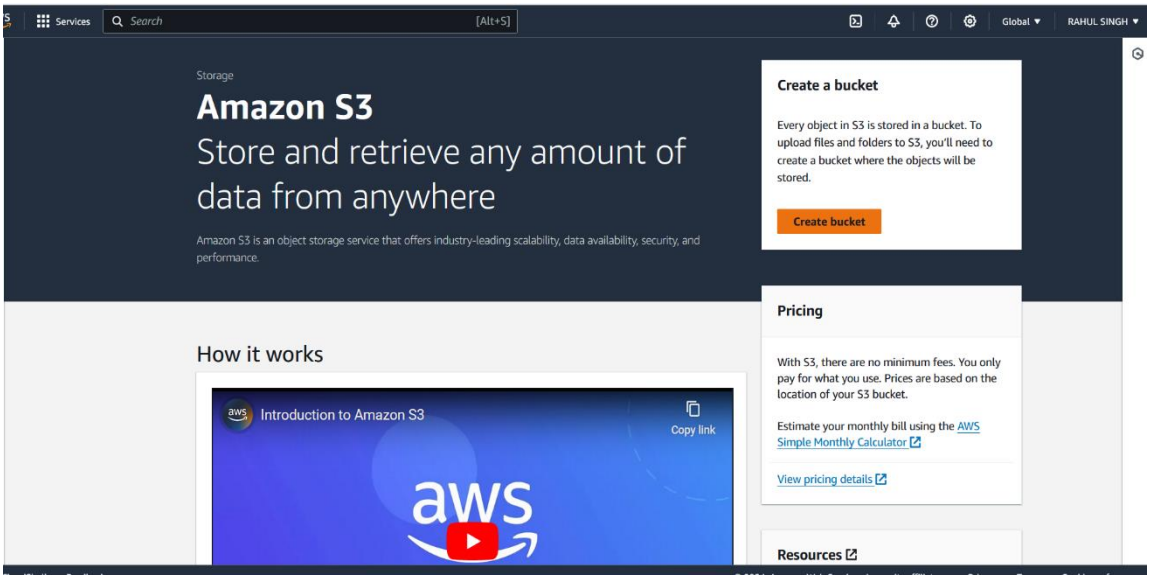
ASSIGNMENT 6

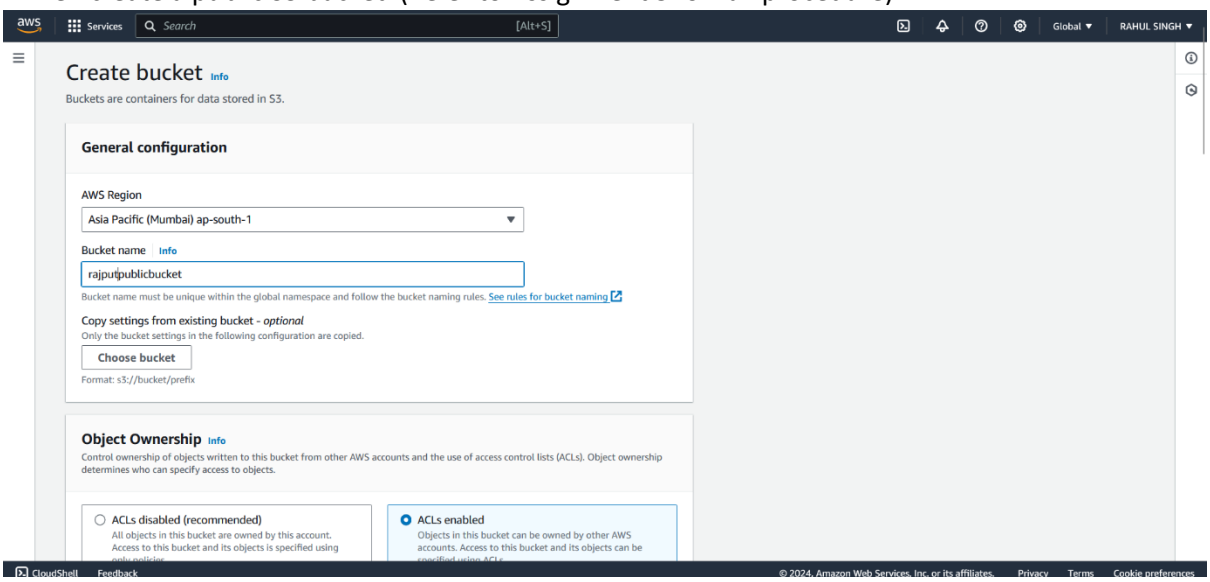
Problem Statement: Upload a static website on S3.

