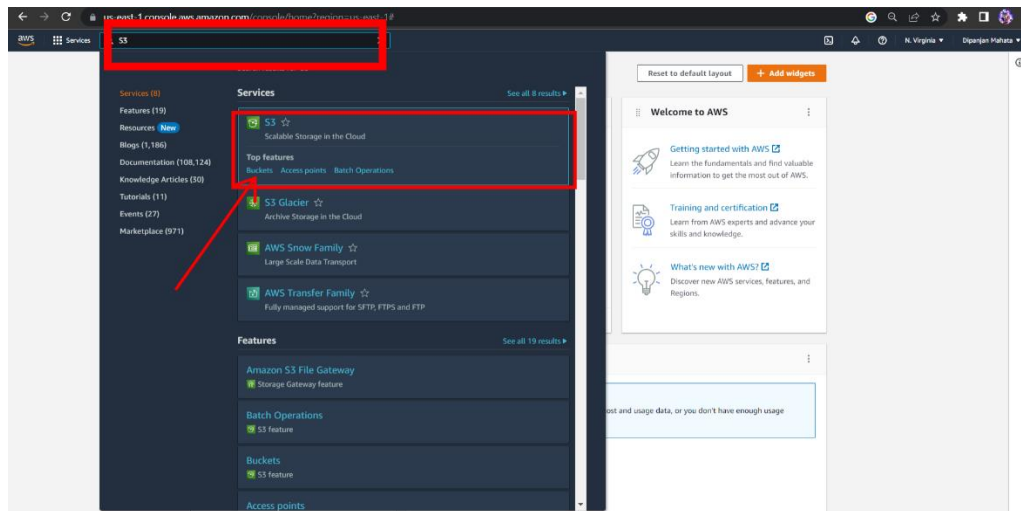


Assignment 5

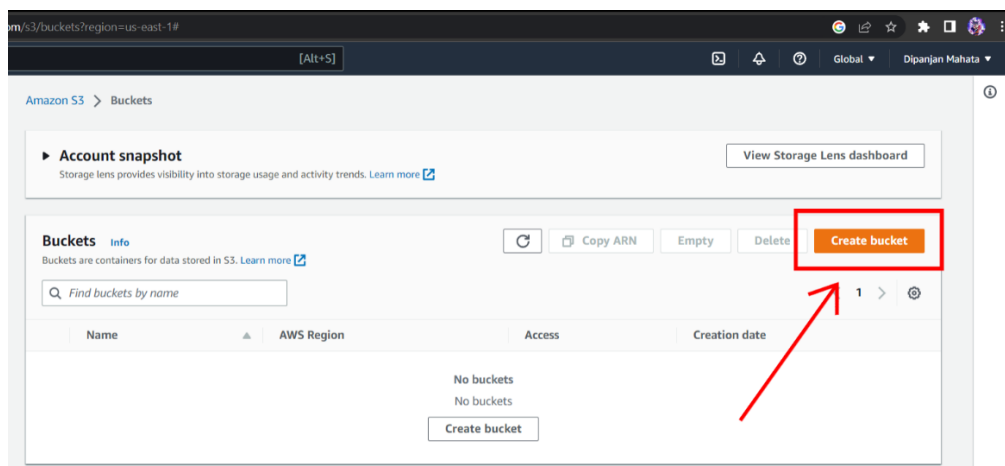
Create a public bucket in AWS. Upload a file and give the necessary permission to check the file url is working or not.

Steps for creating an AWS account:

1. **Sign in.** Sign in as a root user. Provide username and password when prompted.
2. Search on the search bar **S3**. After that click on **bucket** in the **S3**.



3. Now click on **Create bucket**.



4. Give a **Unique** bucket name.

aws Services Search [Alt+S]

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

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

General configuration

Bucket name

Dip12

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

5. Now click on **ACLs enable**. After that click on **Bucket owner preferred**.

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 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.


