

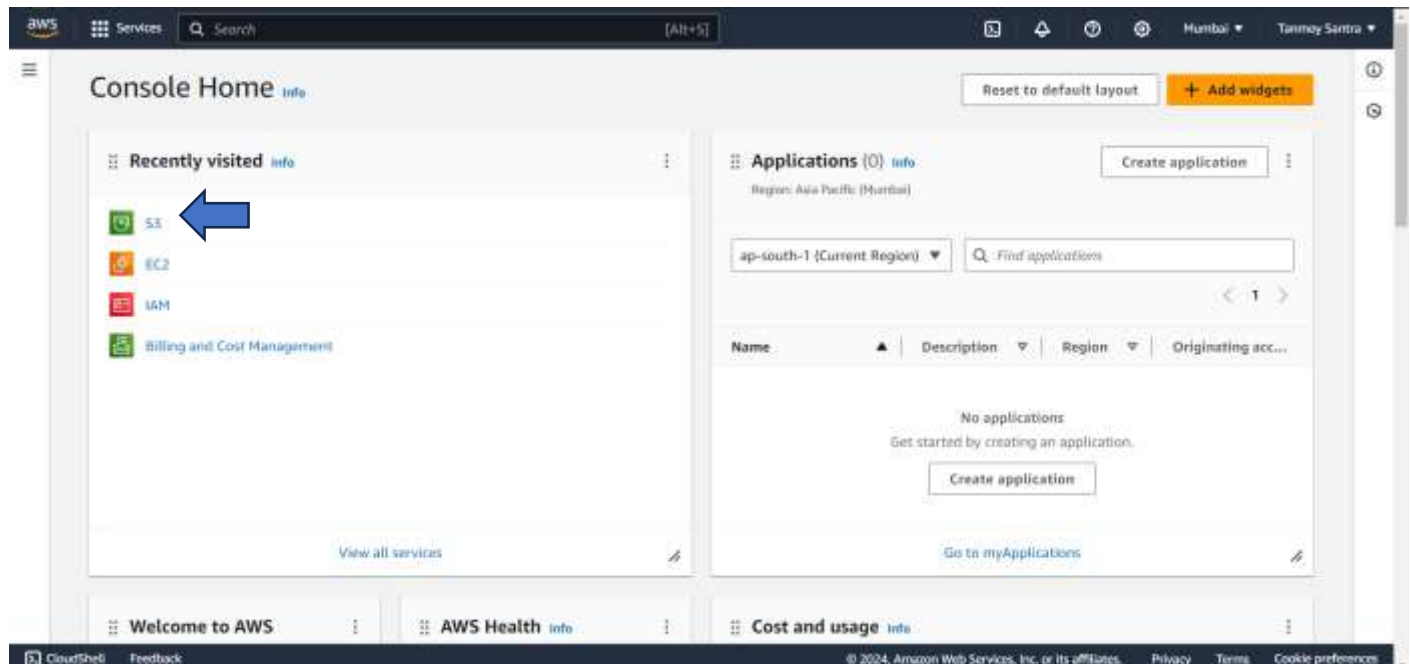
ASSIGNMENT - 6

PROBLEM STATEMENT : Upload a static website on S3.

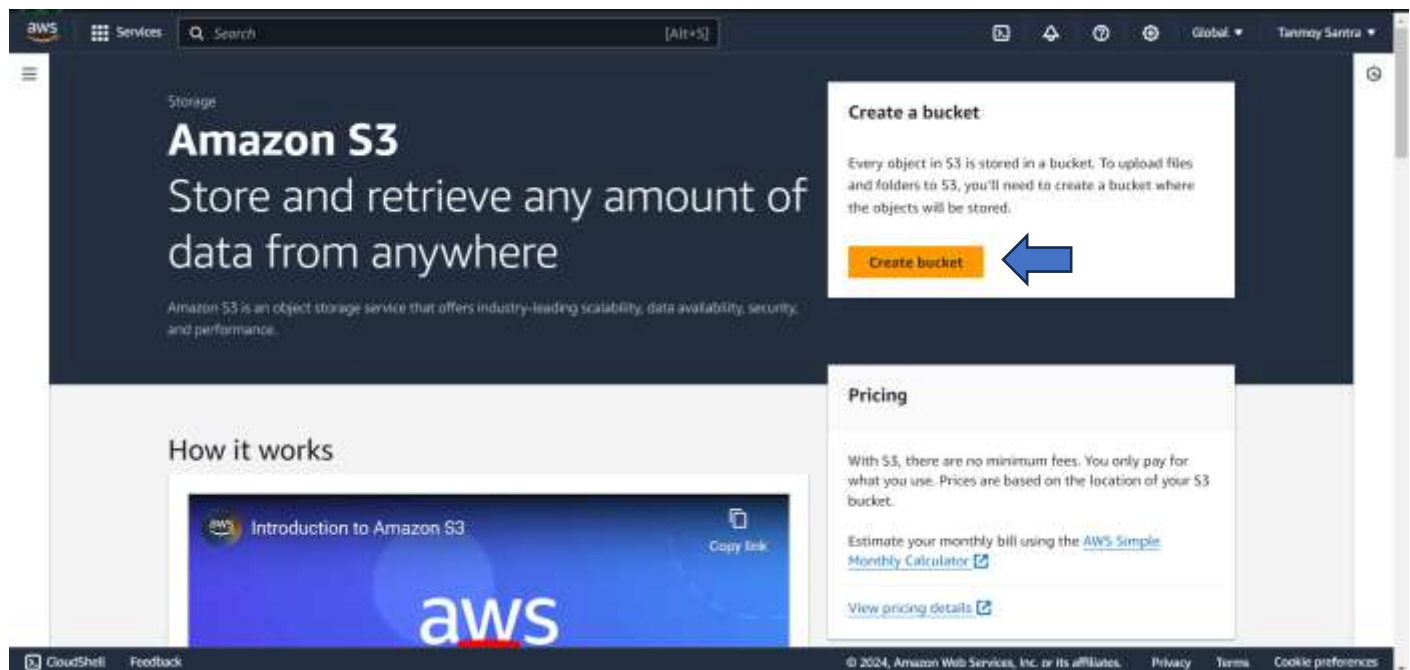
To upload the website -

STEP 1-Create 3 Static Webpages using HTML .