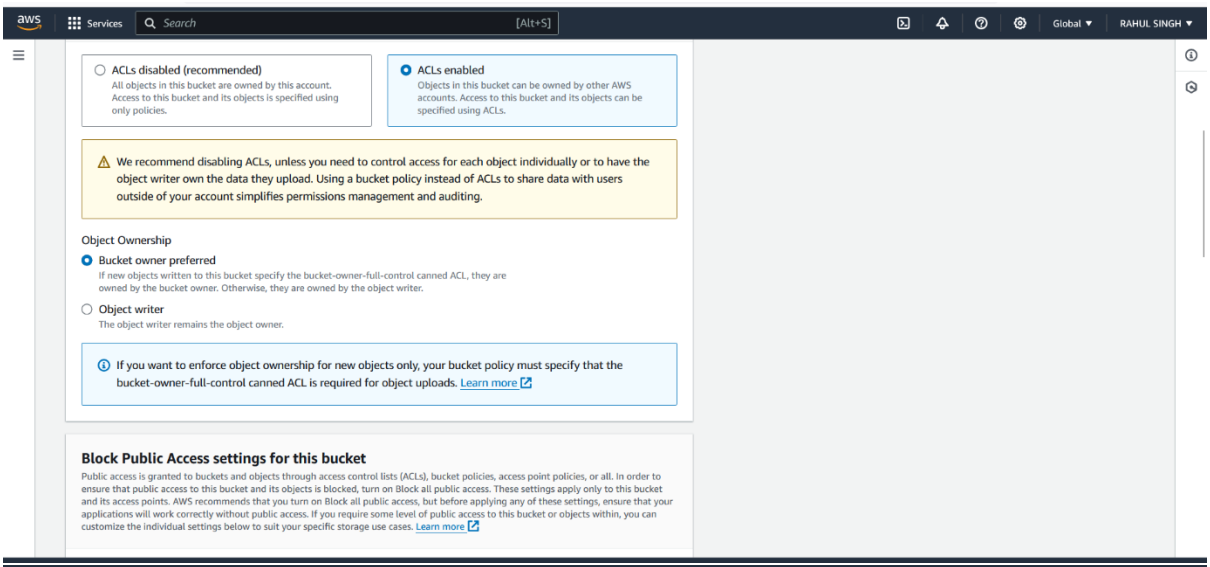
Procedure:

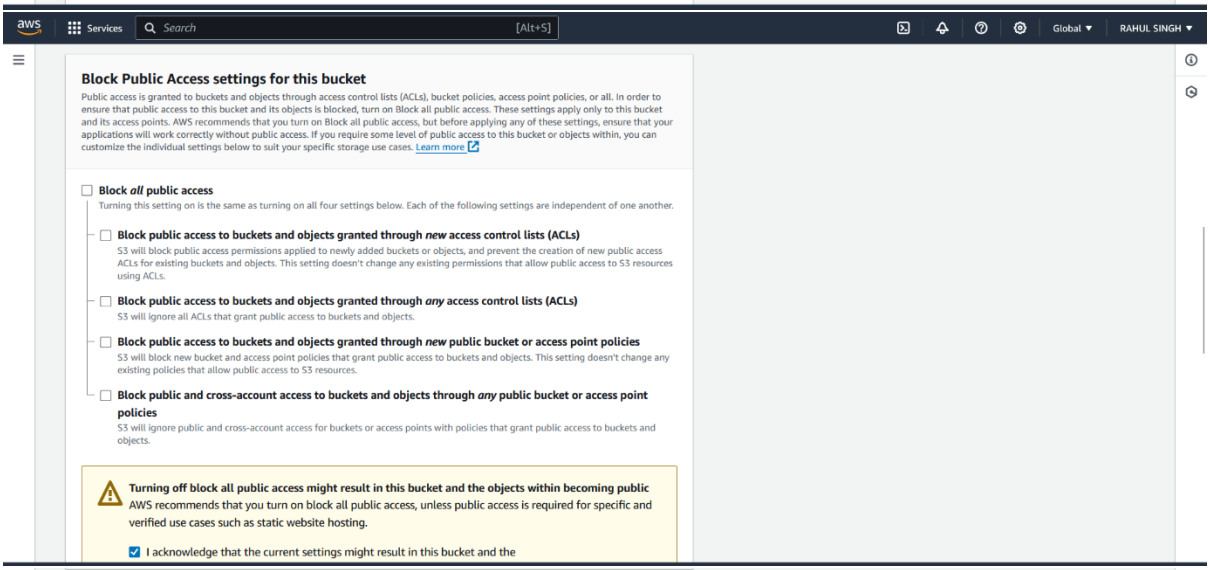
1. Sign in to your AWS account as a root user.

