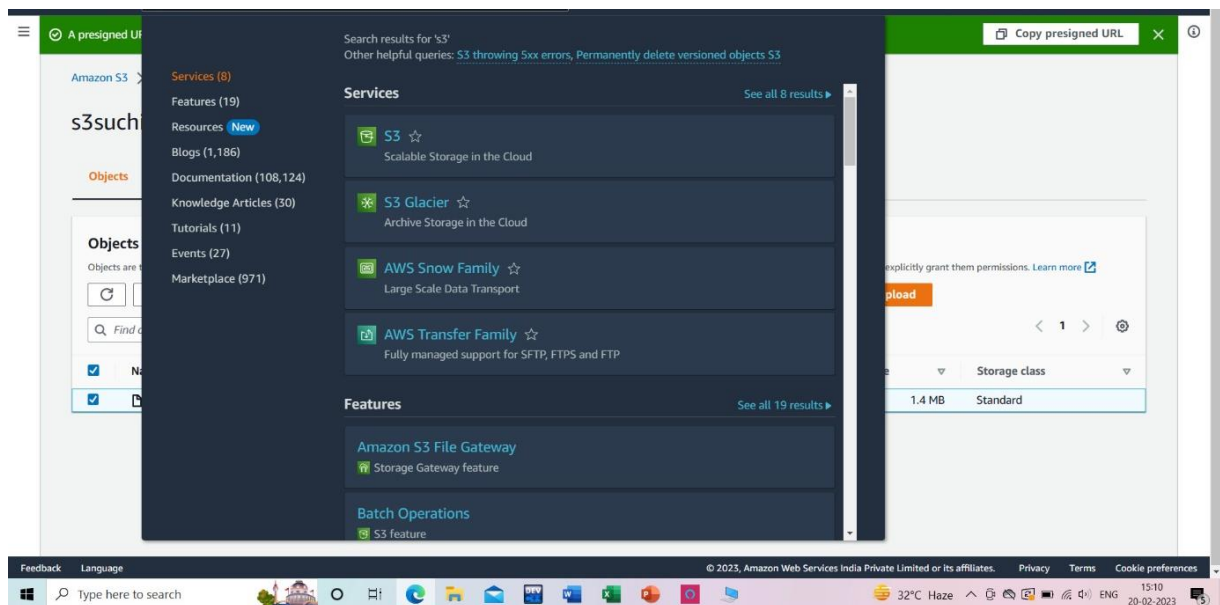


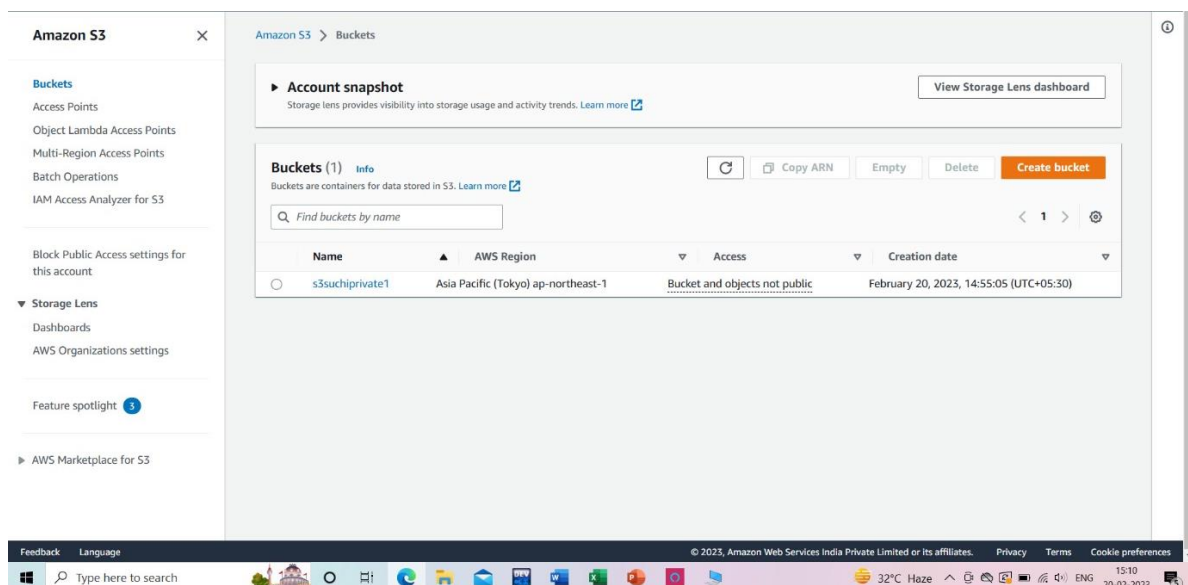
AWS-5

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

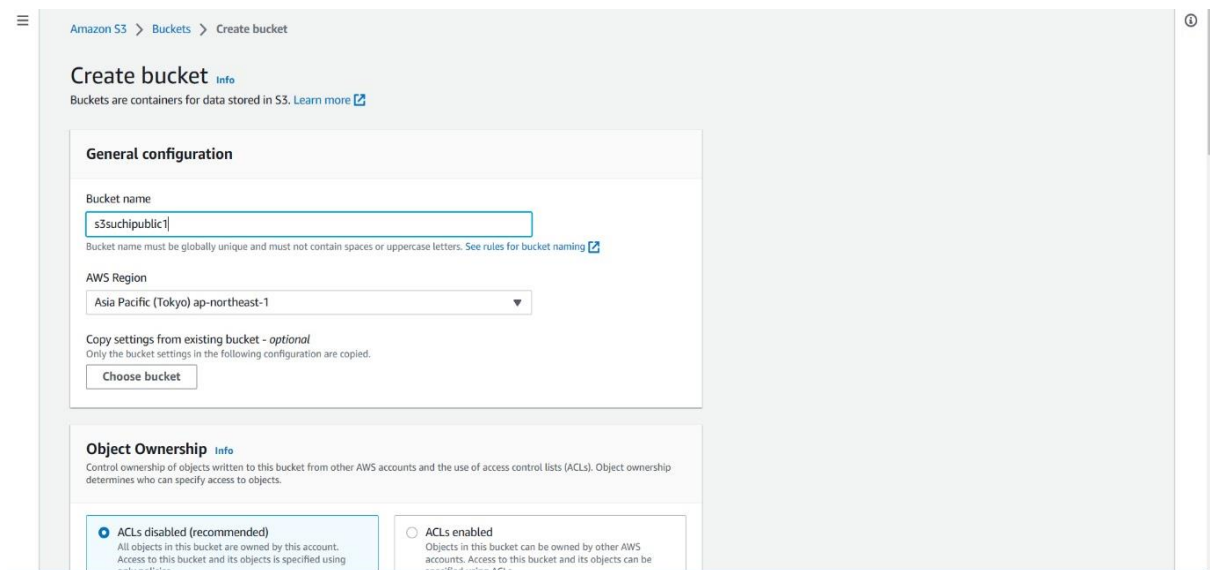
1. First search s3 then click on it.



2. Then click on Create bucket.



3. Then enter Bucket name.



Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