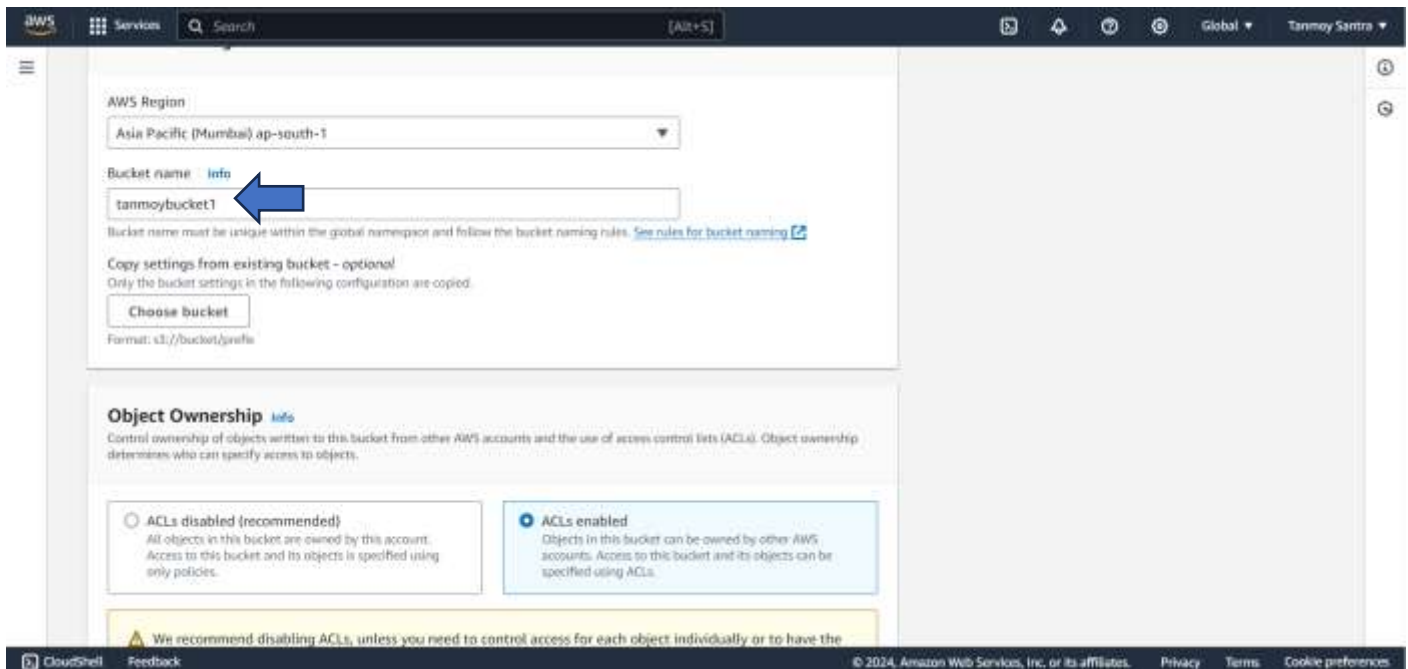
STEP 2- Click on the S3 button.



STEP 3- Click on “Create Bucket”.



STEP 4- Give name, and Select “ACLs enabled” option under the Object Ownership heading.



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

Bucket name: **tanmoybucket1** [info](#)

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.

Choose bucket

Format: v1././bucket/prefix

Object Ownership [info](#)

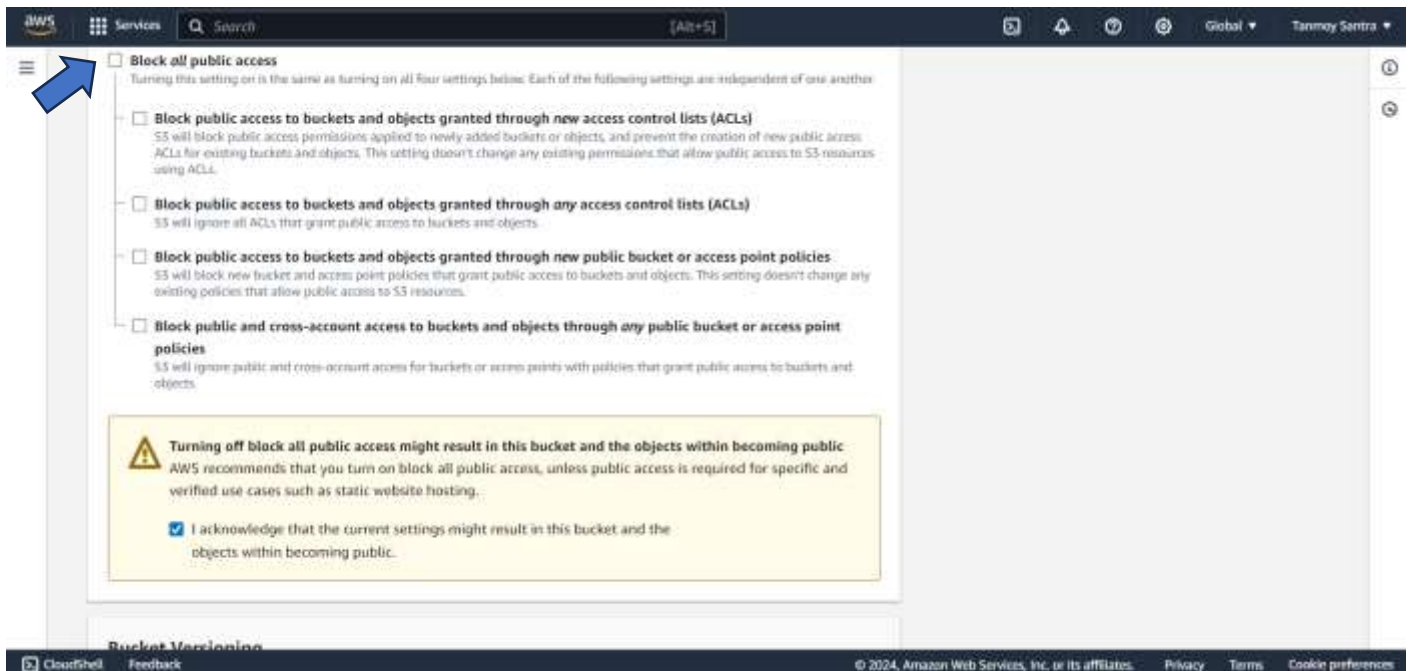
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☐ **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.