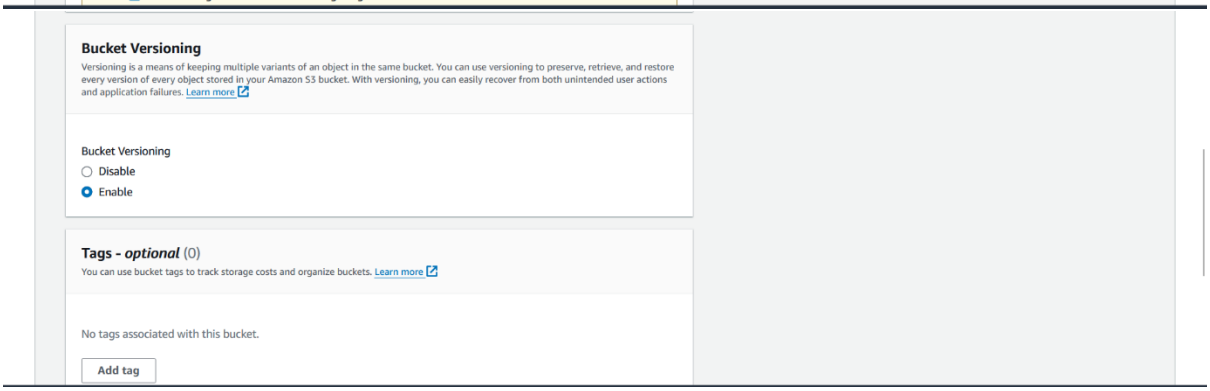


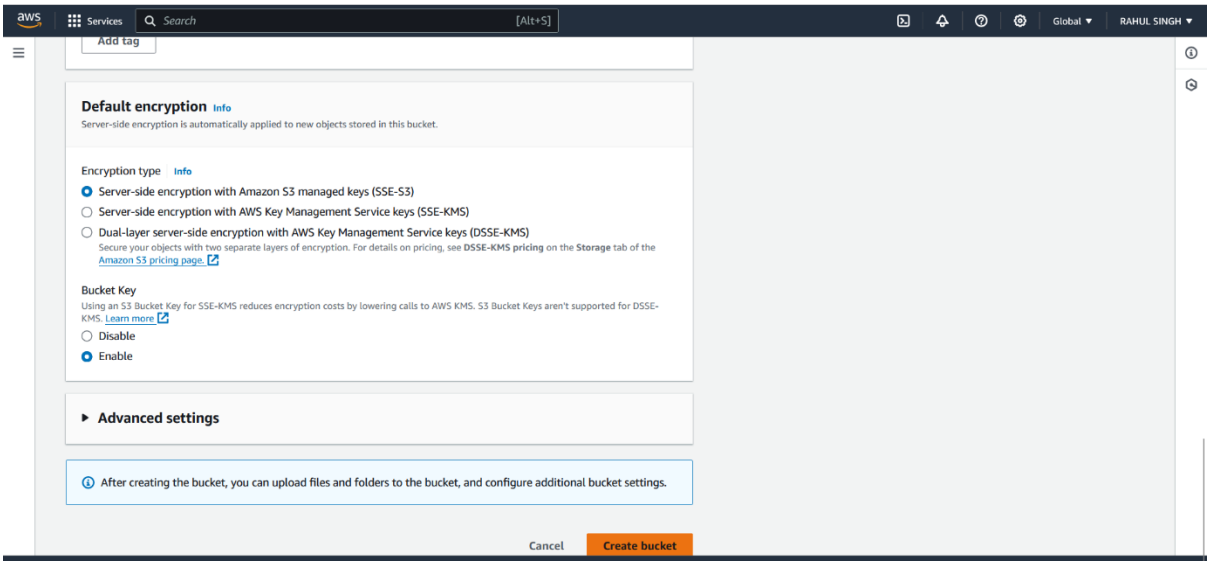
2.Then create a public S3 bucket. (Refer to Assignment 5 for full procedure)