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

General configuration

Bucket name

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

AWS Region

Asia Pacific (Tokyo) ap-northeast-1

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

[Choose bucket](#)

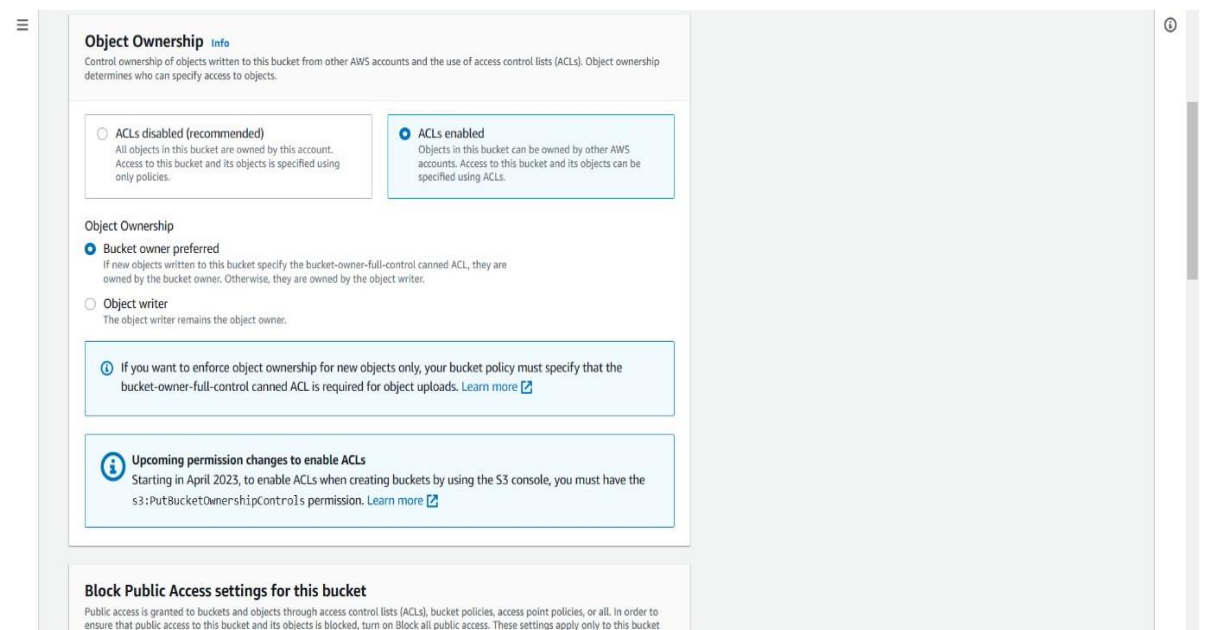
Object Ownership [Info](#)