We recommend disabling ACLs, unless you need to control access for each object individually or to have the

STEP 5- Uncheck Block all public access & click the I acknowledge checkbox.



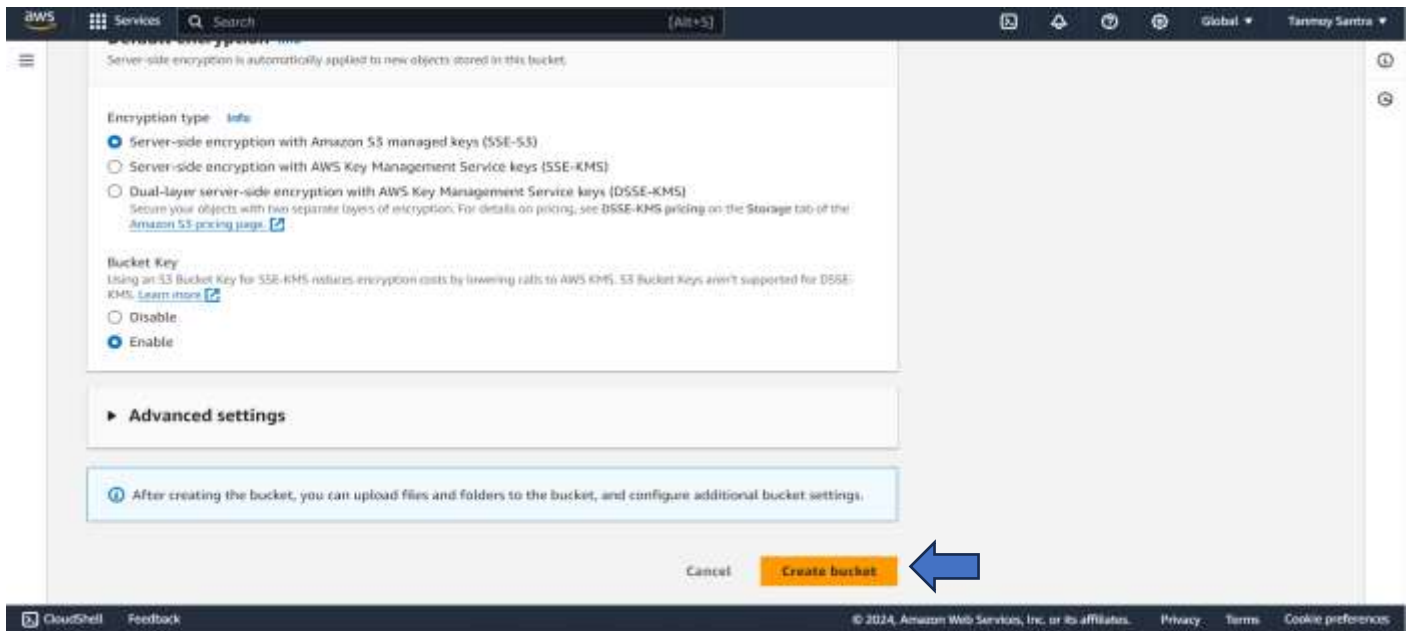
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **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.

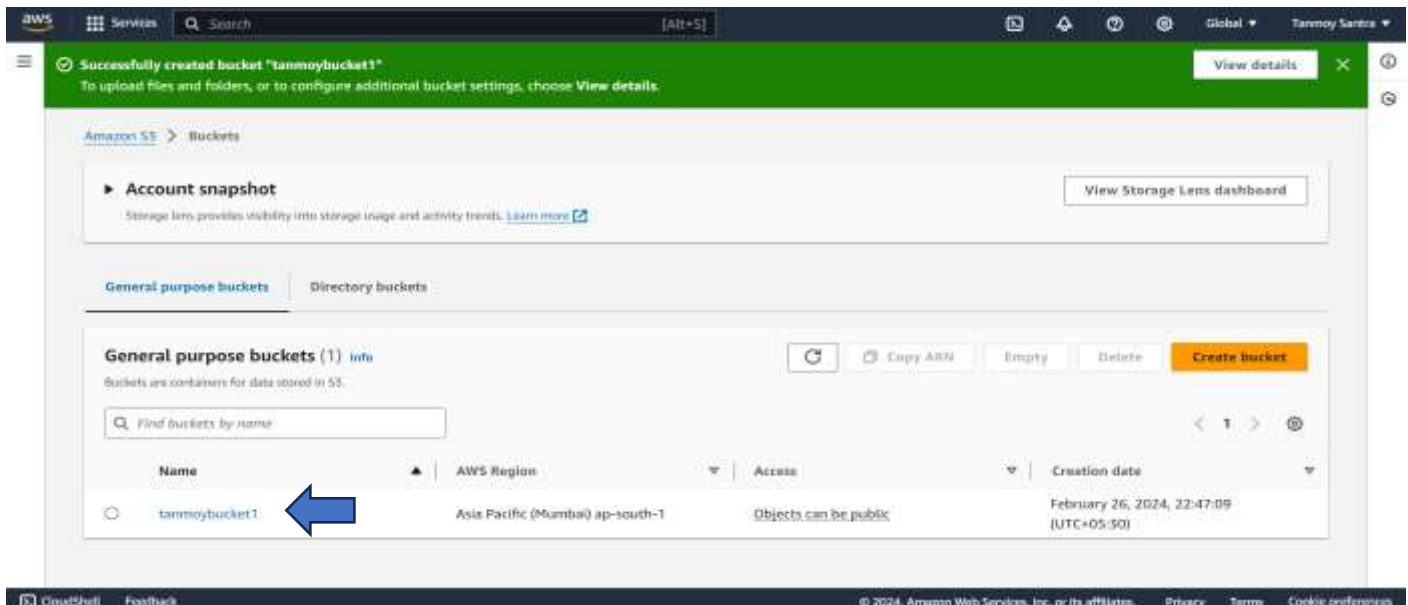
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ **I acknowledge that the current settings might result in this bucket and the objects within becoming public.**

