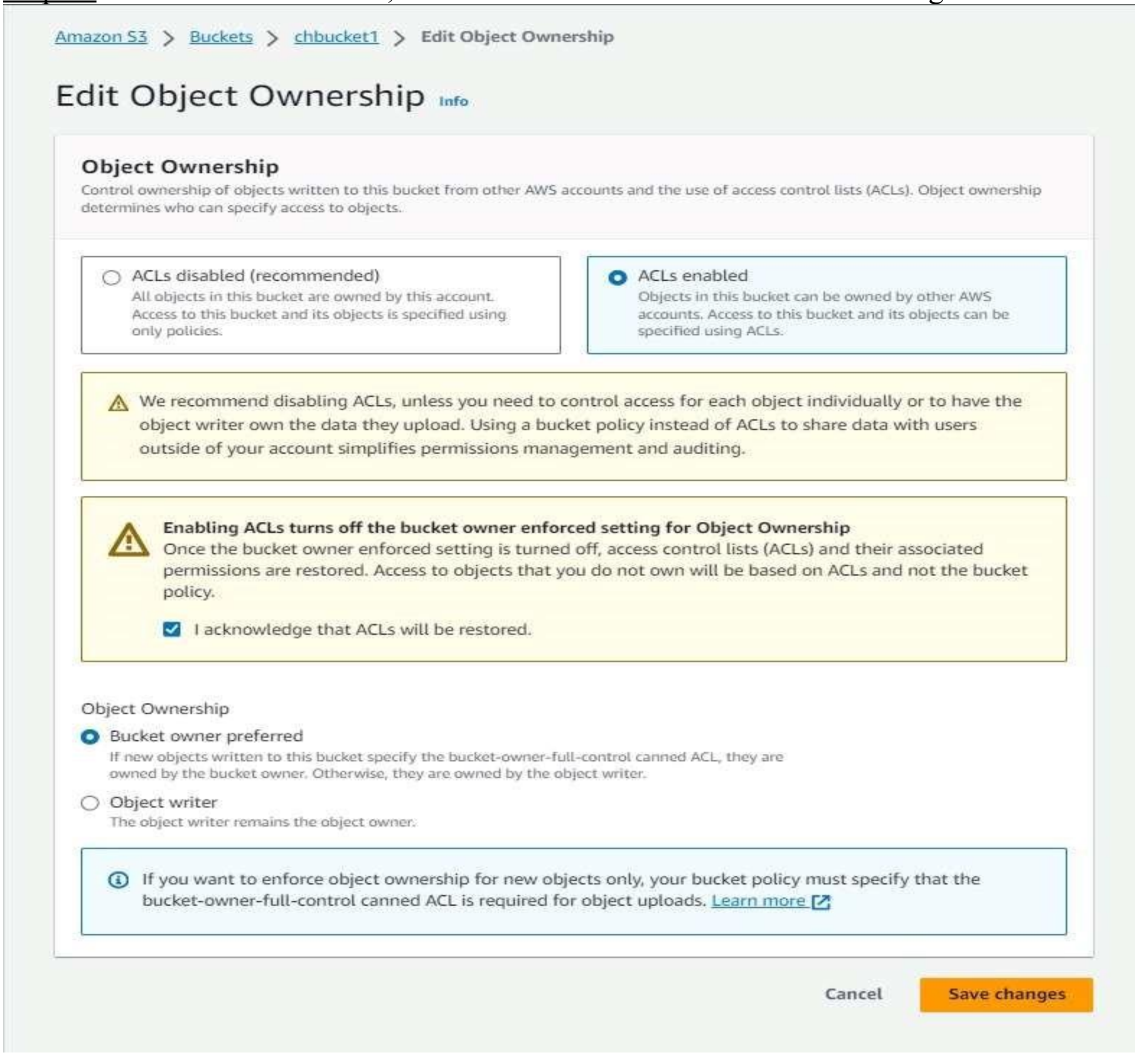
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Object Ownership

Bucket owner enforced

ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

Step 13: Choose ACLs enabled, check the checkbox and click on save changes.