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.

4. Then click on ACLs enabled.



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](#)

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.

5. Then don't click on "Block all public access".

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.

6. Then click on Create bucket.

No tags associated with this bucket.

Add tag

Default encryption

Info

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

Encryption key type

Info

☒ Amazon S3-managed keys (SSE-S3)

☐ AWS Key Management Service key (SSE-KMS)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS.
[Learn more](#)

☐ Disable

☒ Enable

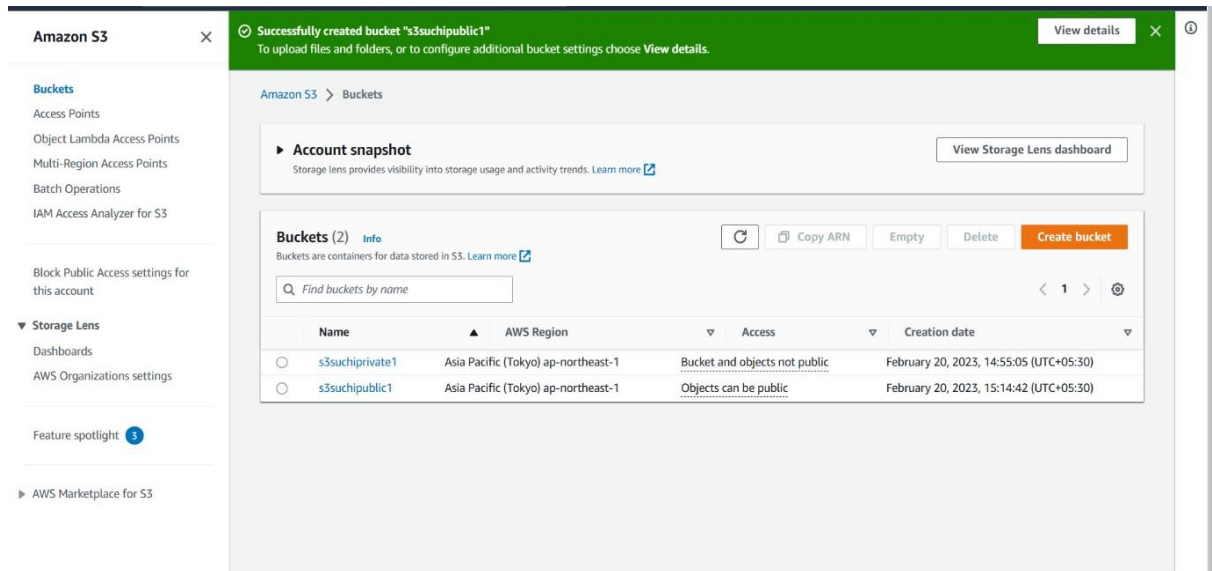
► Advanced settings

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

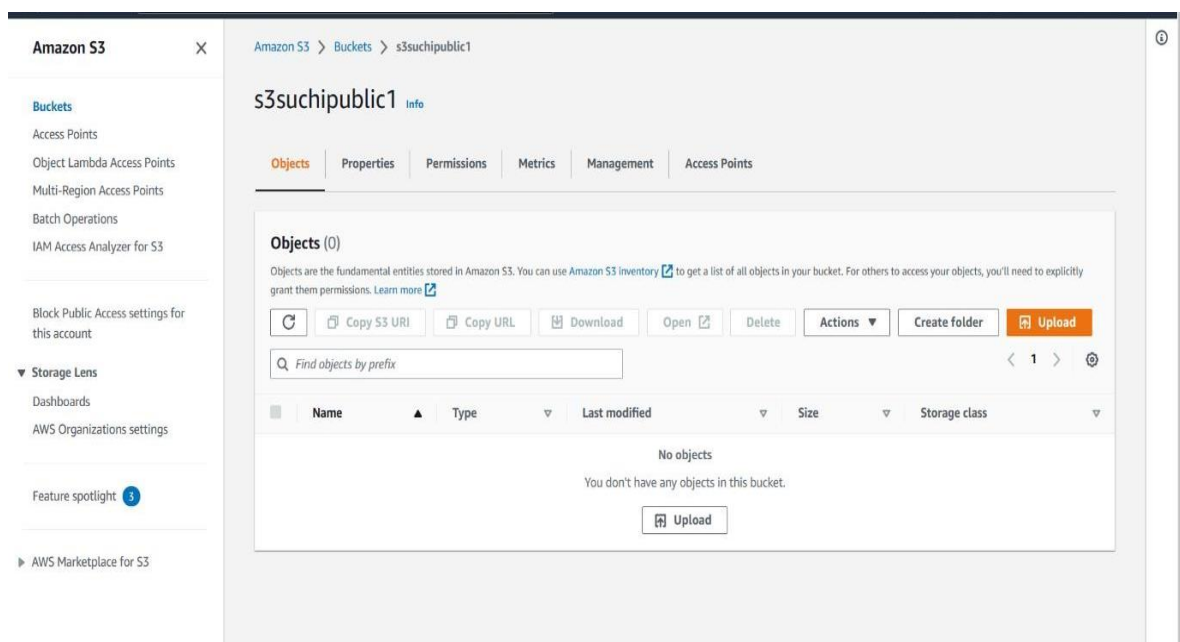
Cancel

Create bucket

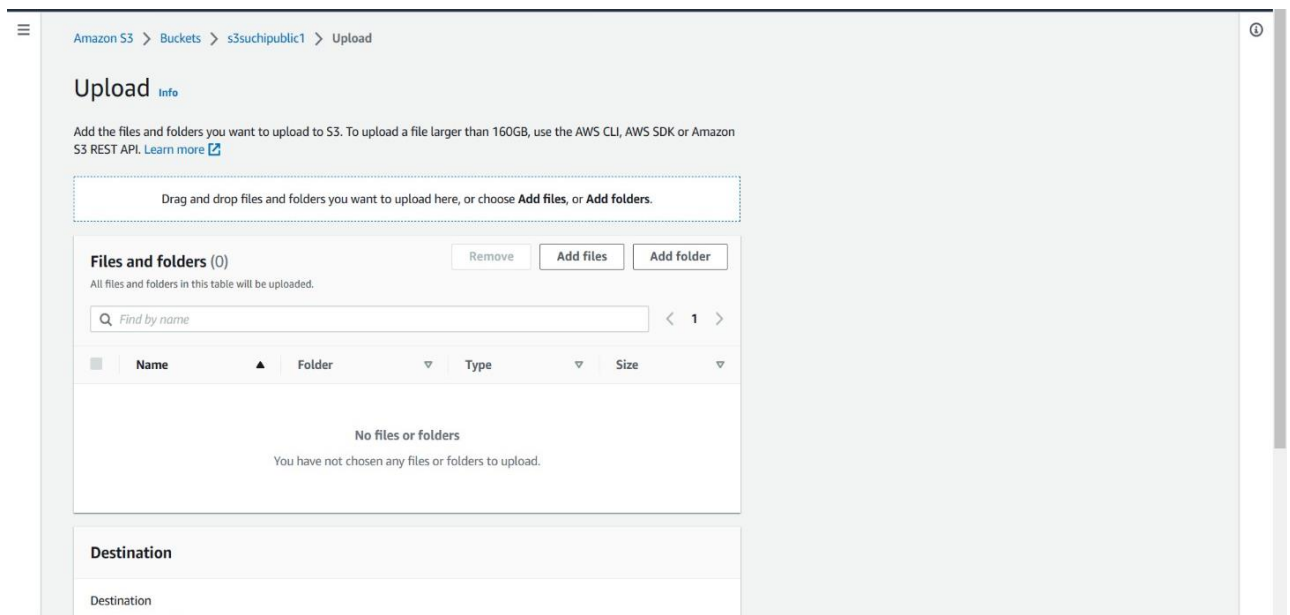
7. Successfully created public bucket. Then click on bucket which is created.