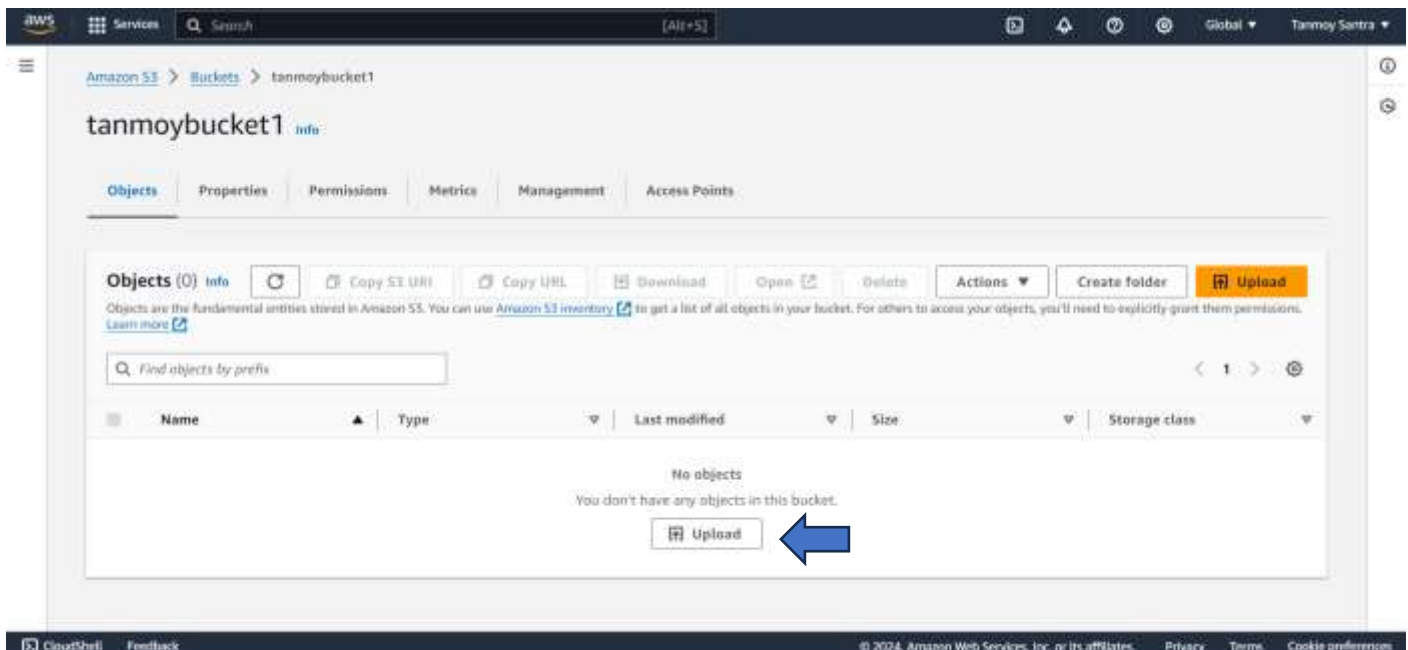
STEP 6- Click on Create Bucket.



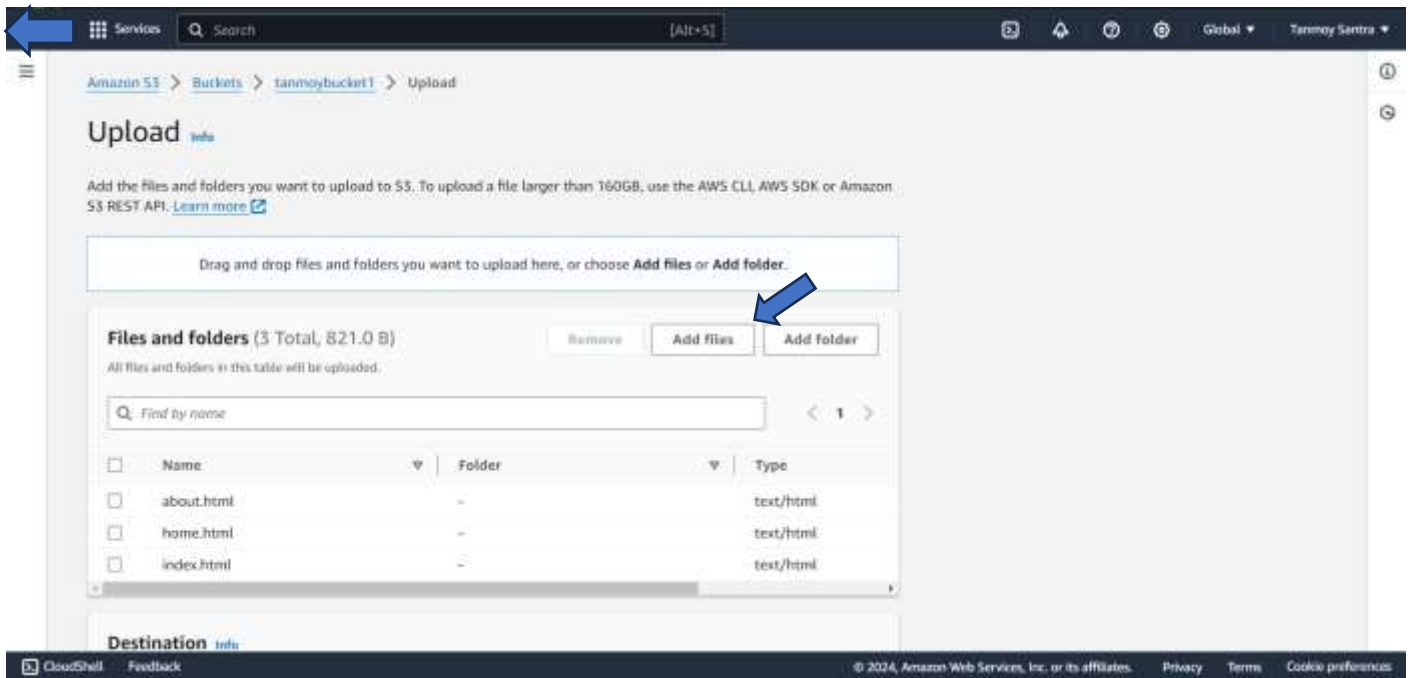
STEP 7- The Bucket is thus created successfully.