Info 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](#)

Info **Upcoming permission changes to enable ACLs**
Starting in April 2023, to enable ACLs when creating buckets by using the S3 console, you must have the s3:PutBucketOwnershipControls permission. [Learn more](#)


6. Uncheck the **Block all public access** and check **I acknowledge**.


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.**

7. Now give the **Bucket versioning** as **disable**.

[s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1](#)

console, you will no longer need the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#)

Bucket Versioning

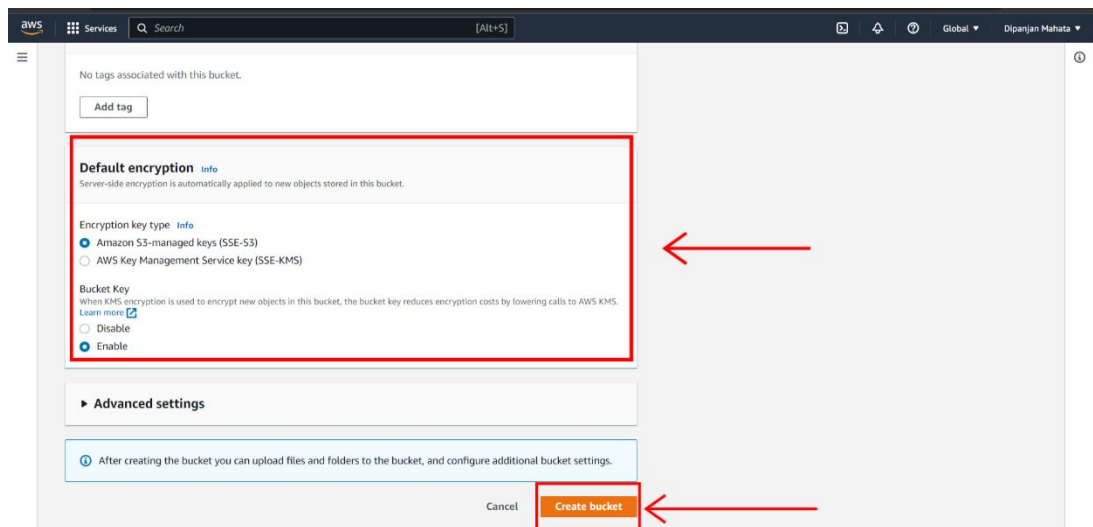
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