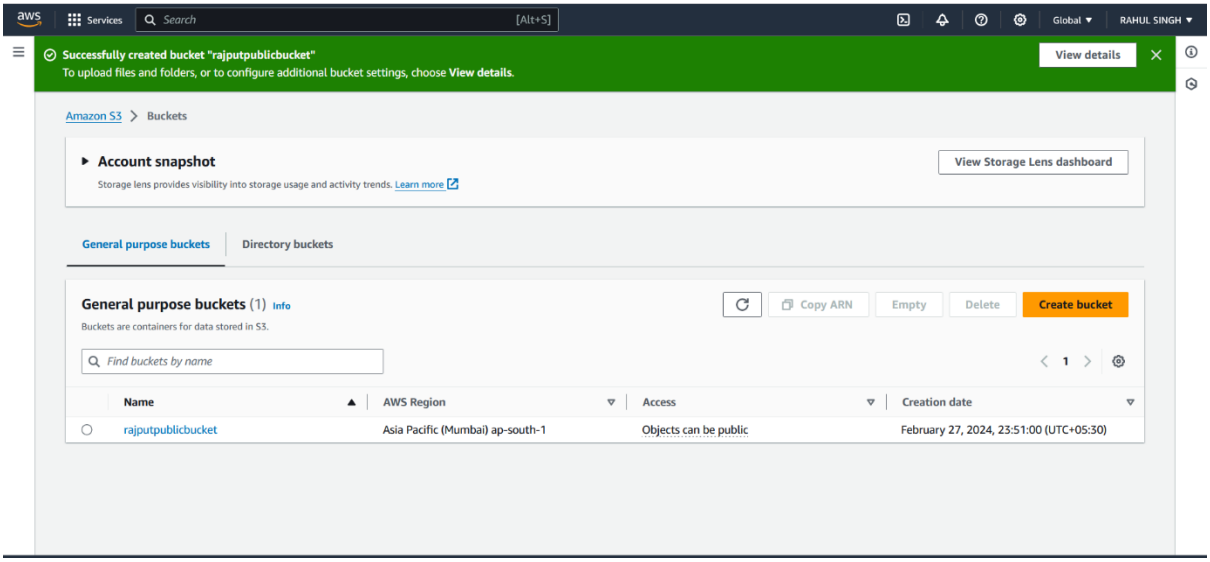



aws
Services
Search
[Alt+S]
Global
RAHUL SINGH
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its 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.
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
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


aws
Services
Search
[Alt+S]
Global
RAHUL SINGH
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


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 (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag





3. Now create three html files anywhere in your computer (preferably in a folder in the Desktop).

a. The first one is named page1.html

b. The second one is named page2.html

c. The third one is named index.html

Remember, you can give any name to the files but you have to modify the steps shown further accordingly. We are going to use the given file names to proceed.

The contents of the files are shown in the given snapshots.....

File Edit View

```
<html>
<head>
<title>About Page</title>
</head>
<body>
<h1>Services</h1>
<a href = "page1.html">Services</a>
<h1>Index</h1>
<a href = "index.html">index</a>
</body>
</html>
```

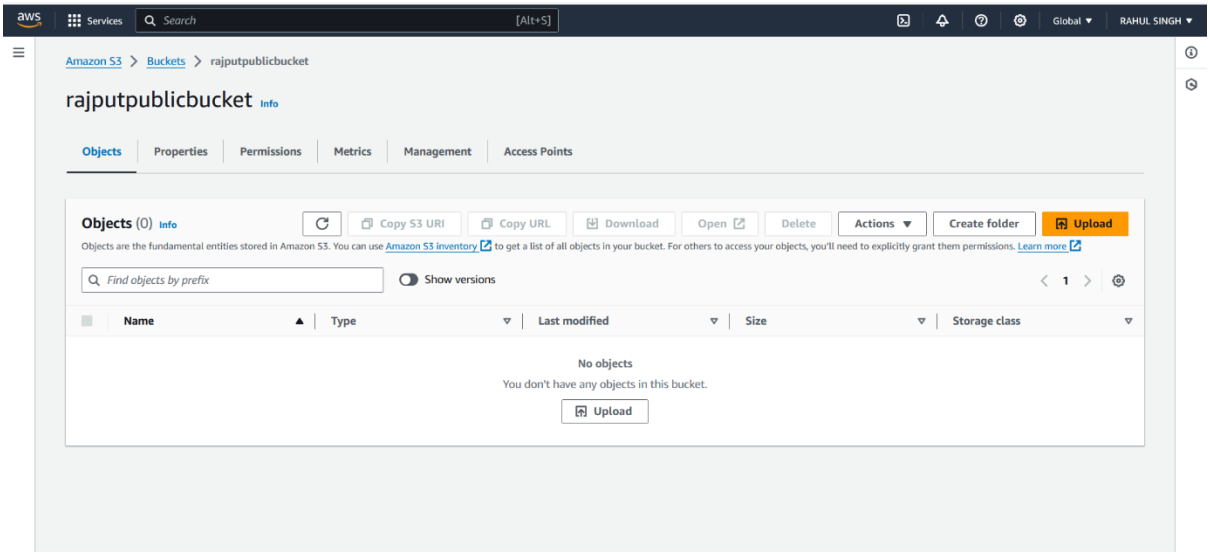
File Edit View

```
<html>
<head>
<title>Service Page</title>
</head>
<body>
<h1>index</h1>
<a href = "index.html">Services</a>
<h1>About</h1>
<a href = "page2.html">About</a>
</body>
</html>
```