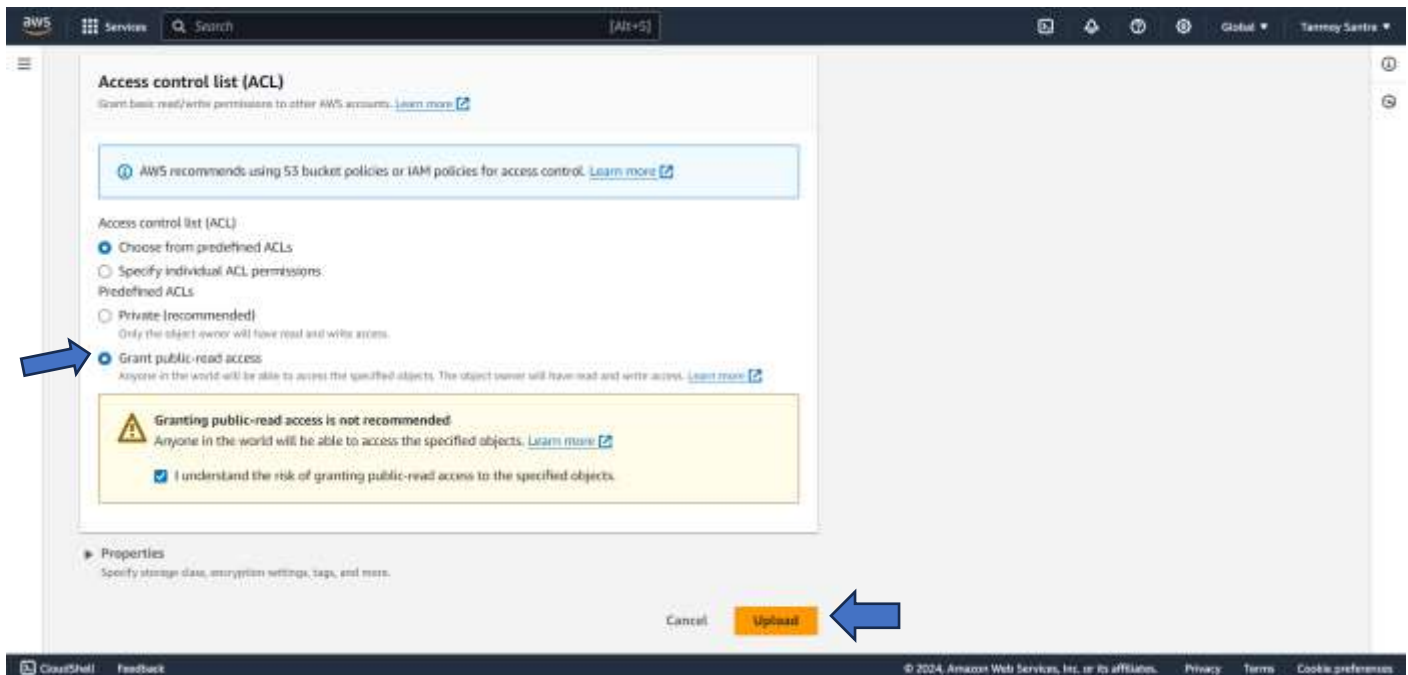
STEP 8- Click on the Upload.



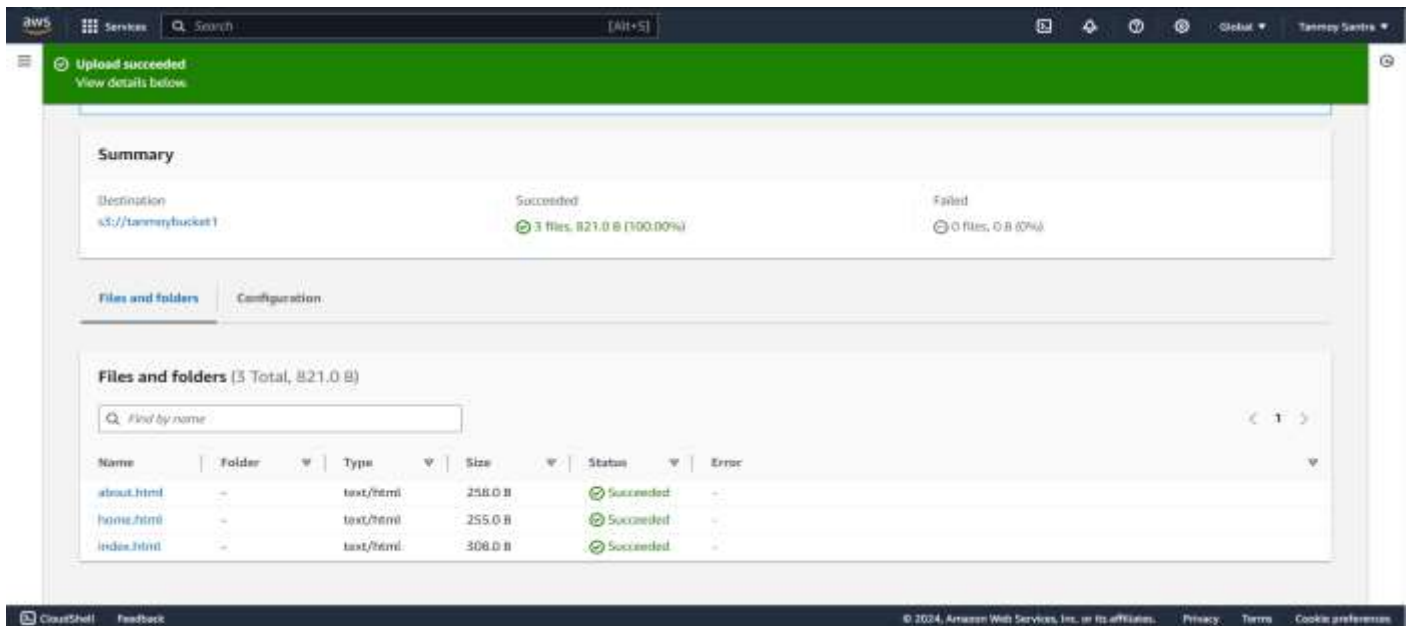
STEP 9- Click on Add file and add the html files.



