S3 SERVICE In AWS

S3 is simple service storage. It is object -based storage you can storage images,word files, pdf files etc

The files which store in s3 in 0 byte to 5 kb.Files are stored in Bucket. A bucket is like a folder available in S3 that stores the files.
Built for 99.99 % availability for s3 platform
Amazon Guarantee 99.99999999999% availbale
Lifecycle management,Versioning,Encryption
Secure your data using Access control list and bucket policy
S3 allows the hosting static website

CREATING IN S3 BUCKET

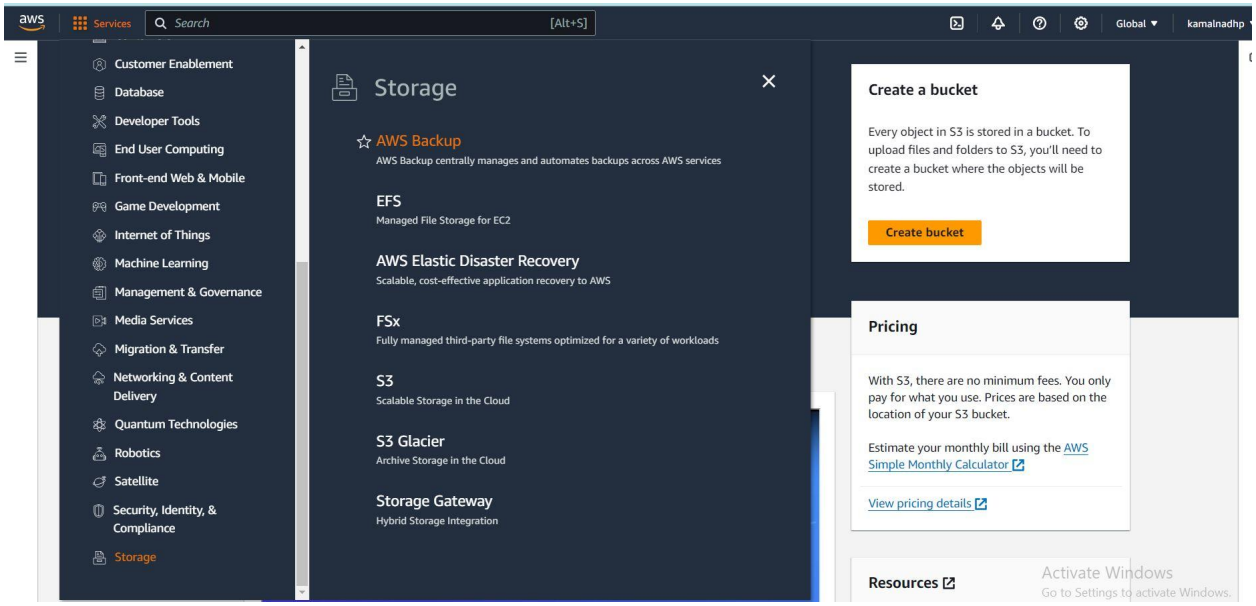
Bucket : bucket is the containter used for storing the objects. Each bucket has own policies and configurationsYou can created 100 buckets in one aws accont .but it requested more bucket you need the aws support

RULES OF CREATETING in s3 bucket

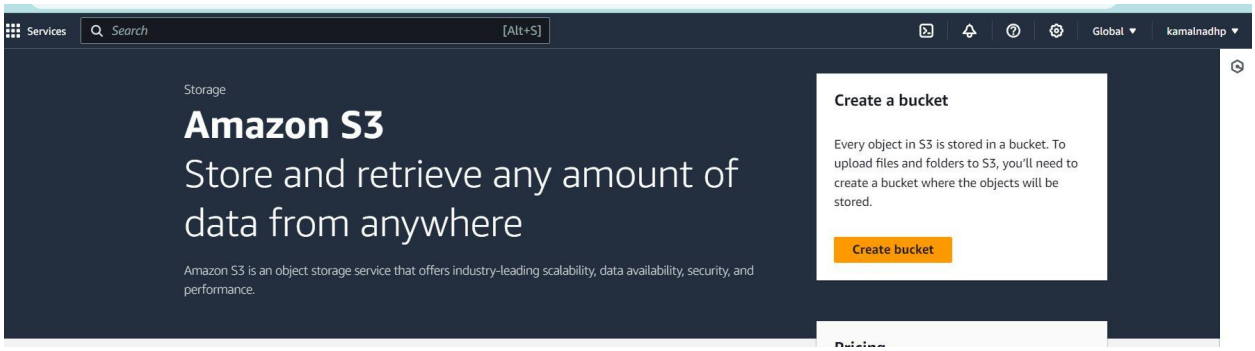
* Bucket is name should be consist the lowercase ,numbers,dots
* Bucket is start and ends with numbers or letters
*Bucket should not contains the adjacent sides
* bucket name should the not contains ip address
* bucket name is should be uniquely
* bucket name is should start with the ip address