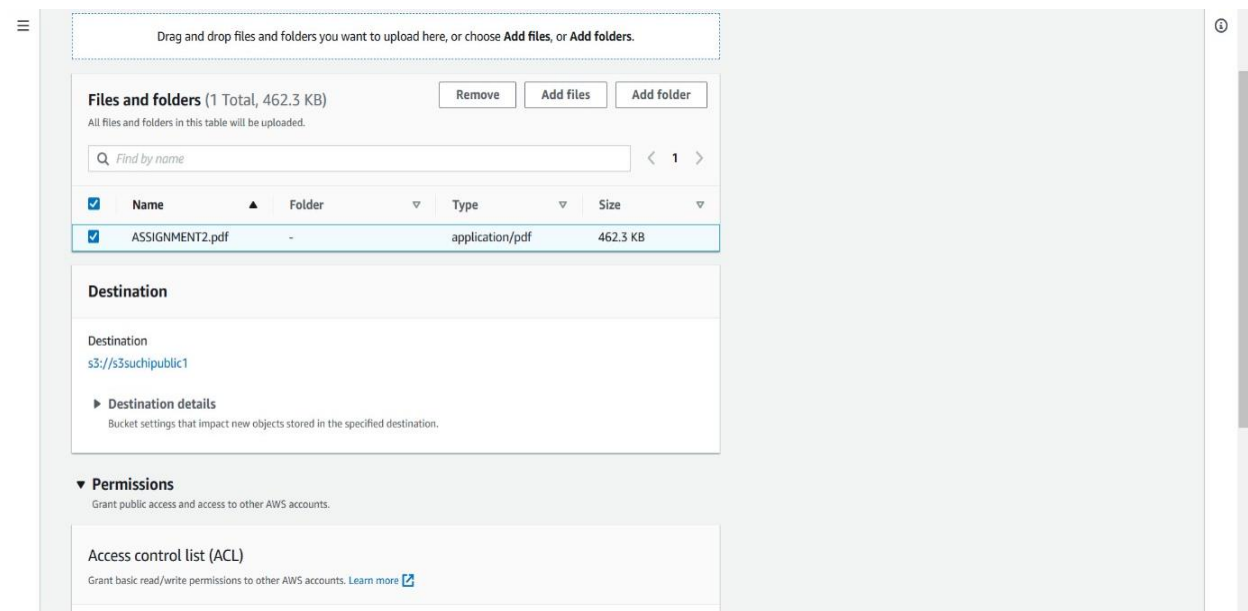
8. Then click on Upload and upload a file or a folder.



9. Then click on Add files and choose the file.



10. Then check on that file which you have chosen then click on upload.



11. Successfully file is uploaded. Then click on that file.

Upload: status Close

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

Summary

Destination s3://s3suchipublic1	Succeeded 1 file, 462.3 KB (100.00%)	Failed 0 files, 0 B (0%)
------------------------------------	---	-----------------------------

Files and folders (1 Total, 462.3 KB)

Find by name

Name	Folder	Type	Size	Status	Error
ASSIGNMENT2.pdf	-	application/pdf	462.3 KB	Succeeded	-