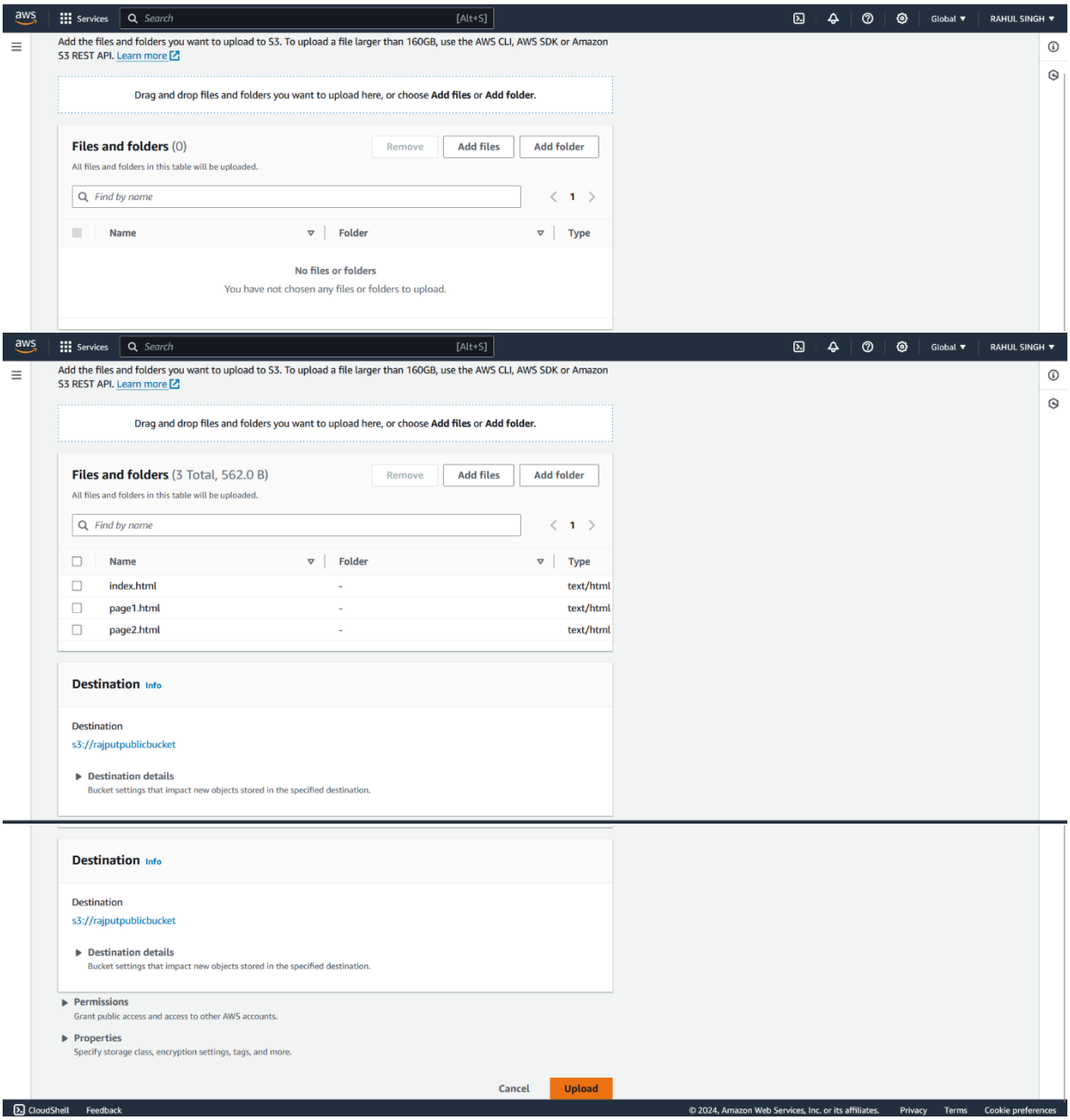
File Edit View

```
<html>
<head>
<title>Index Page</title>
</head>
<body>
<h1>Services</h1>
<a href = "page1.html">Services</a>
<h1>About</h1>
<a href = "page2.html">About</a>
</body>
</html>
```

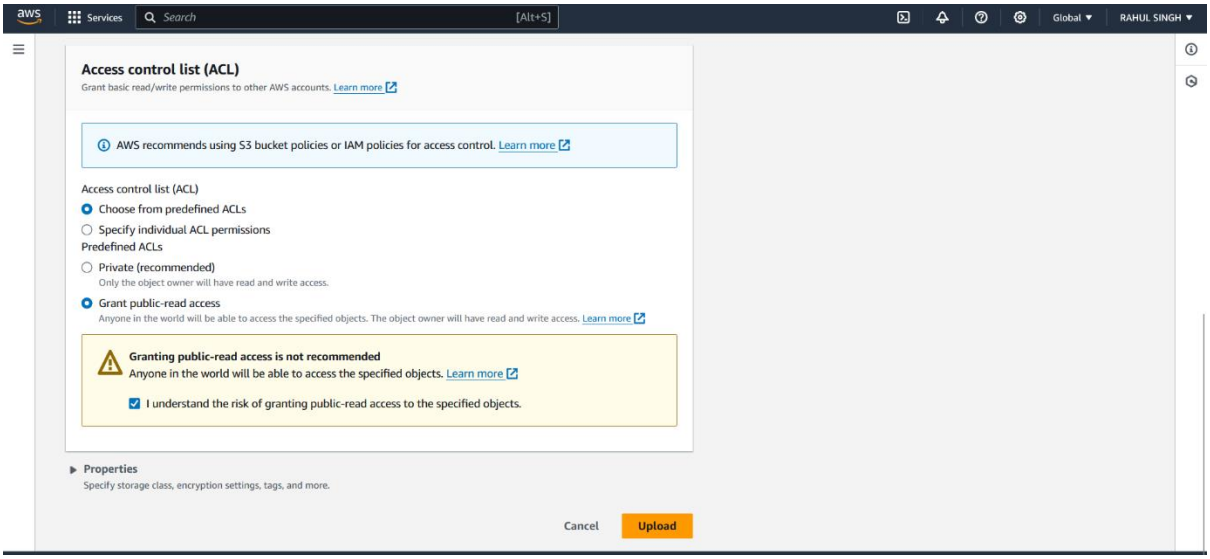
4. Now let us go back to AWS. Select the newly created public bucket.
5. Click the upload button.