STEPS OF CREATING IN S3 BUCKET

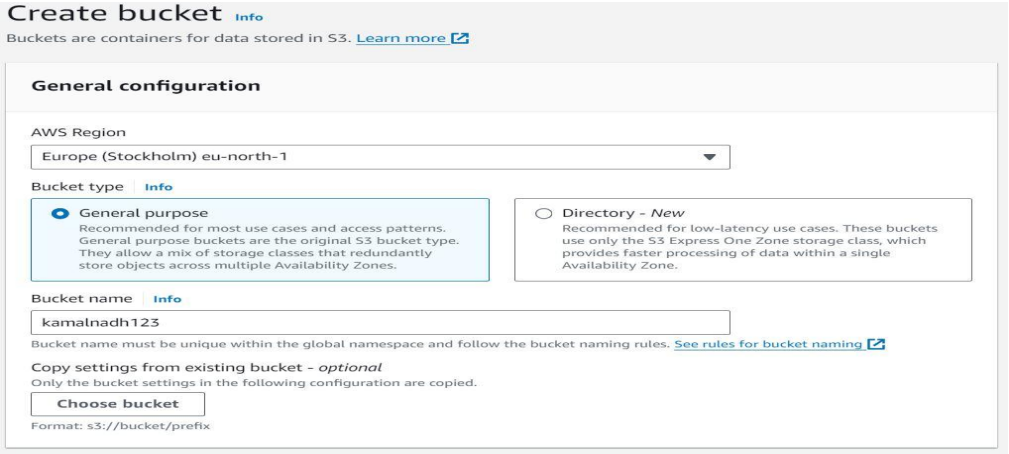
1. Go the storage select on s3 bucket



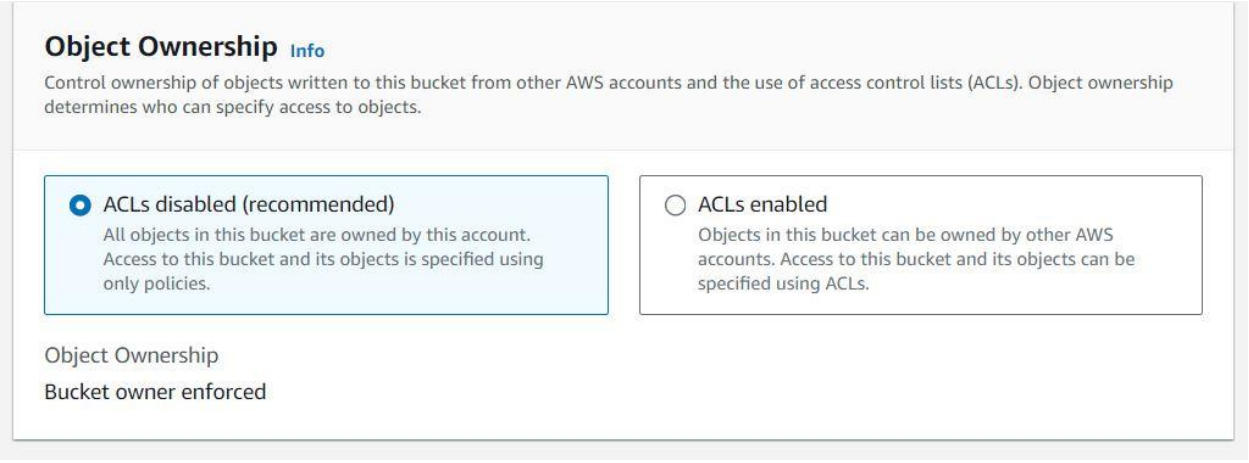
2.click the s3 storage if you want the storage can flies you need to created s3 bucket