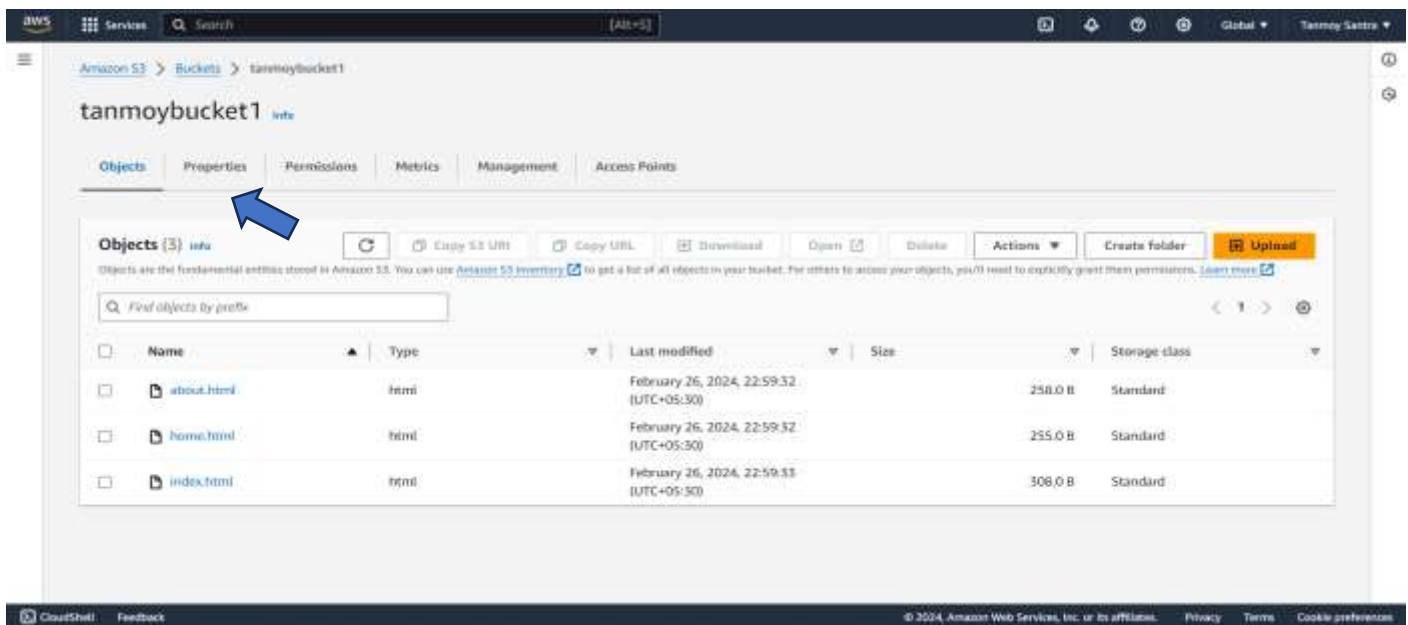
STEP 10- Select Granting Public Read Access option. Click the “I understand” then click Upload.



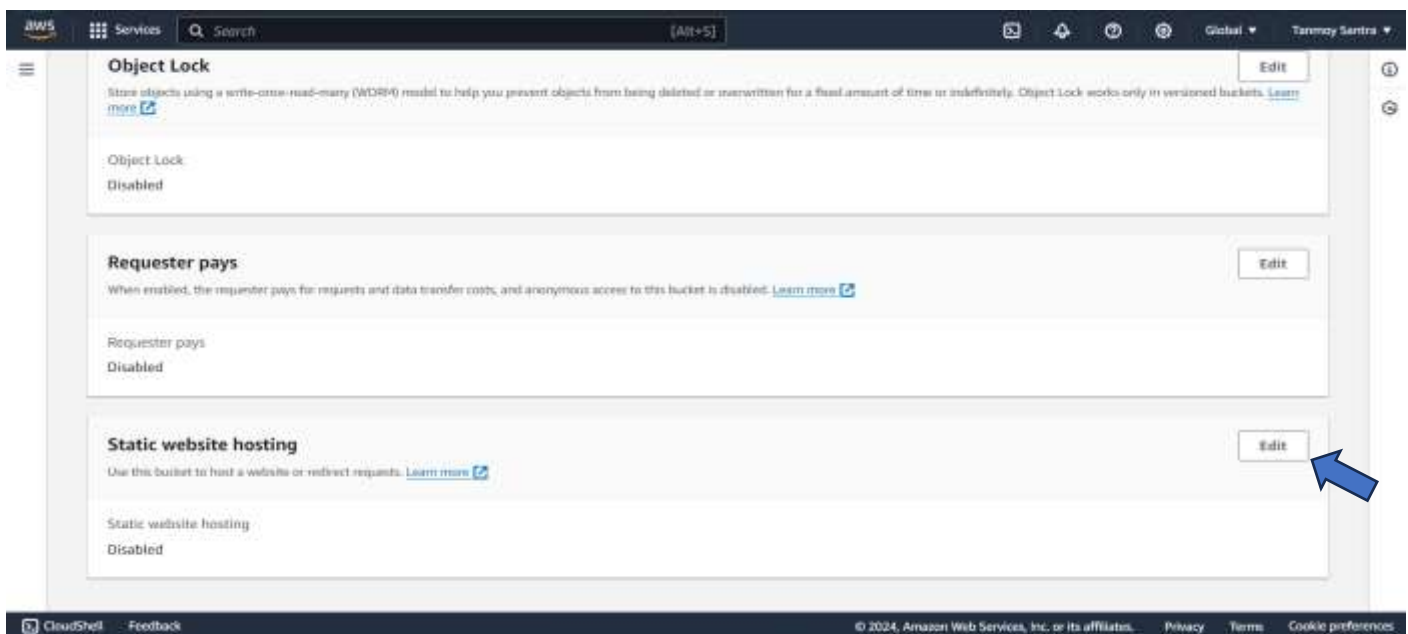
STEP 11- The file has been uploaded successfully.