Edit Object Ownership

Object Ownership

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.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

⚠ **Enabling ACLs turns off the bucket owner enforced setting for Object Ownership**
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

☑ I acknowledge that ACLs will be restored.

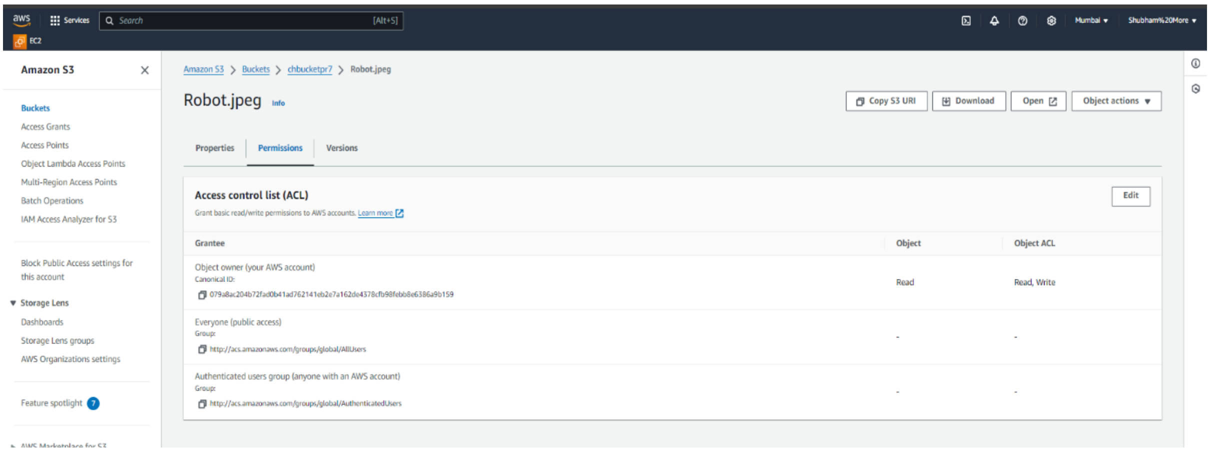
Object Ownership

● Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

Step 14: Now go to object in bucket and click on that image and then click on permissions to edit permissions.