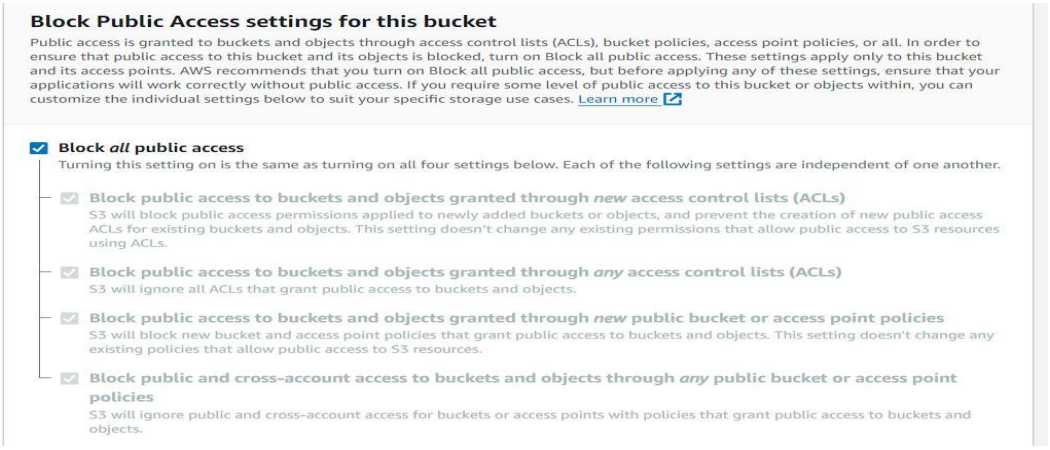
3.given bucketname should be unique



4. ACL is the access control list it is used for control you bucket with respect the security

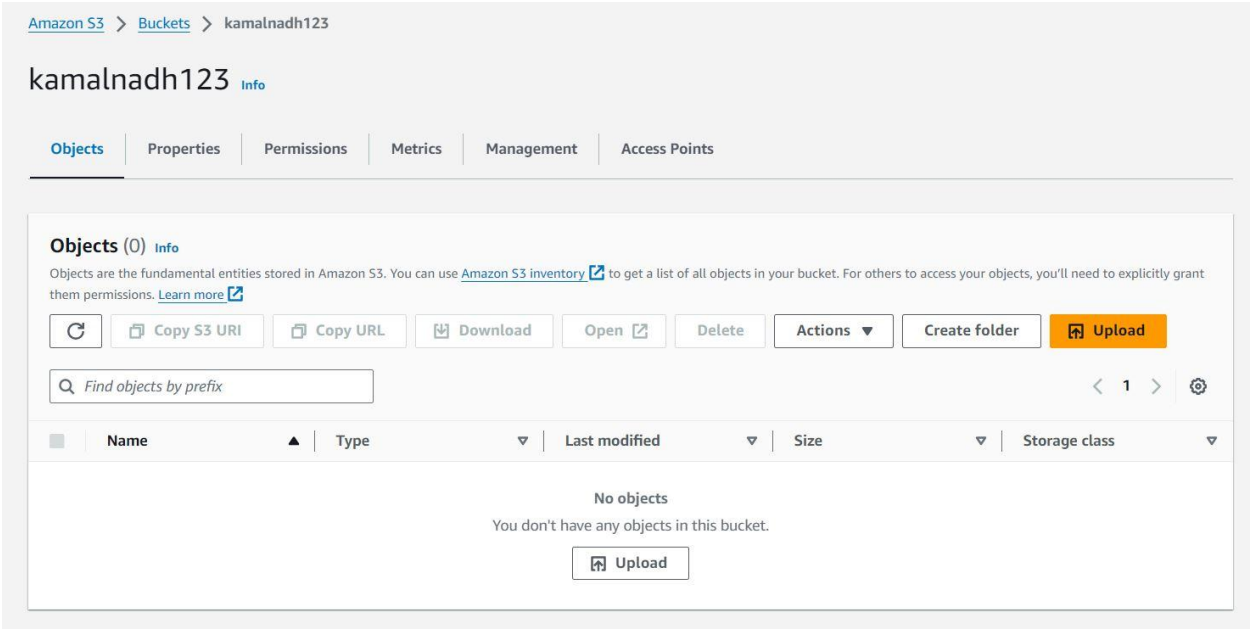