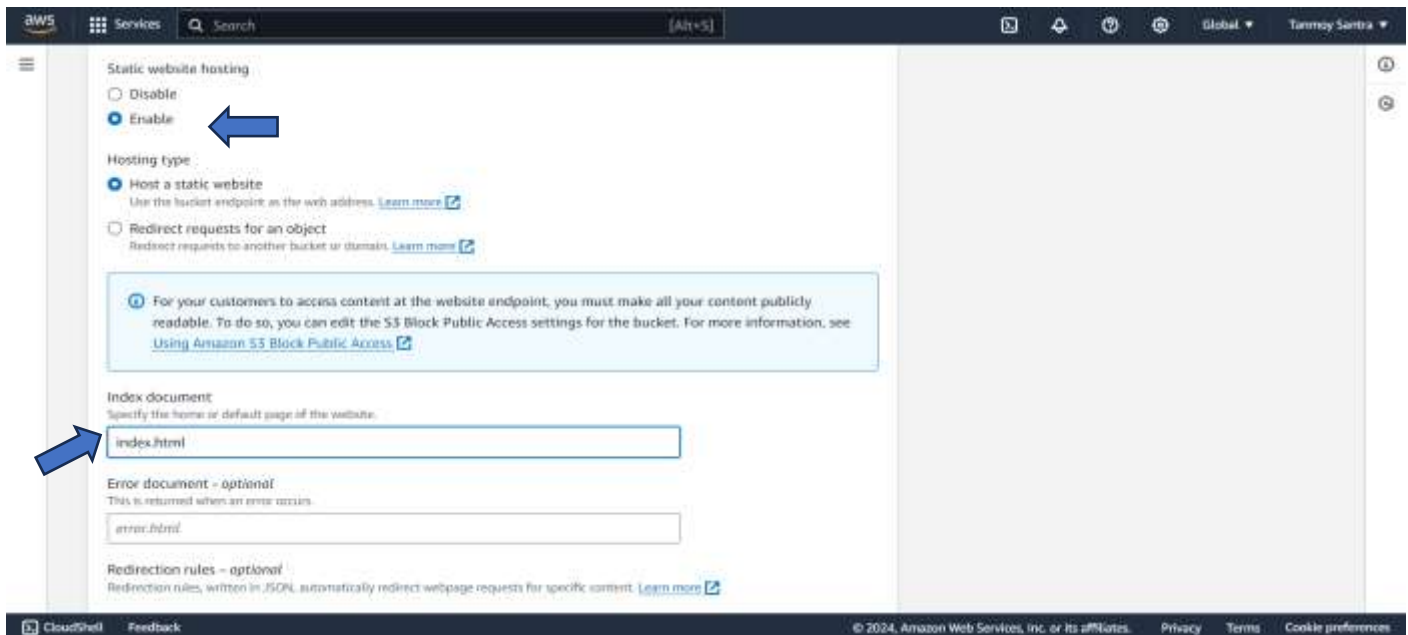
STEP 12- From the bucket go to the Properties.



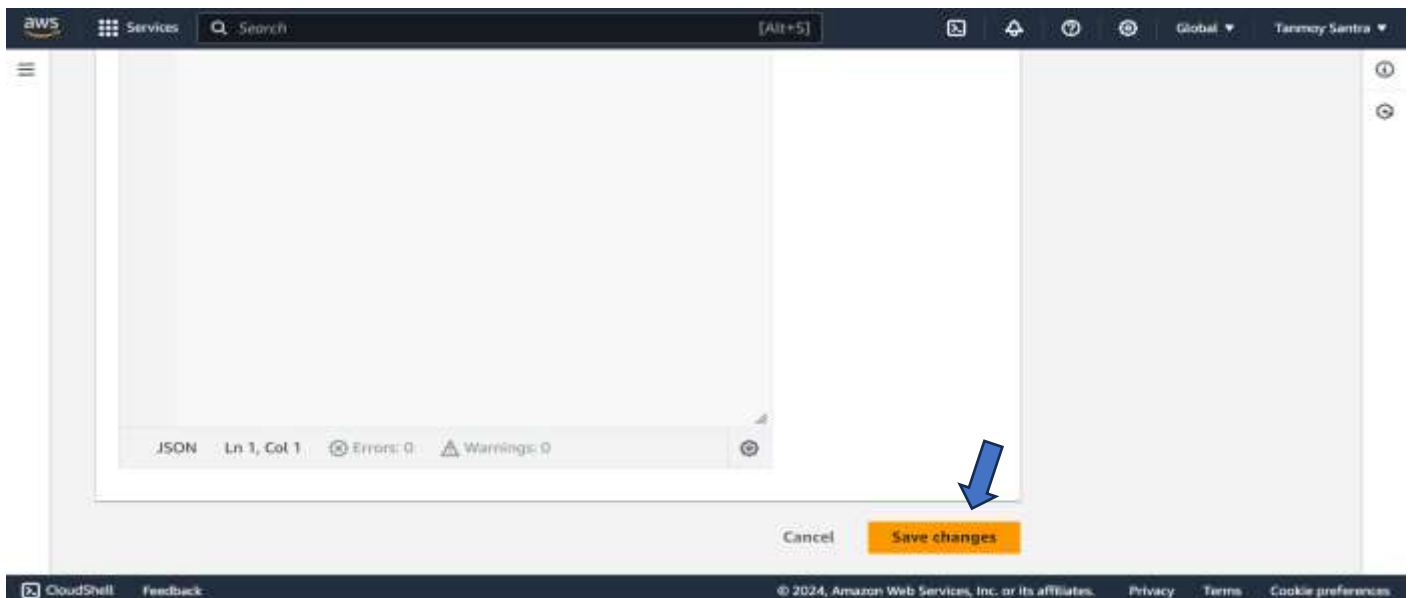
STEP 13- In Static Website Hosting, click on Edit .