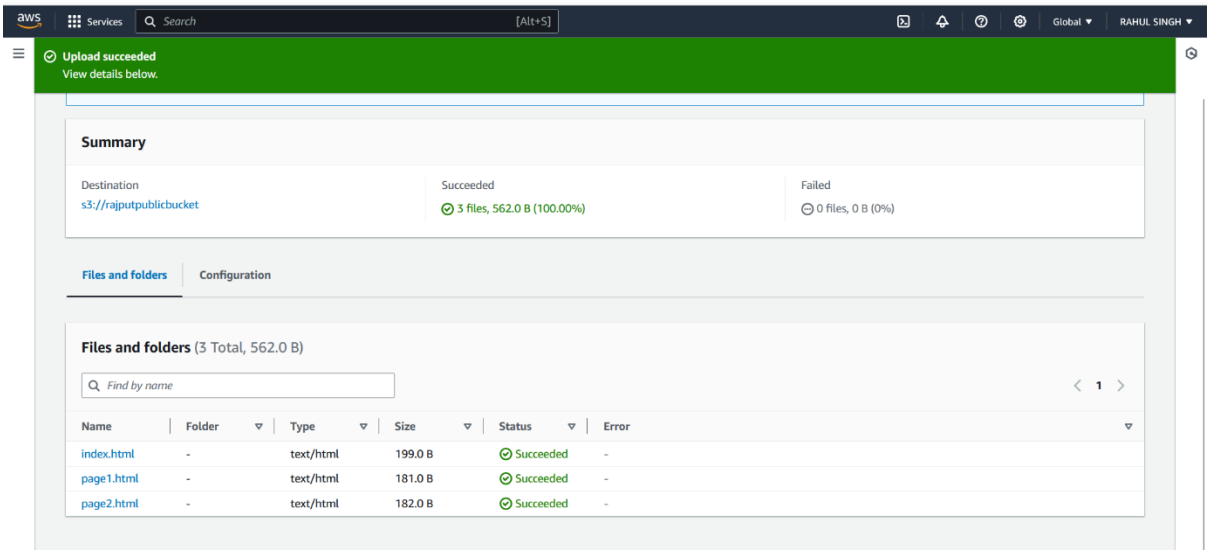


6. Next click on the add files button. Select all the three html files and upload them by pressing the upload button.

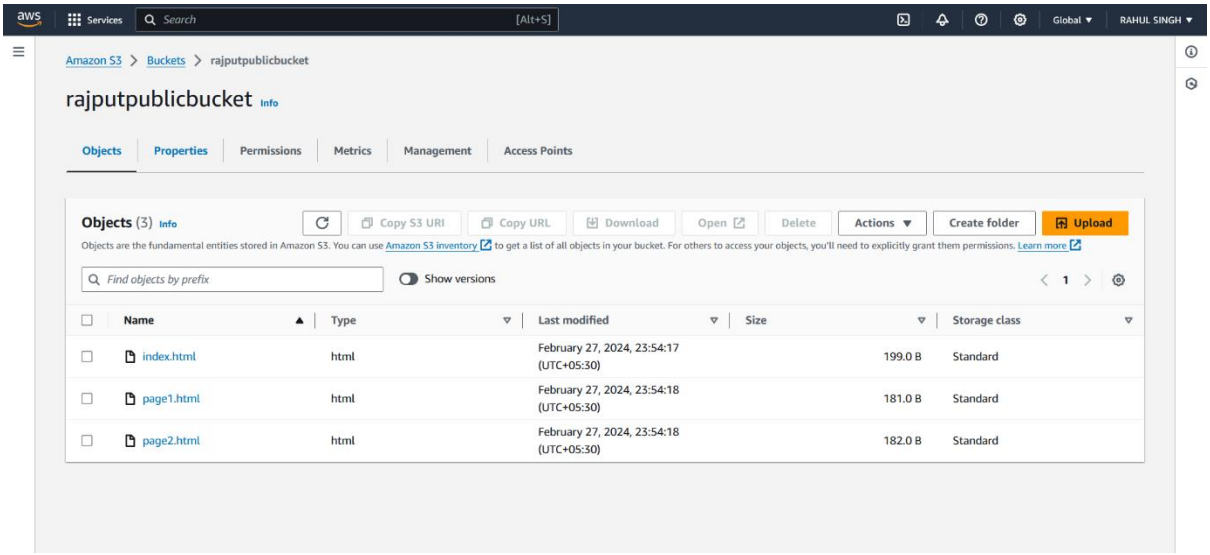


8. Click on the actions button and from the subsequent dropdown menu select Make public using ACL.





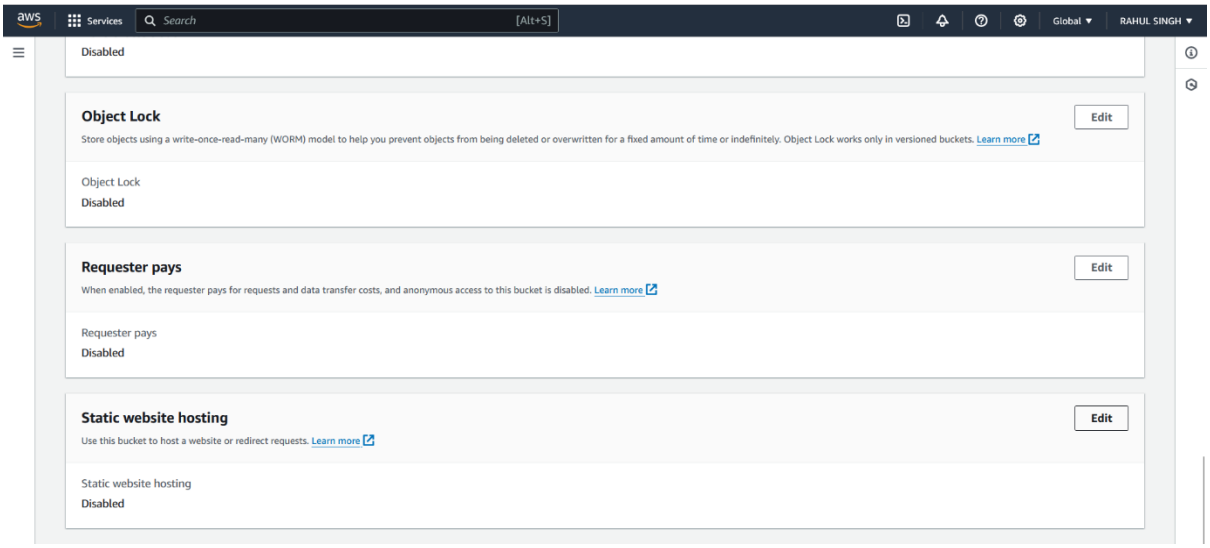
10. Now, we after making public we close the status page and we are redirected to our public bucket