5.all the bucket by default is private as shown figure

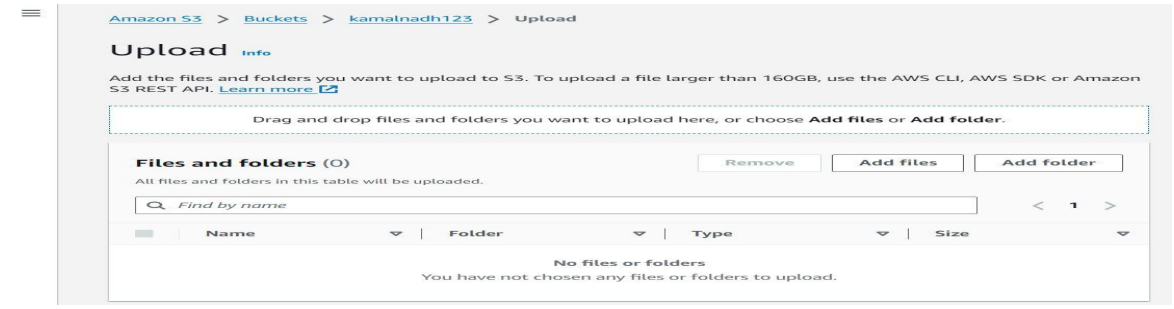


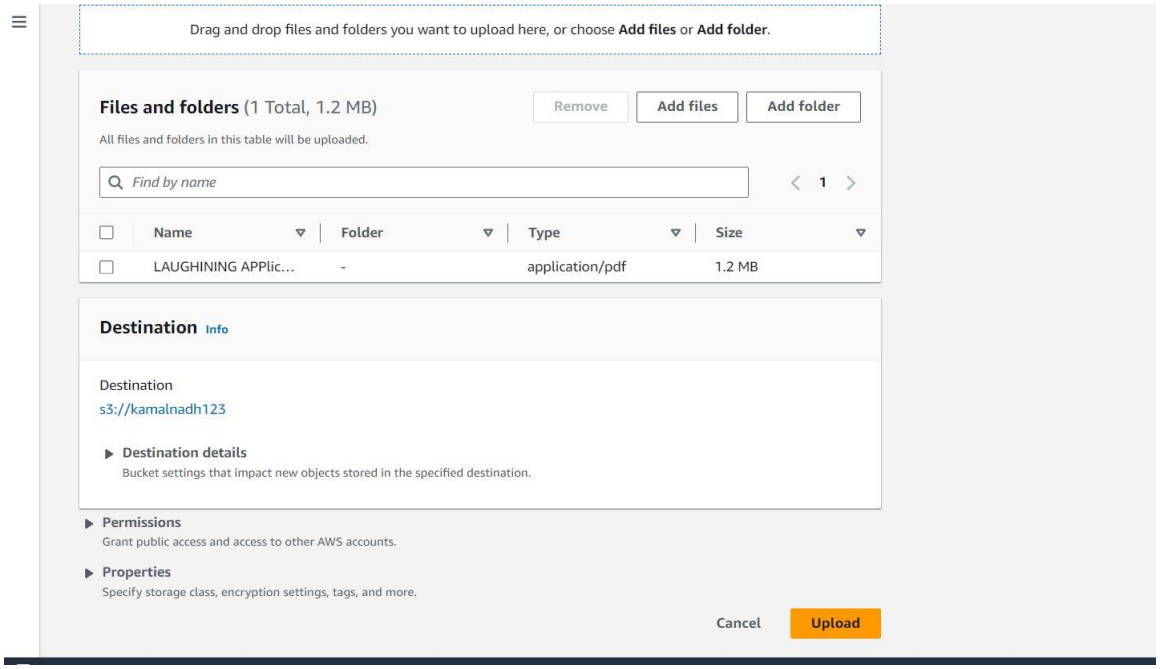
5.click on the created bucket

6.upload the file the kamalnadh123 bucket click upload the files as shown in figure