12. Then copy the URL

Amazon S3 × Amazon S3 > Buckets > s3suchipublic1 > ASSIGNMENT2.pdf

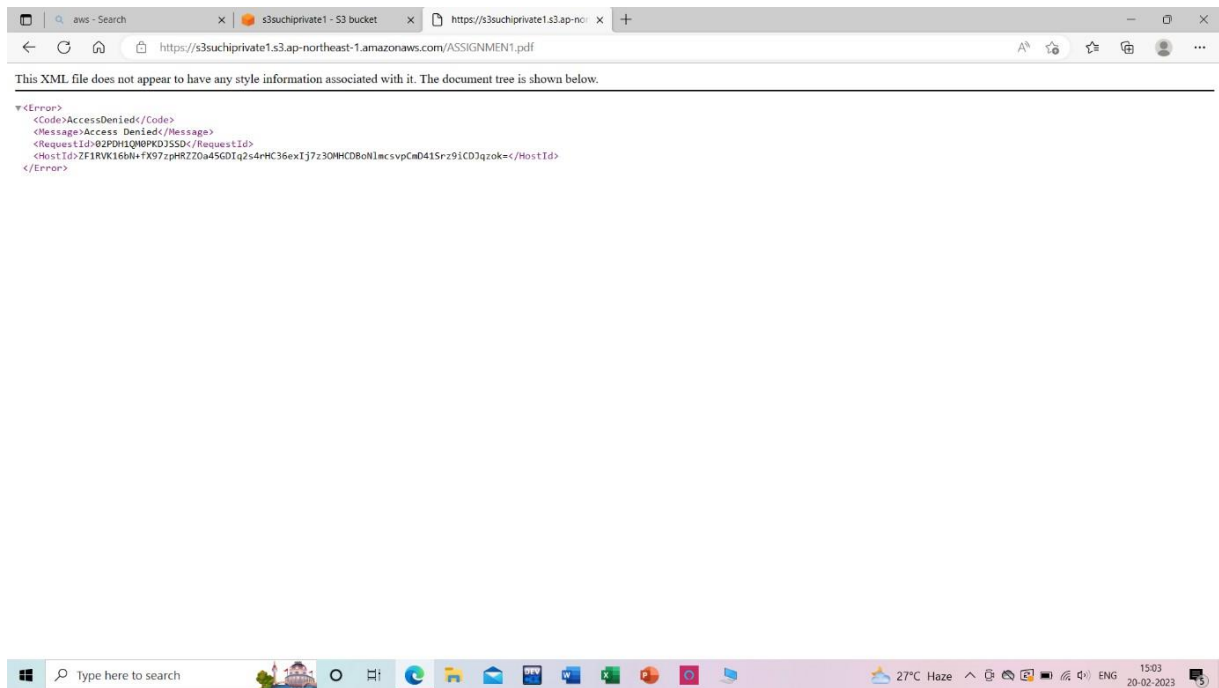
ASSIGNMENT2.pdf Info Copy S3 URI Download Open Object actions