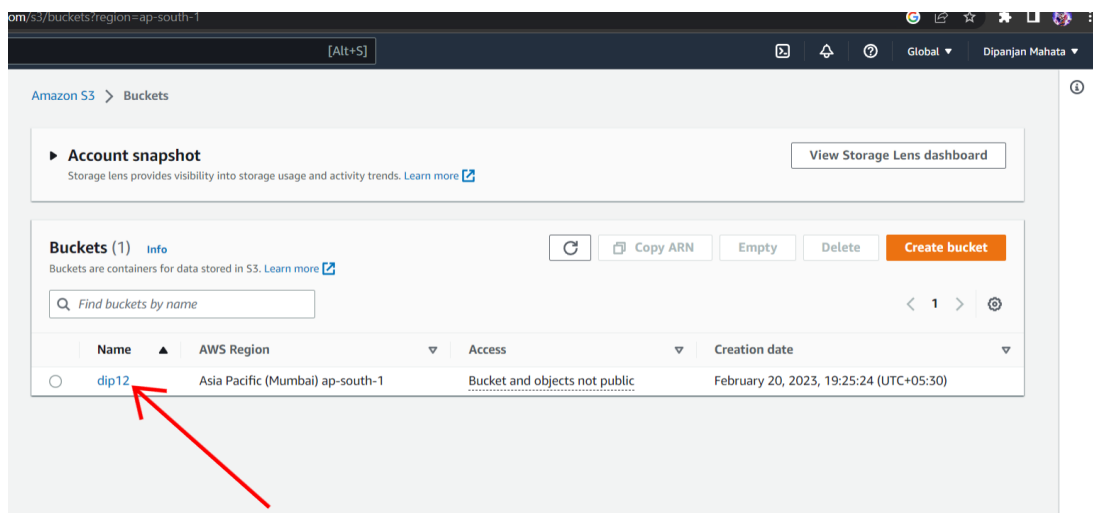
☒ Disable

☐ Enable

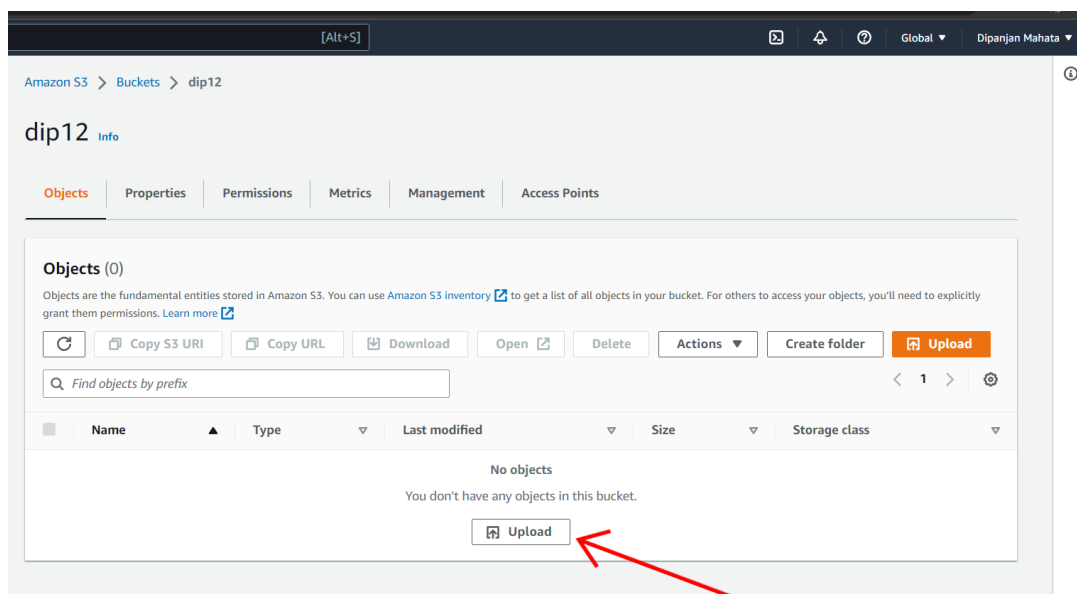
8. In the **Default encryption** section don't change anything. Click on **create bucket**.



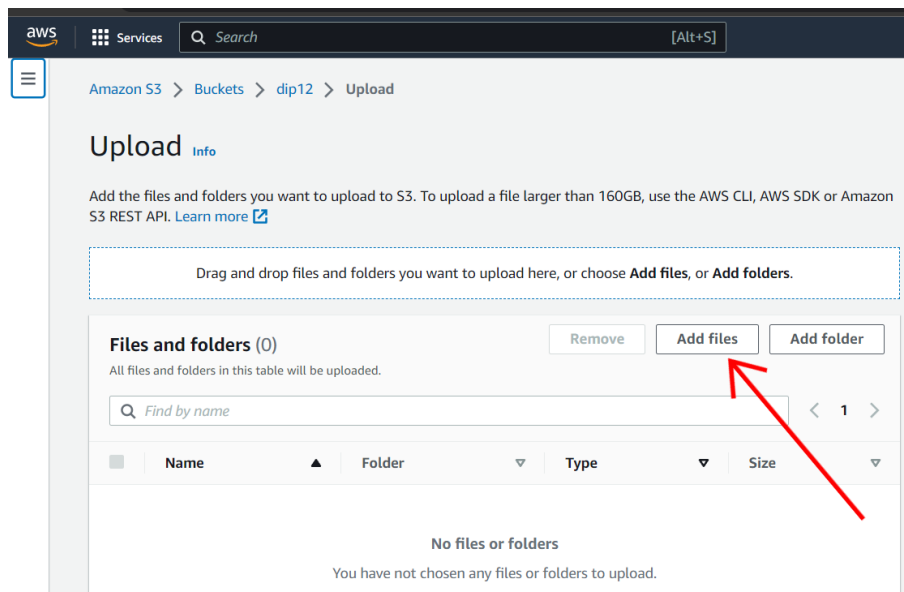
9. After your bucket has created click on the **bucket name**.



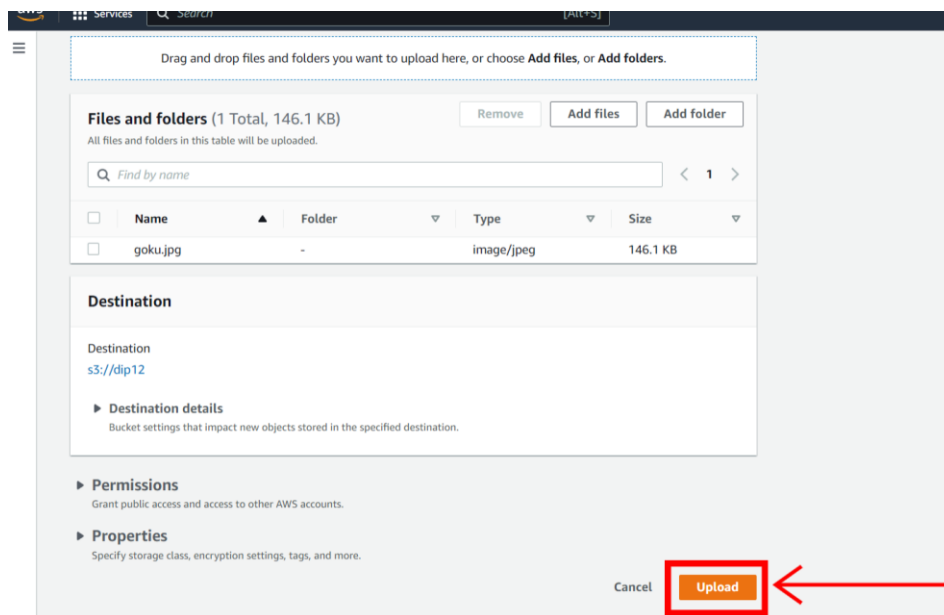
10. After that click on **upload** to upload files or folders.