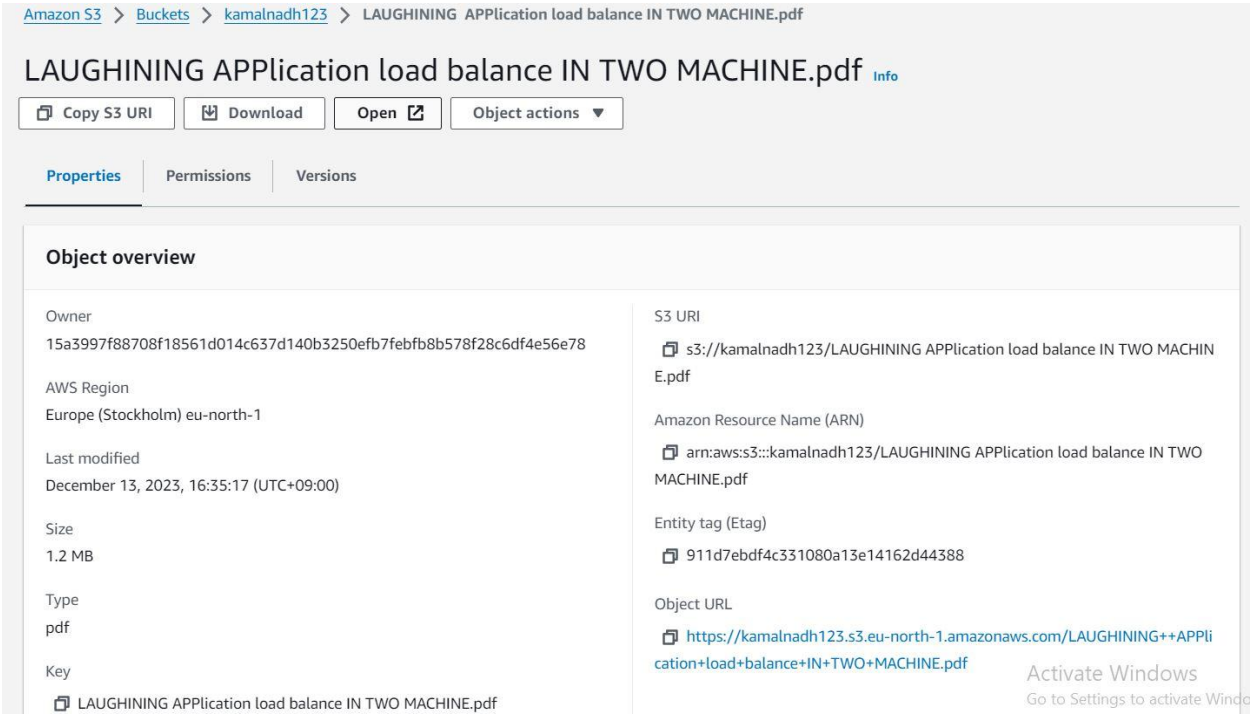


Click upload add file or add folder as you requriments

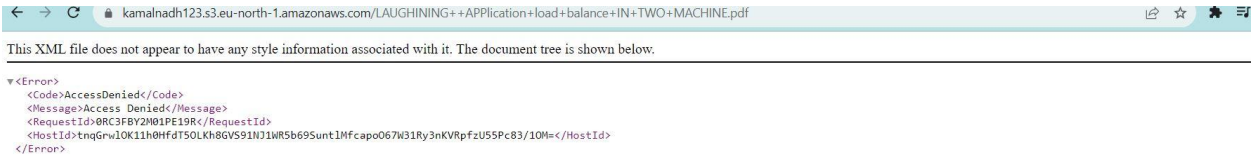




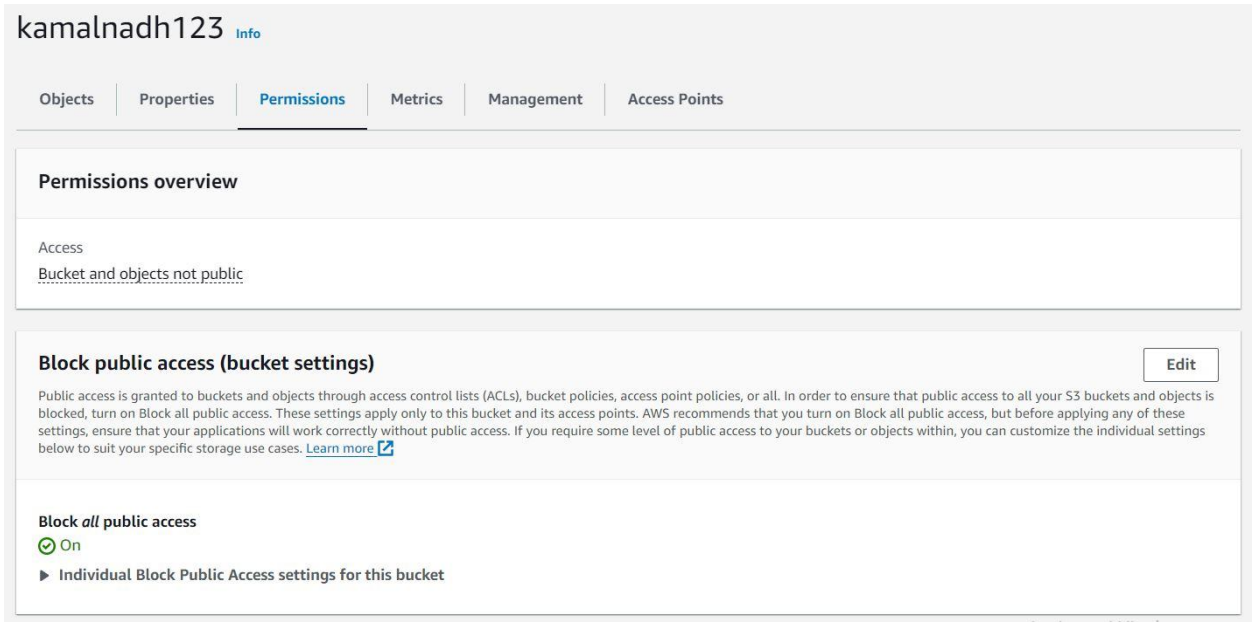
After upload the files in click on it go the propeties copy url as shown below