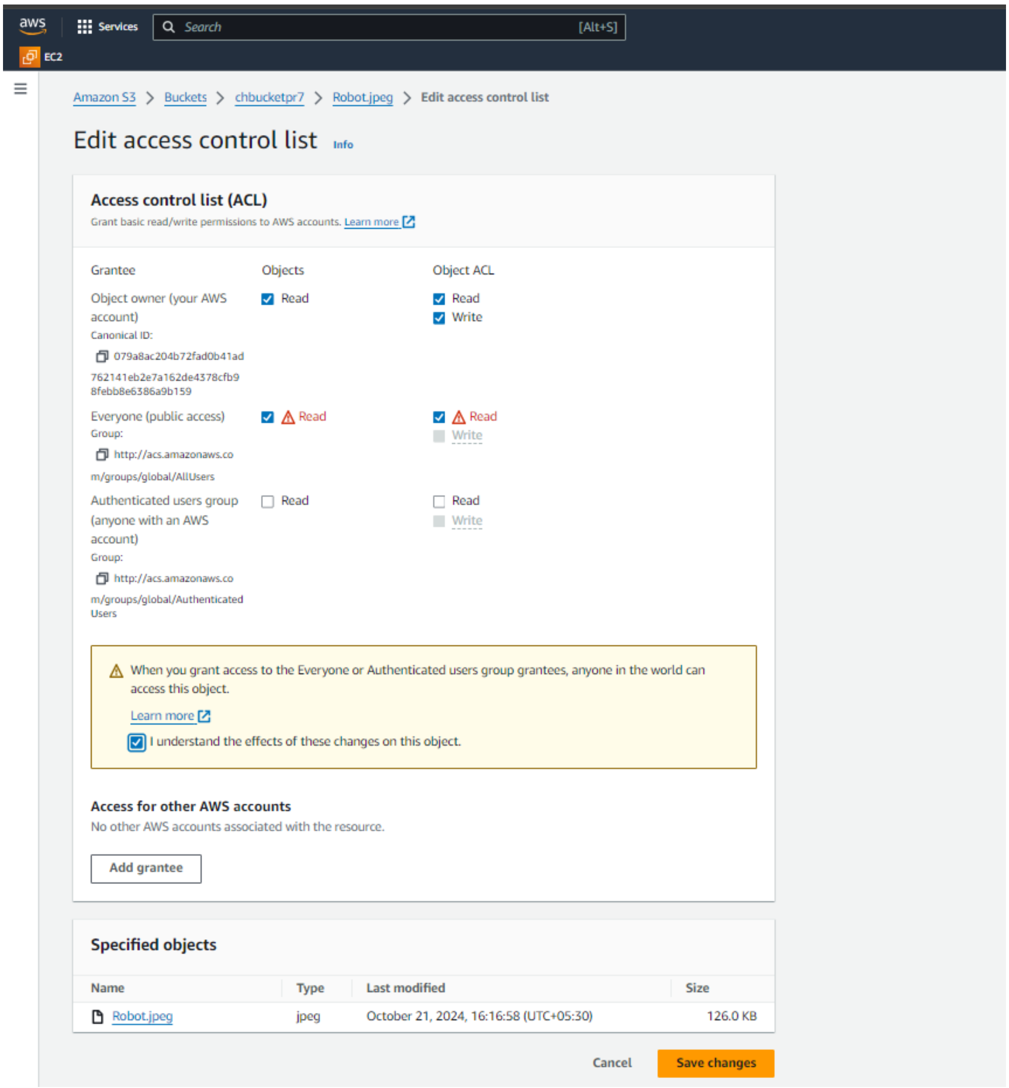
Robot.jpeg Info

Access control list (ACL)

Grant basic read/write permissions to AWS accounts. Learn more

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: 079a8ac204b72fad0b41ad762141eb2e7a162de4378cfb98febb8e6386a9b159	Read	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-

Step 15: Give permissions as shown below and click on save.


aws
Services
Search
[Alt+S]
EC2
Amazon S3 > Buckets > chbucketpr7 > Robot.jpeg > Edit access control list
Add grantee
Cancel
Save changes

Edit access control list Info

Access control list (ACL)

Grant basic read/write permissions to AWS accounts. Learn more

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID: 079a8ac204b72fad0b41ad762141eb2e7a162de4378cfb98febb8e6386a9b159	☑ Read	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ Read	☑ ⚠ Read □ Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	□ Read	□ Read □ Write

⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

Learn more

☑ I understand the effects of these changes on this object.