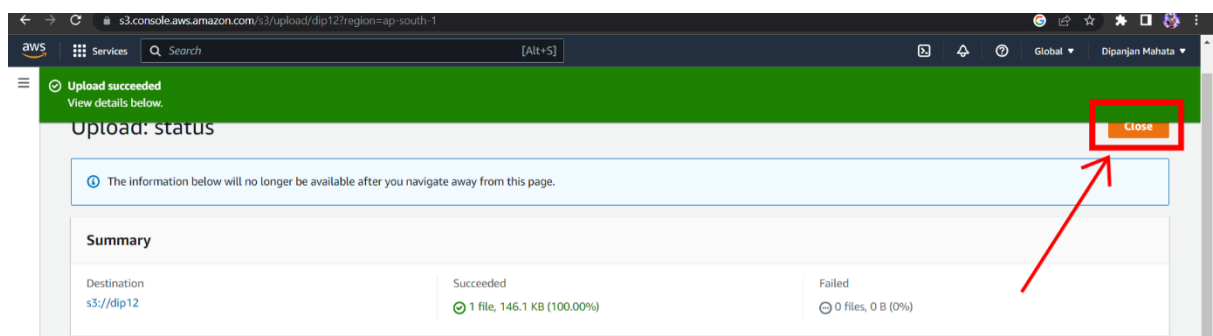
11. Click on **Add files** to add files or **Add folder** to add folders.



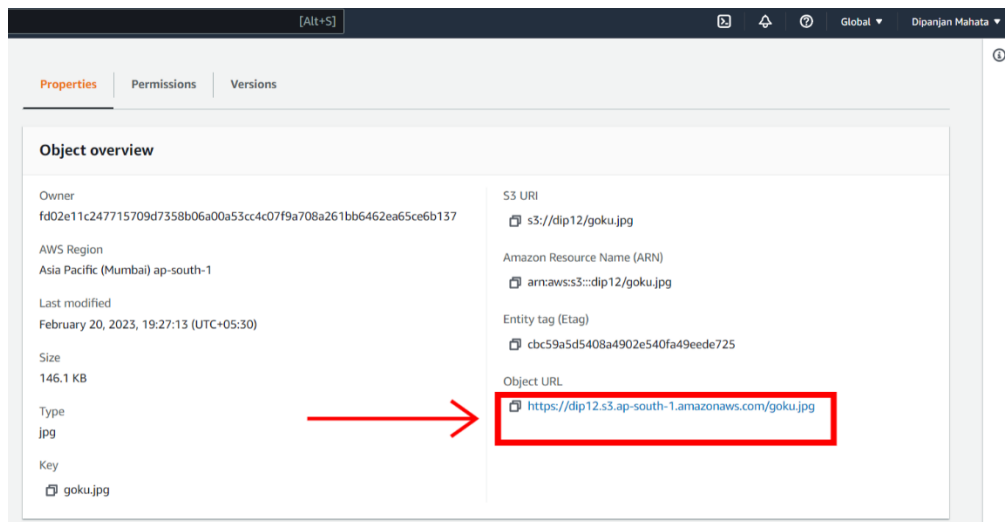
12. After that click on **upload**.