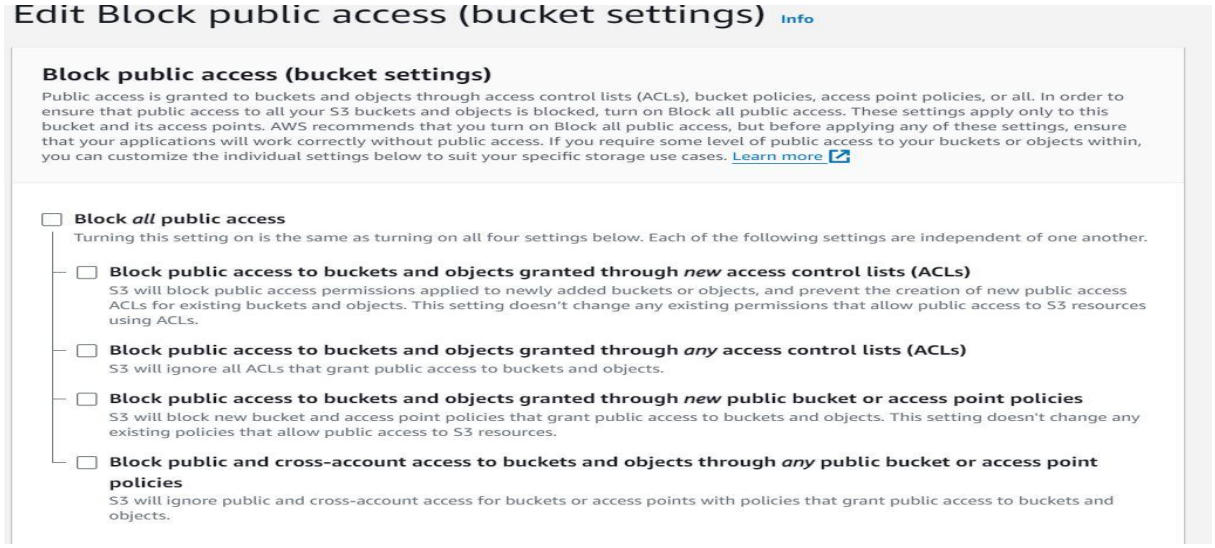


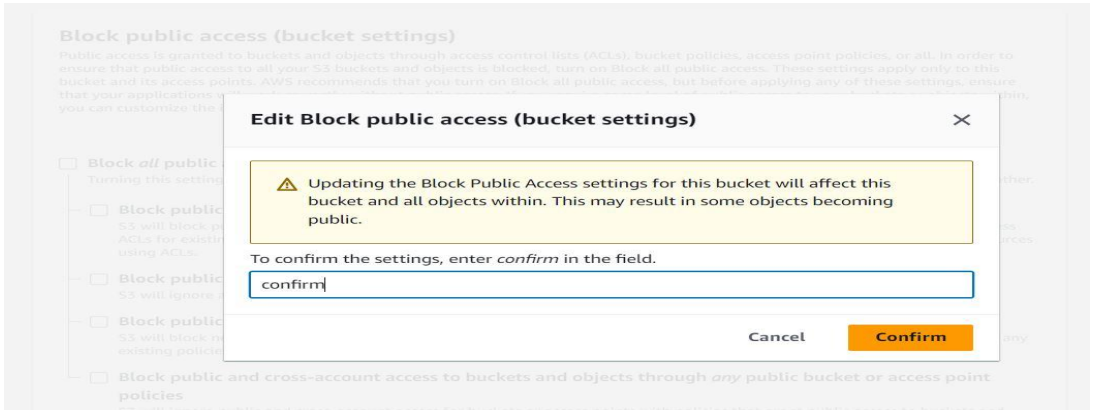
The url copy and paste it will be error because bucket and object are private you need the change to public