Properties Permissions Versions

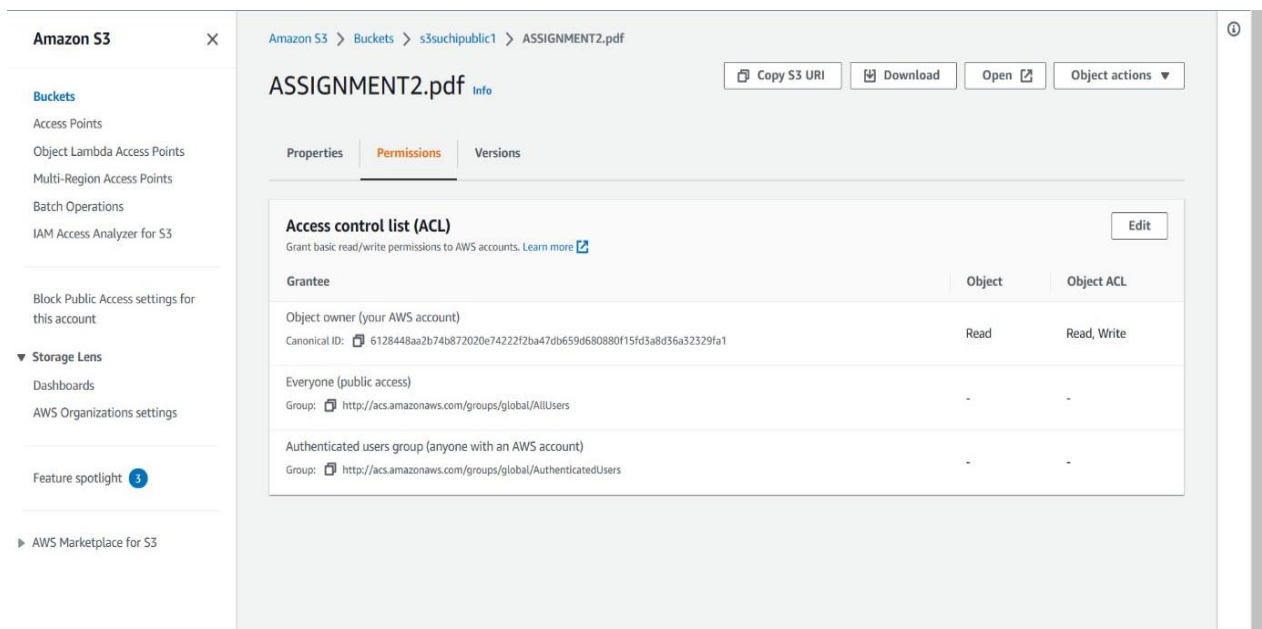
Object overview

Owner kumarisuchi569	S3 URI s3://s3suchipublic1/ASSIGNMENT2.pdf
AWS Region Asia Pacific (Tokyo) ap-northeast-1	Amazon Resource Name (ARN) arn:aws:s3::s3suchipublic1/ASSIGNMENT2.pdf
Last modified February 20, 2023, 15:16:44 (UTC+05:30)	Entity tag (Etag) 601126db8a839580c85de8ac2bee4f0f
Size 462.3 KB	Object URL https://s3suchipublic1.s3.ap-northeast-1.amazonaws.com/ASSIGNMENT2.pdf
Type pdf	
Key ASSIGNMENT2.pdf	

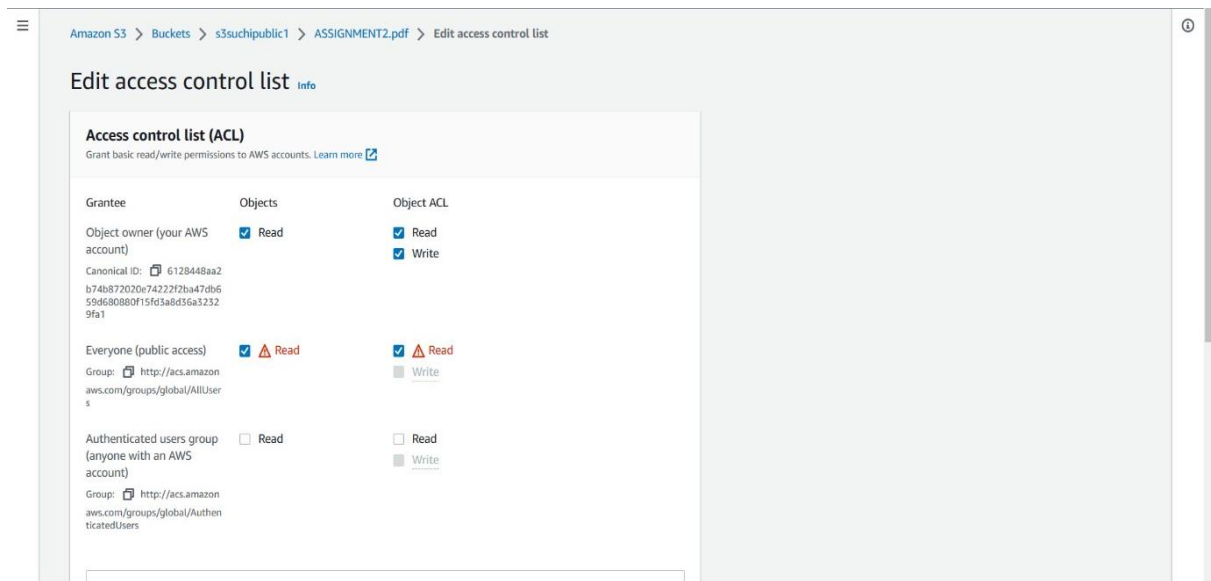
13. Then paste it to another browser, no one can access it. Error is shown.