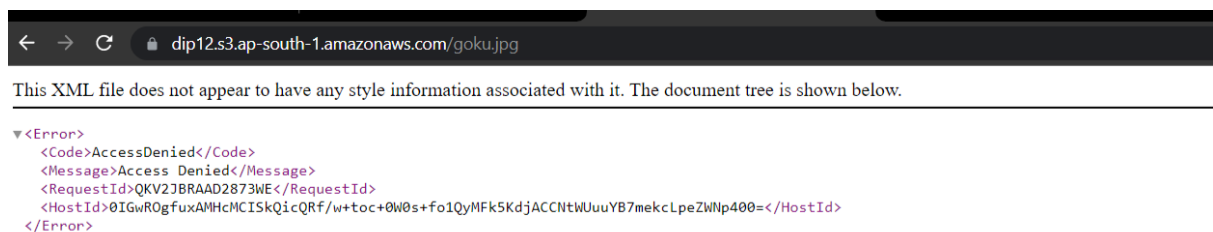
13. Now click **Close**.



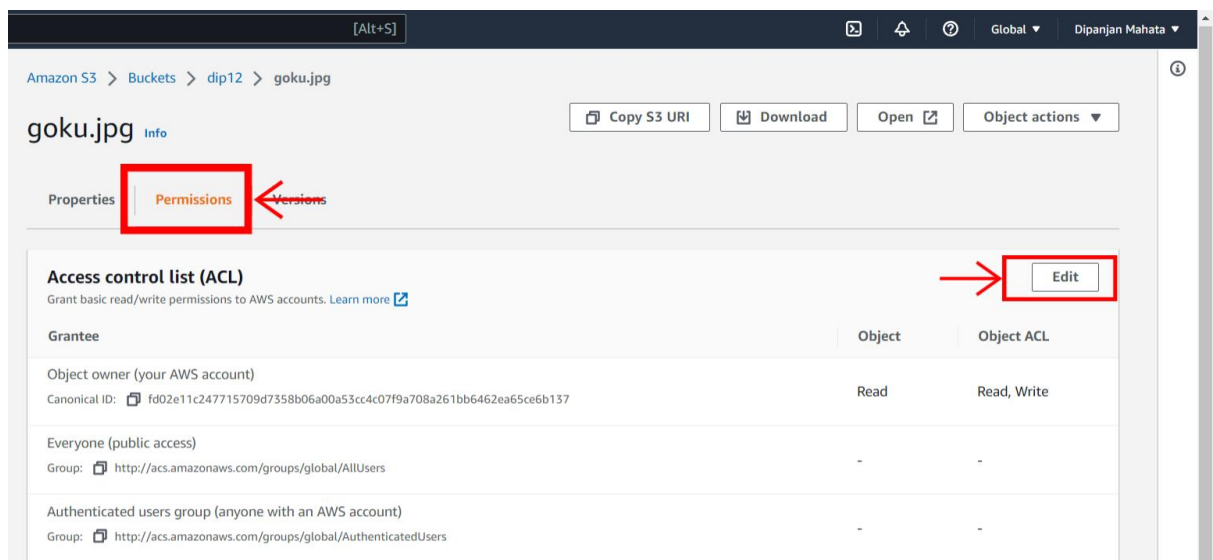
14. Click on the **object URL** to copy the URL so that we can see the file on web.



15. As we have not given the permission as public we can't able to see the file.



16. Now click on **permission**, after that click on **edit**.



17. Check on **Read and Read** in the **Everyone (public access)**.

Amazon S3 > Buckets > dip12 > goku.jpg > Edit access control list

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: fd02e11c247715709d7358b06a00a53cc4c07f9a708a261bb6462ea65ce6b137	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> Read ←	<input checked="" type="checkbox"/> Read ← <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> Read	<input type="checkbox"/> Read <input type="checkbox"/> Write

18. Check on **I understand**.

Amazon S3 > Buckets > dip12 > goku.jpg > Edit access control list

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: fd02e11c247715709d7358b06a00a53cc4c07f9a708a261bb6462ea65ce6b137	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> Read ←	<input checked="" type="checkbox"/> Read ← <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> Read	<input type="checkbox"/> Read <input type="checkbox"/> Write


Warning: 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.

[Add grantee](#)

19. Check on **save changes**.


⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.
[Learn more](#) 

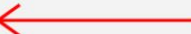
☒ I understand the effects of these changes on this object.

Access for other AWS accounts
No other AWS accounts associated with the resource.

[Add grantee](#)

Specified objects

Name	Type	Last modified	Size
 goku.jpg	jpg	February 20, 2023, 19:30:53 (UTC+05:30)	146.1 KB

Cancel **Save changes** 

20. Now if you copy the object URL and open in new tab you can see the file which I have uploaded.