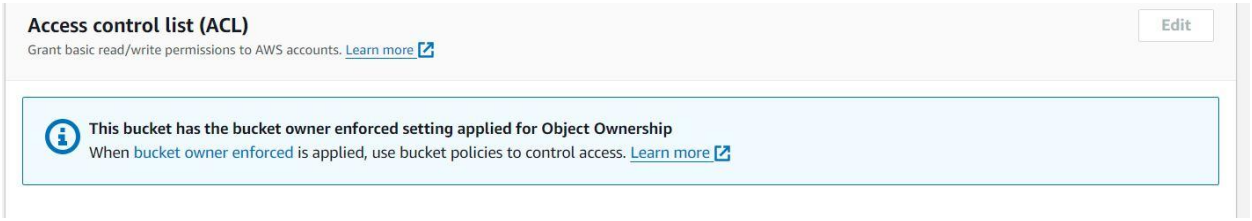
Go the bucket change permisssions block public access edit


kamalnadh123 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Bucket and objects not public
Block public access (bucket settings)
Edit
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

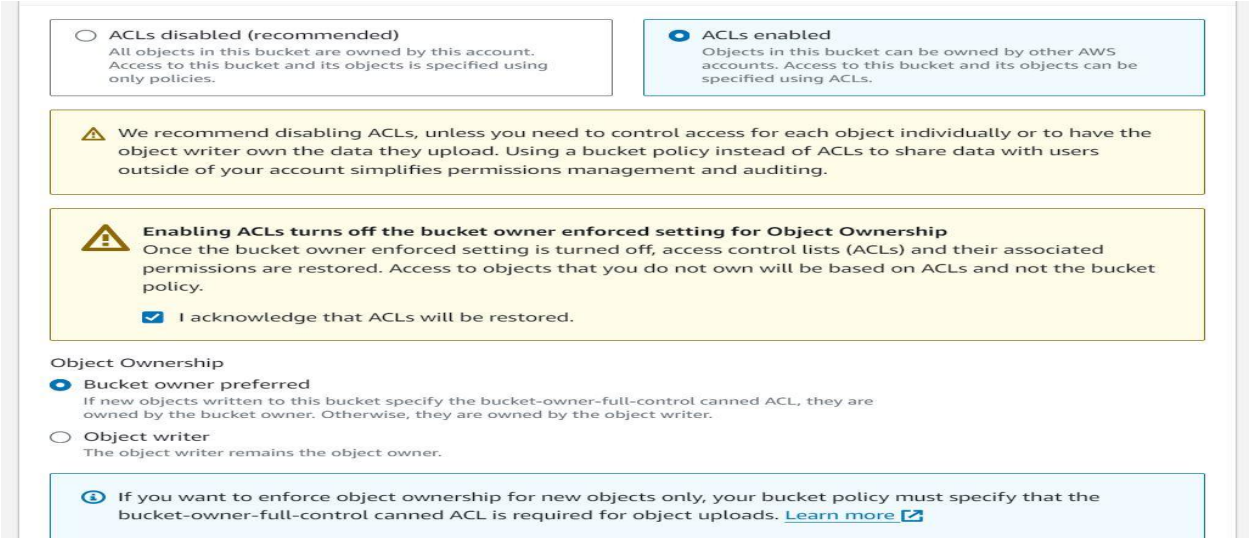

Edit Block public access (bucket settings) Info
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, 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.


Edit Block public access (bucket settings)
Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.
To confirm the settings, enter confirm in the field.
confirm
Cancel
Confirm