page. Now we select the properties tab of the bucket which is located in the right side of the objects tab (in orange font).



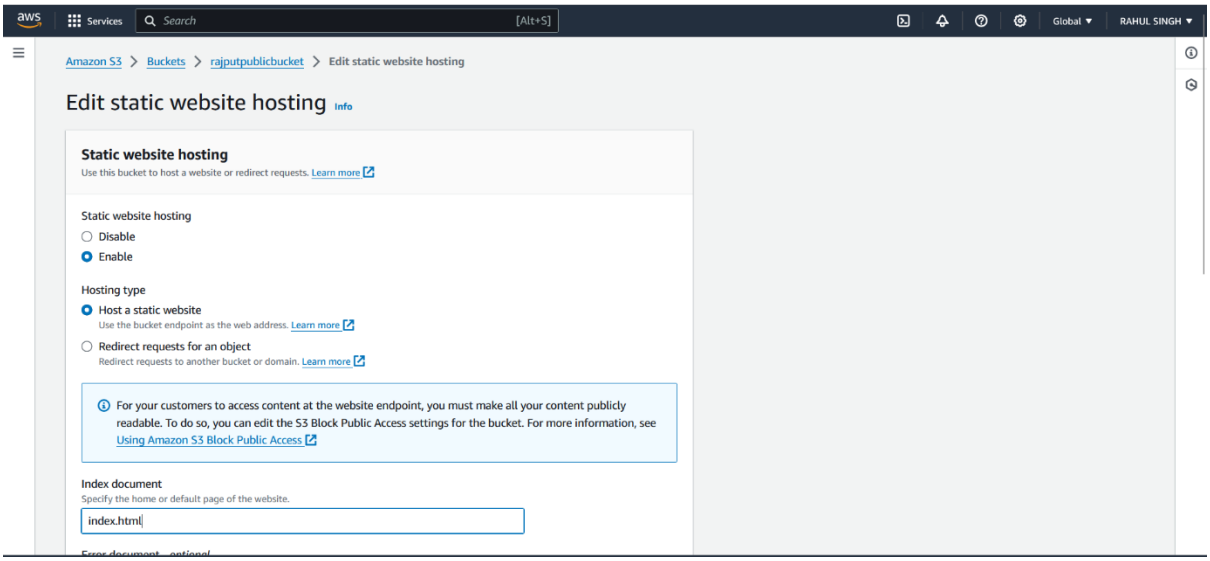
11. After arriving in the properties tab. Scroll down all the way to the bottom. We will focus only on the Static website hosting section.

By default, it will show disabled.

We have to enable it. In order to do so click on the Edit button on the right-hand side of the section.