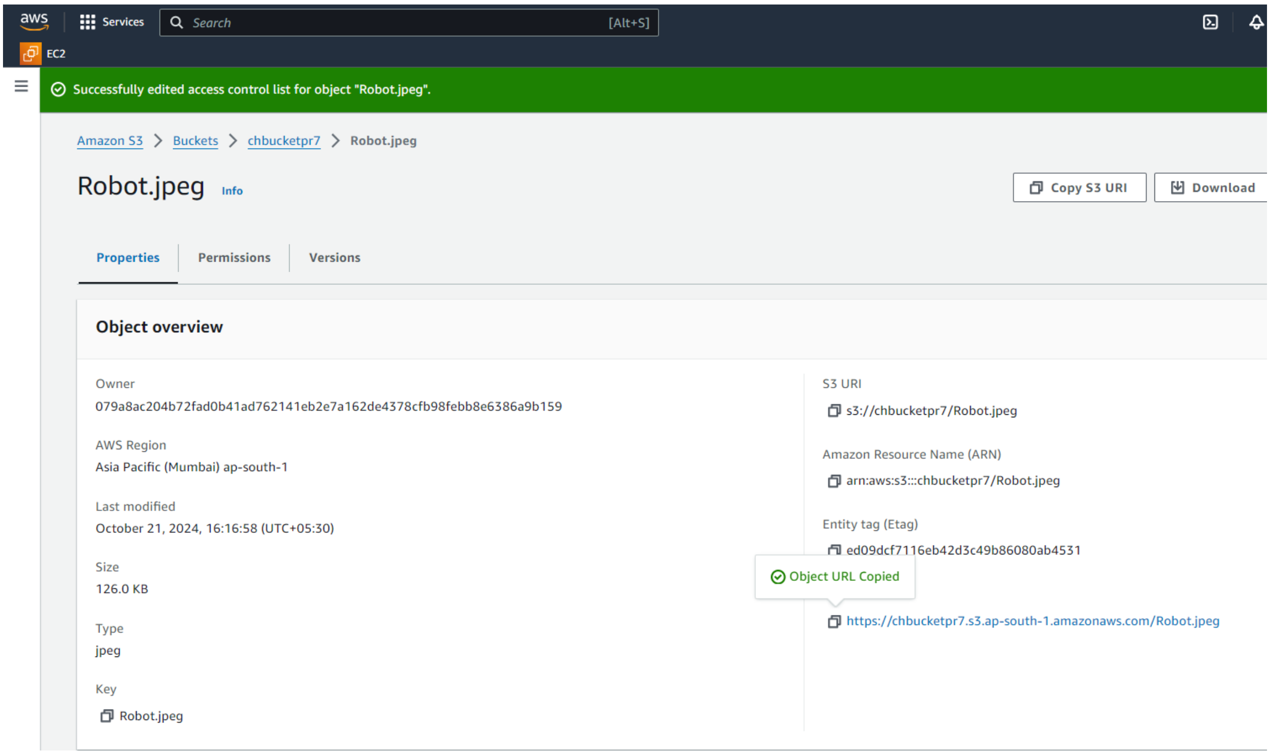
Access for other AWS accounts

No other AWS accounts associated with the resource.

Specified objects

Name	Type	Last modified	Size
Robot.jpeg	jpeg	October 21, 2024, 16:16:58 (UTC+05:30)	126.0 KB

Step 16: To check whether the image has successfully applied public access copy that Object URL as shown.



Successfully edited access control list for object "Robot.jpeg".

Amazon S3 > Buckets > chbucketpr7 > Robot.jpeg

Robot.jpeg Info

Object overview

Owner
079a8ac204b72fad0b41ad762141eb2e7a162de4378cfb98febb8e6386a9b159

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

Last modified
October 21, 2024, 16:16:58 (UTC+05:30)

Size
126.0 KB

Type
jpeg

Key
Robot.jpeg

S3 URI
s3://chbucketpr7/Robot.jpeg

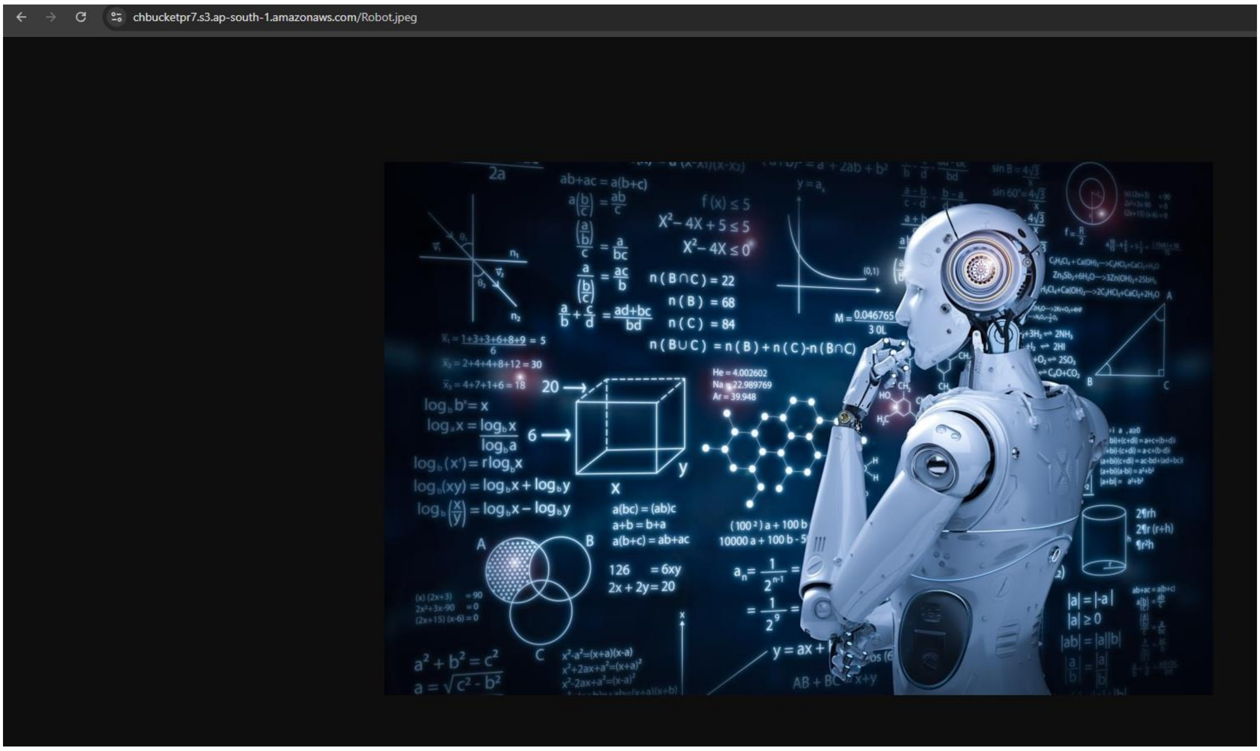
Amazon Resource Name (ARN)
arn:aws:s3:::chbucketpr7/Robot.jpeg