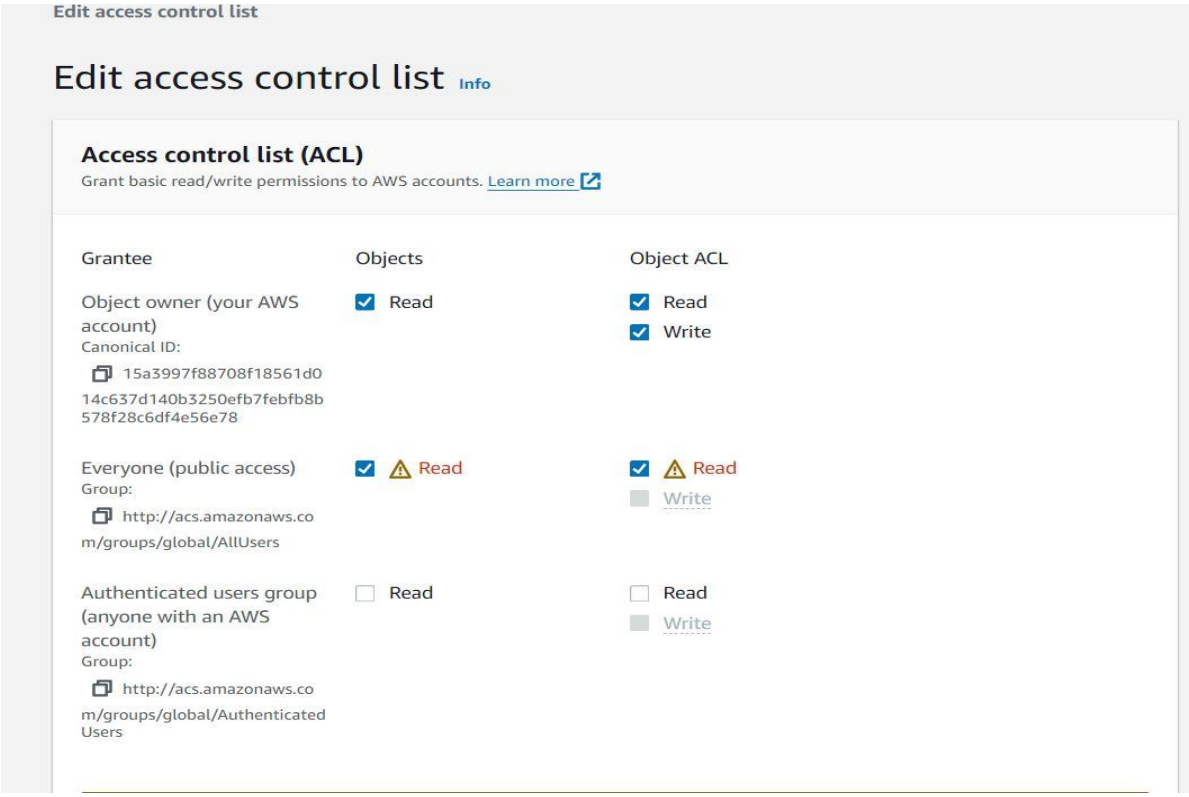
You upload the file in bucket change the object in public go object permissions change acl disable as shown in figure



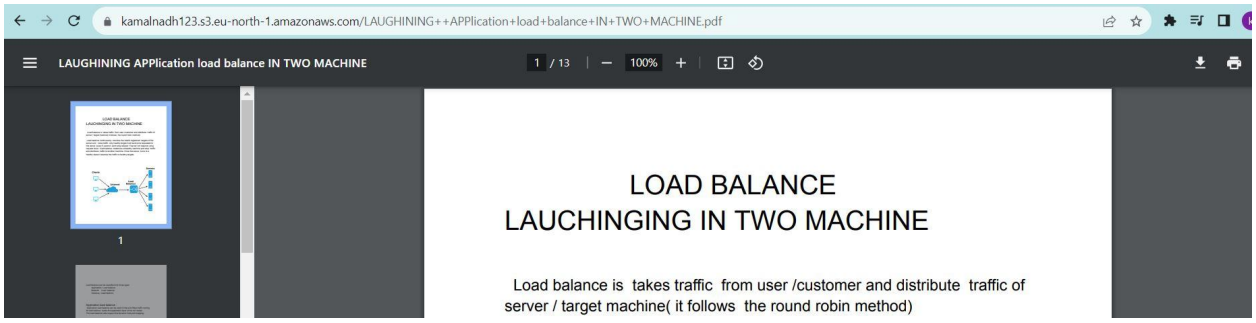
Click on the bucket owner enforced change ACLS enabled as shown figure



Click on read object and read the object ACL as shown in figure



Copy the url the paste chrome it open as shown in figure


kamalnadh123.s3.eu-north-1.amazonaws.com/LAUGHINING++APPlication+load+balance+IN+TWO+MACHINE.pdf
LAUGHINING APPlication load balance IN TWO MACHINE
1 / 13
100%
1
LOAD BALANCE
LAUCHINGING IN TWO MACHINE
Load balance is takes traffic from user /customer and distribute traffic of server / target machine(it follows the round robin method)