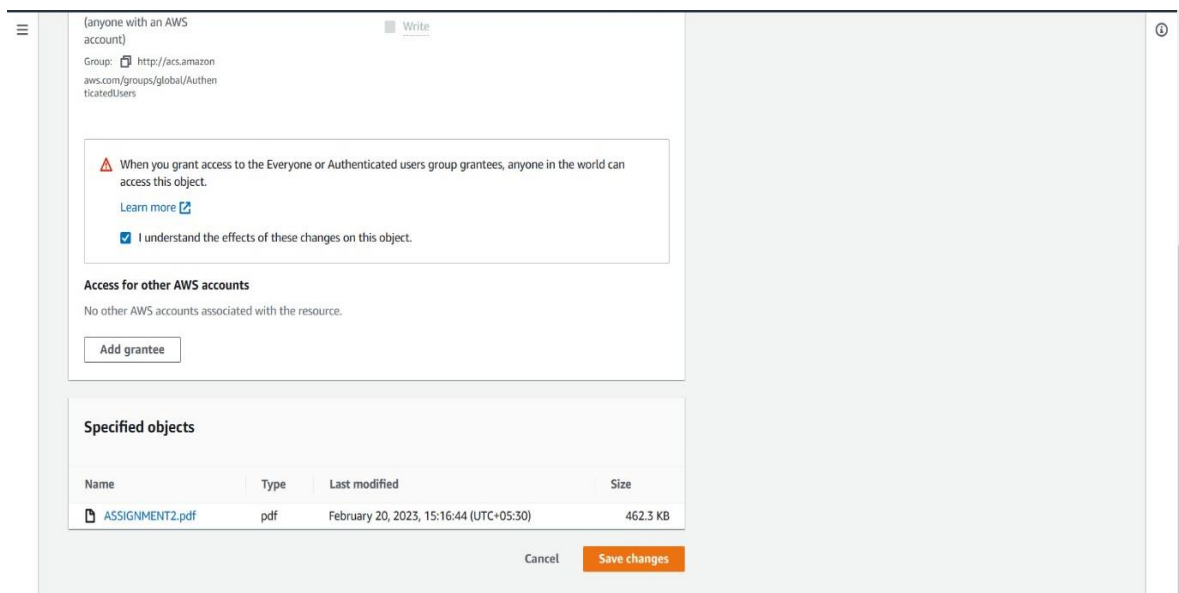
14. Then click on Permissions and then click on Edit.



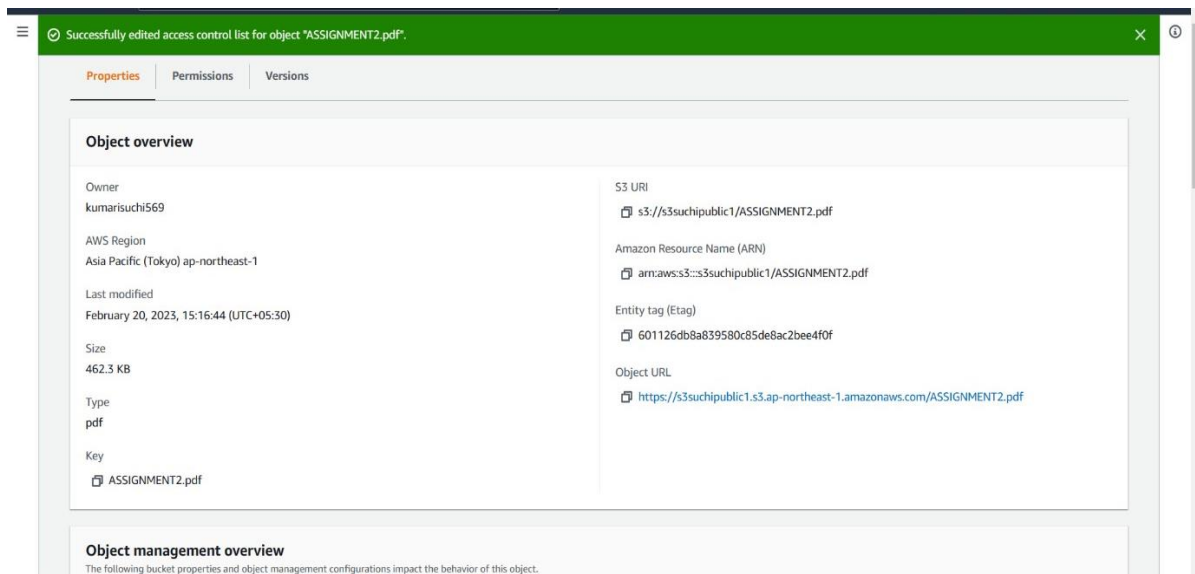
15. Then check on Read option for Everyone(public access).



16. Then click on Save changes. Now the file can be viewed.



17. Then copy the URL.



18. Then paste it to another browser. So the file is opened.