Entity tag (Etag)
ed09dcf7116eb42d3c49b86080ab4531

Object URL Copied

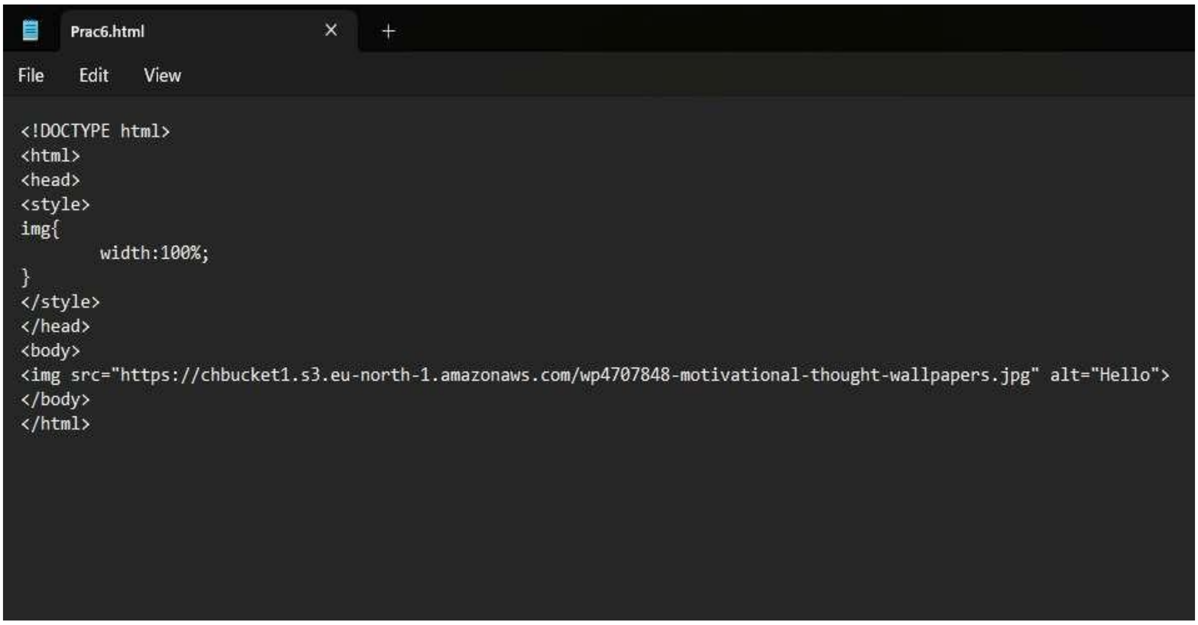
https://chbucketpr7.s3.ap-south-1.amazonaws.com/Robot.jpeg