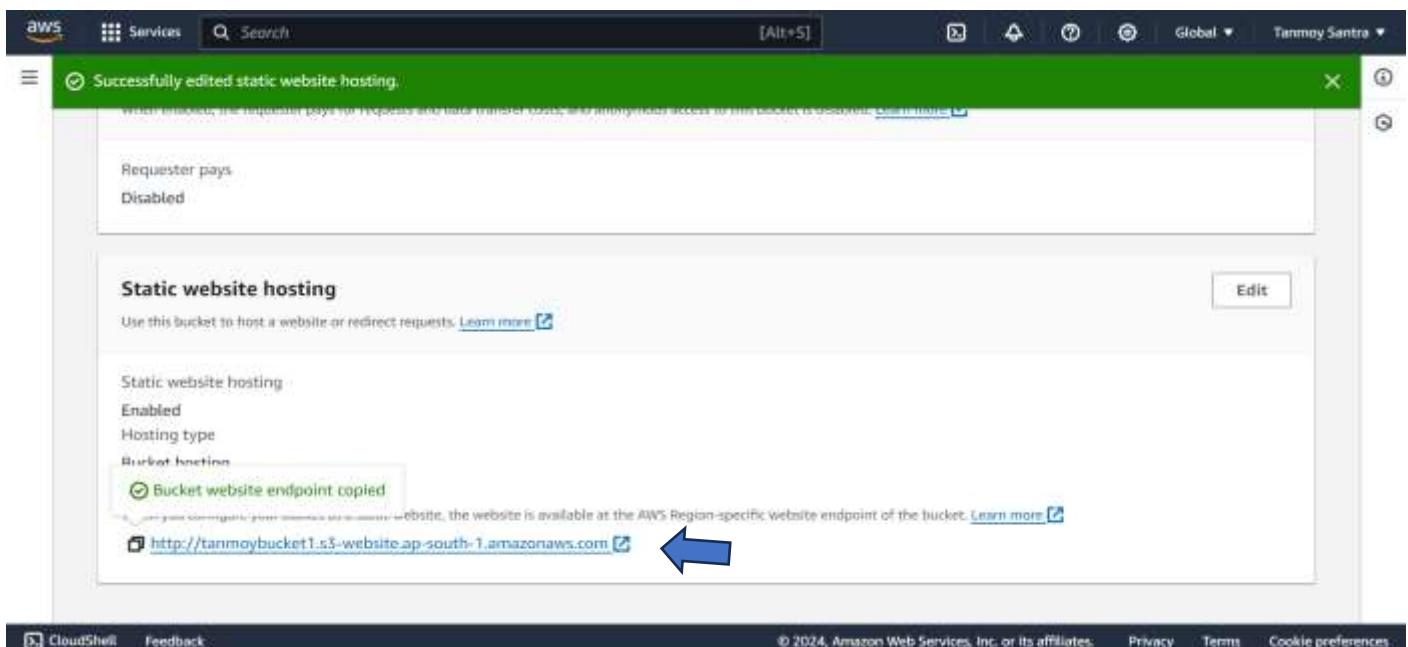
STEP 14- Select Enable. Give the name of the index file “index.html”.



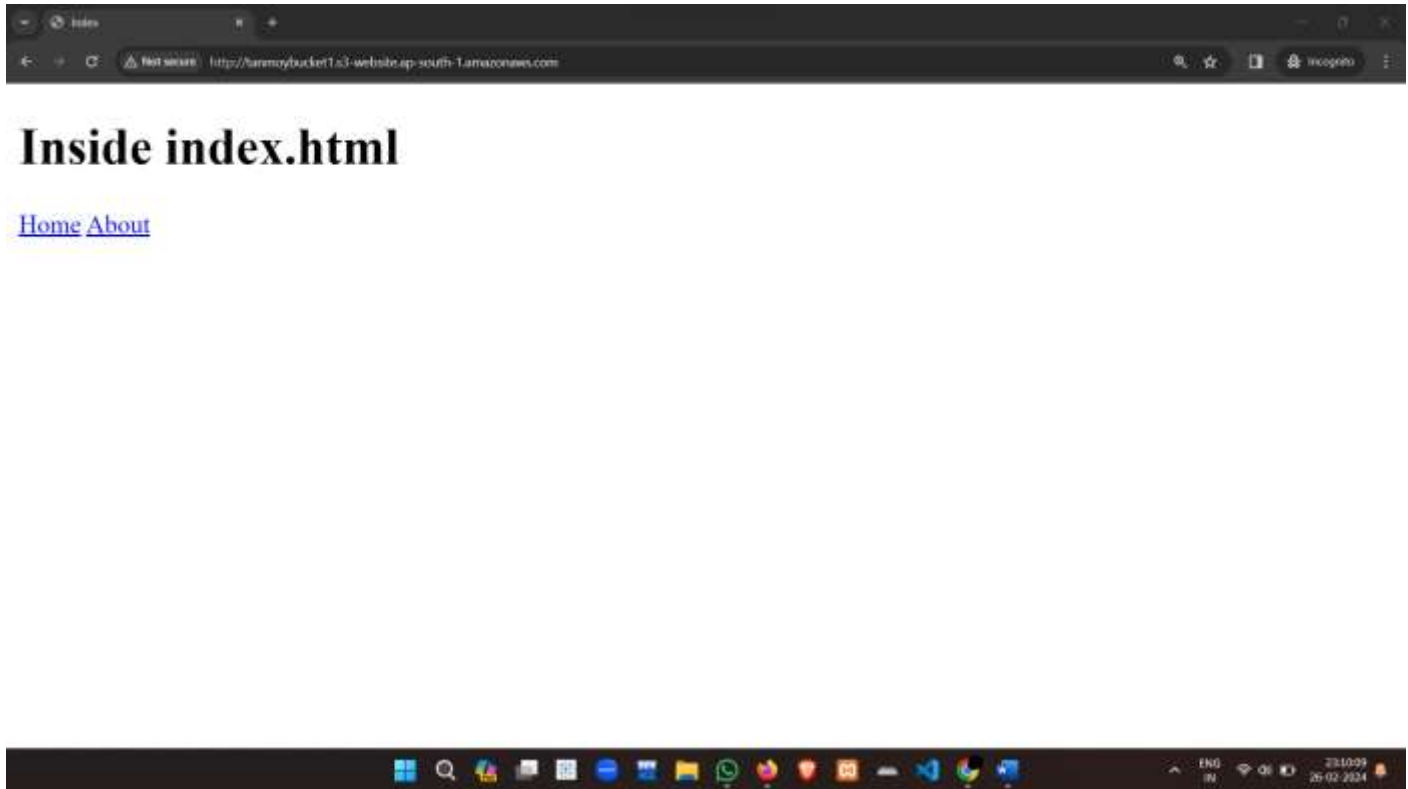
STEP 15- Click on “Save Changes”.



STEP 16- From Static Website Hosting copy the url.



STEP 17- Open a new window and paste the url.



By Click on 'Home' go to the Home.html page.