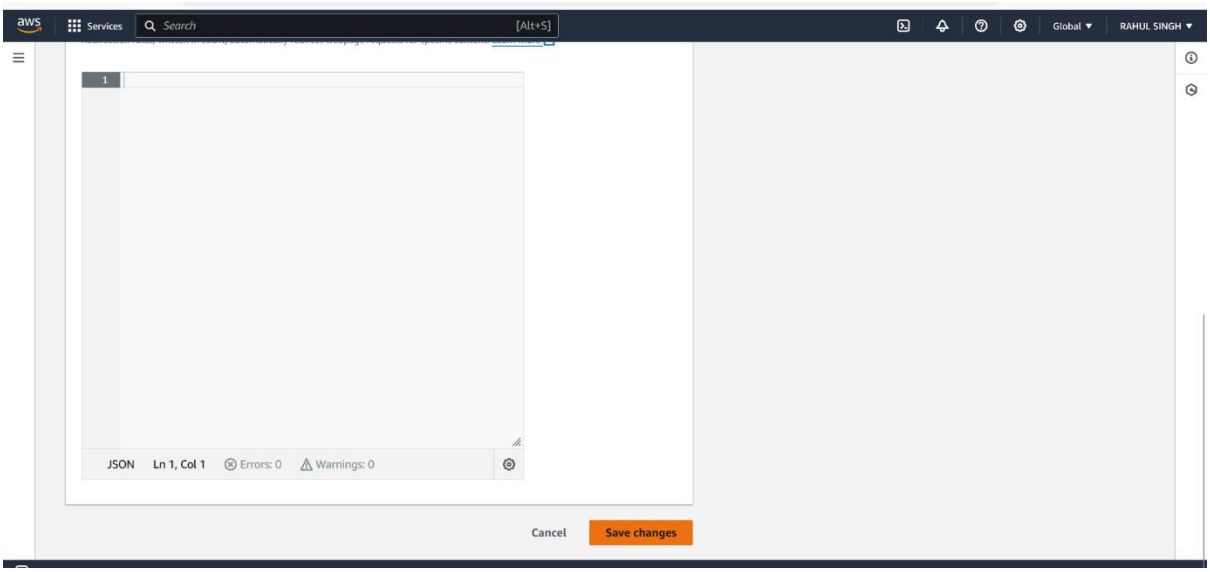


12. Now we will choose the enable option. After choosing it multiple options will appear. Just follow the snapshot provided below and make the same changes.

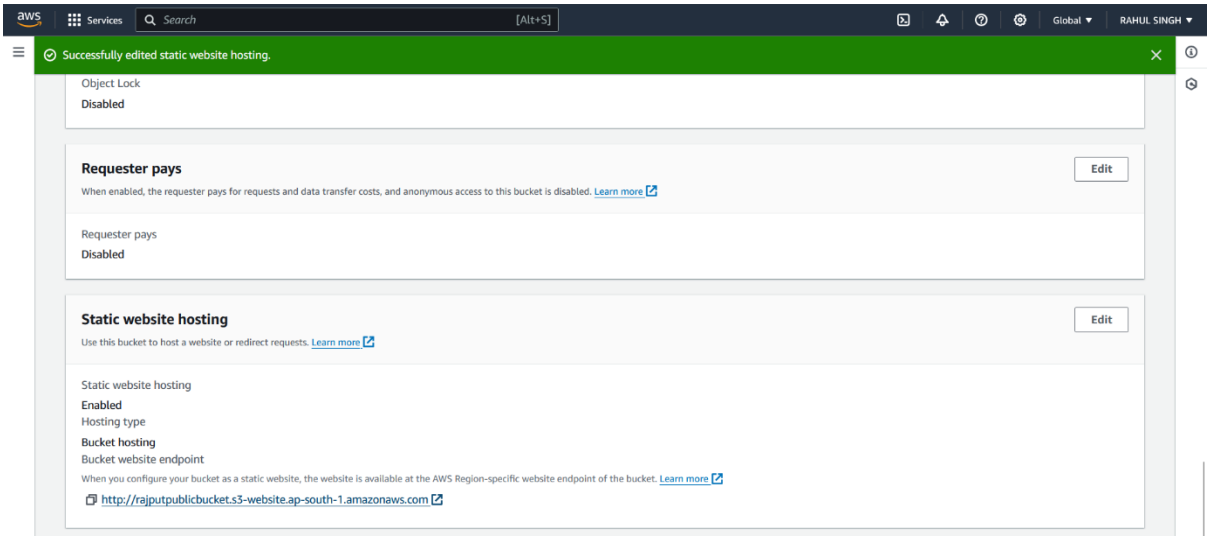


13. Next scroll down. Now we have to mention the html document our link will show. This is the one which anyone can access using the bucket link. In our case we will mention index.html as our index or main html file. You can choose according to your wish and design.

14. Next scroll down and click on save changes button.



15. Now, you will again arrive in the bucket's properties tab. Scroll down to the static website hosting area. Now you can see a link has arrived.



16. Copy the link and paste it in another browser.