Step 17: Paste it into your browser. If it shows image then it has public access.



chbucketpr7.s3.ap-south-1.amazonaws.com/Robot.jpeg

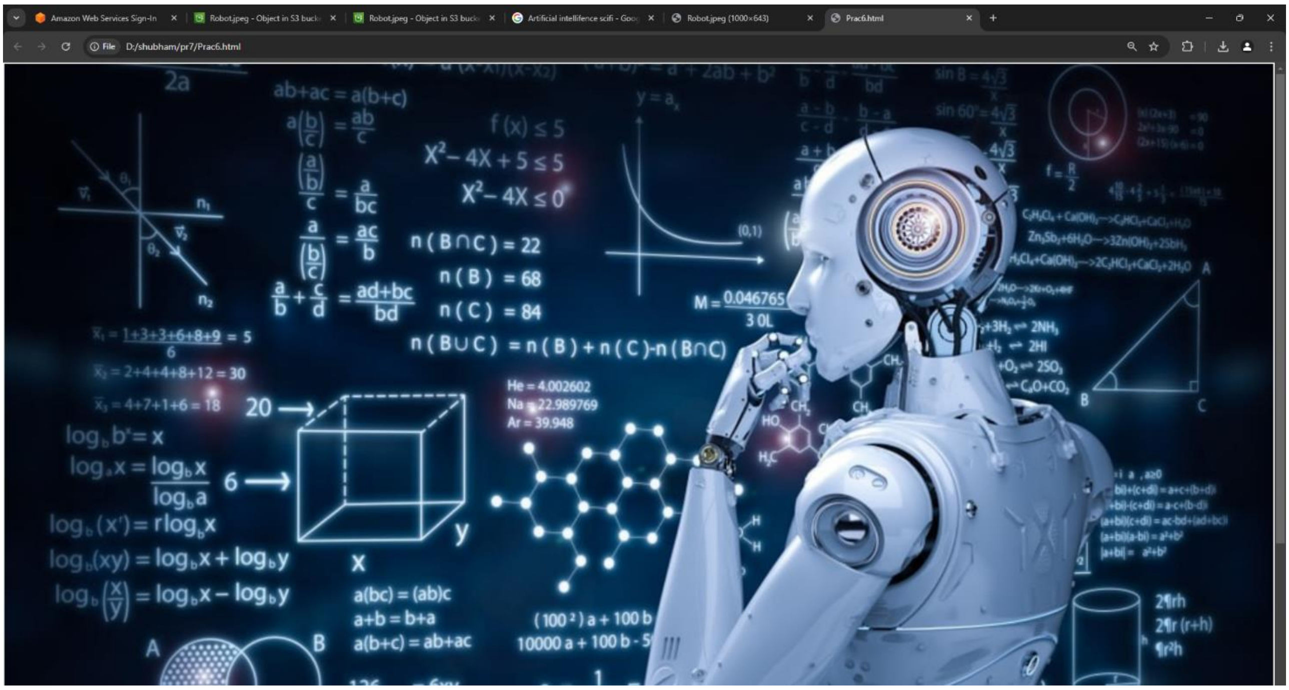
Step 18: Now open notepad and write html code. In img src section paste object url that we have copied earlier.



```
<!DOCTYPE html>
<html>
<head>
<style>
img{
        width:100%;
}
</style>
</head>
<body>
<img src="https://chbucket1.s3.eu-north-1.amazonaws.com/wp4707848-motivational-thought-wallpapers.jpg" alt="Hello">
</body>
</html>
```

Save this file with .html extension as shown.

Step 19: Now Open that .html file in your browser. If the image opens then we have successfully stored image.


Amazon Web Services Sign-In
Robot.jpeg - Object in S3 bucke
Robot.jpeg - Object in S3 bucke
Artificial intellifence scifi - Goo
Robot.jpeg (1000×643)
Prac6.html
File
D:/shubham/pr7/Prac6.html

Conclusion: We have successfully created bucket and stored image in that using S3.