

# HOSTING A STATIC WEBSITE USING AWS S3 (Simple Storage Service)

## What is S3?

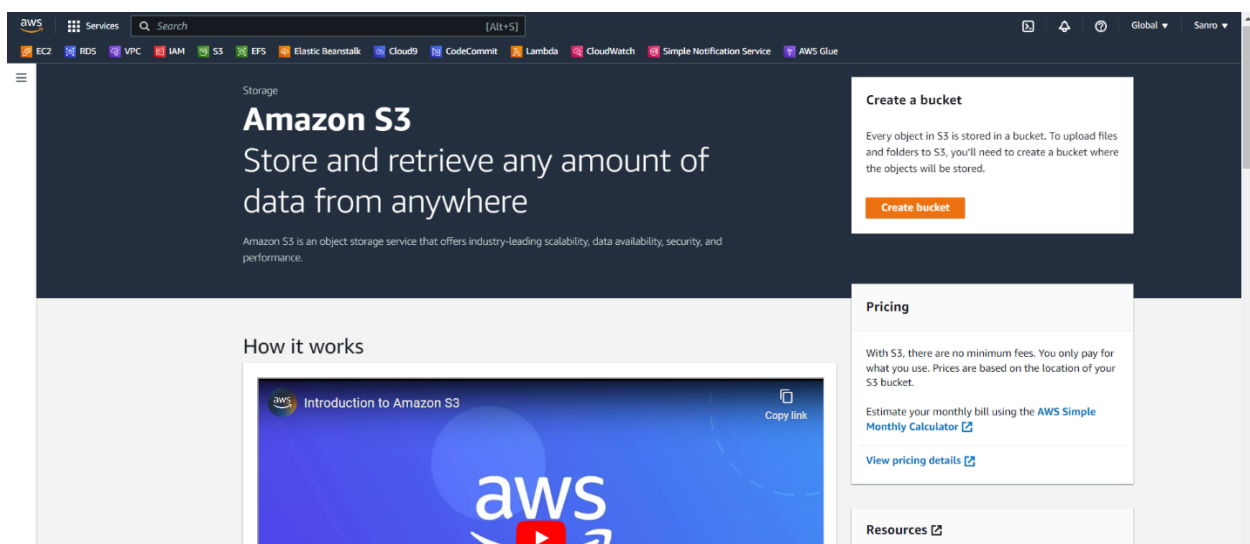
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere.

Amazon S3 is a pioneer in cloud data storage and has uncountable benefits, the 5 most prominent ones are

- Reliable Security
- All-time Availability
- Very Low Cost
- Ease of Migration
- The simplicity of Management

Step-by-Step method to store static websites in an S3 bucket.

**Step 1:** Search for s3 service in AWS management console and click on create bucket



## Step 2: Create bucket by providing the details as shown in below pictures

The screenshot displays the AWS Management Console interface for creating a new S3 bucket. The top navigation bar includes the AWS logo, a search bar, and links to various services like EC2, RDS, VPC, IAM, S3, EFS, Elastic Beanstalk, Cloud9, CodeCommit, Lambda, and CloudWatch. The breadcrumb trail indicates the path: Amazon S3 > Buckets > Create bucket.

### Create bucket [Info](#)

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

#### General configuration

**Bucket name**  
roja12345  
Bucket name must be unique within the global namespace and follow the bucket naming rules. [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](#)

#### 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.

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

- Make sure to allow public access by not clicking on the “block public Access settings” for this bucket
- Enable bucket versioning as it helps with tracking the changes in the bucket data and recovery of it when something happens to the data

aws

Services

Search

[Alt+S]

EC2RDSVPCIAMS3EFSElastic BeanstalkCloud9CodeCommitLambdaCloudWatchS

### 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.

aws

Services

Search [Alt+S]

EC2RDSVPCIAMS3EFSElastic BeanstalkCloud9CodeCommitLambdaCloudWatch

Bucket Versioning

☐ Disable

☒ Enable

Tags (0) - optional

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

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 type [Info](#)

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)

☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☒ Disable

☐ Enable

► Advanced settings

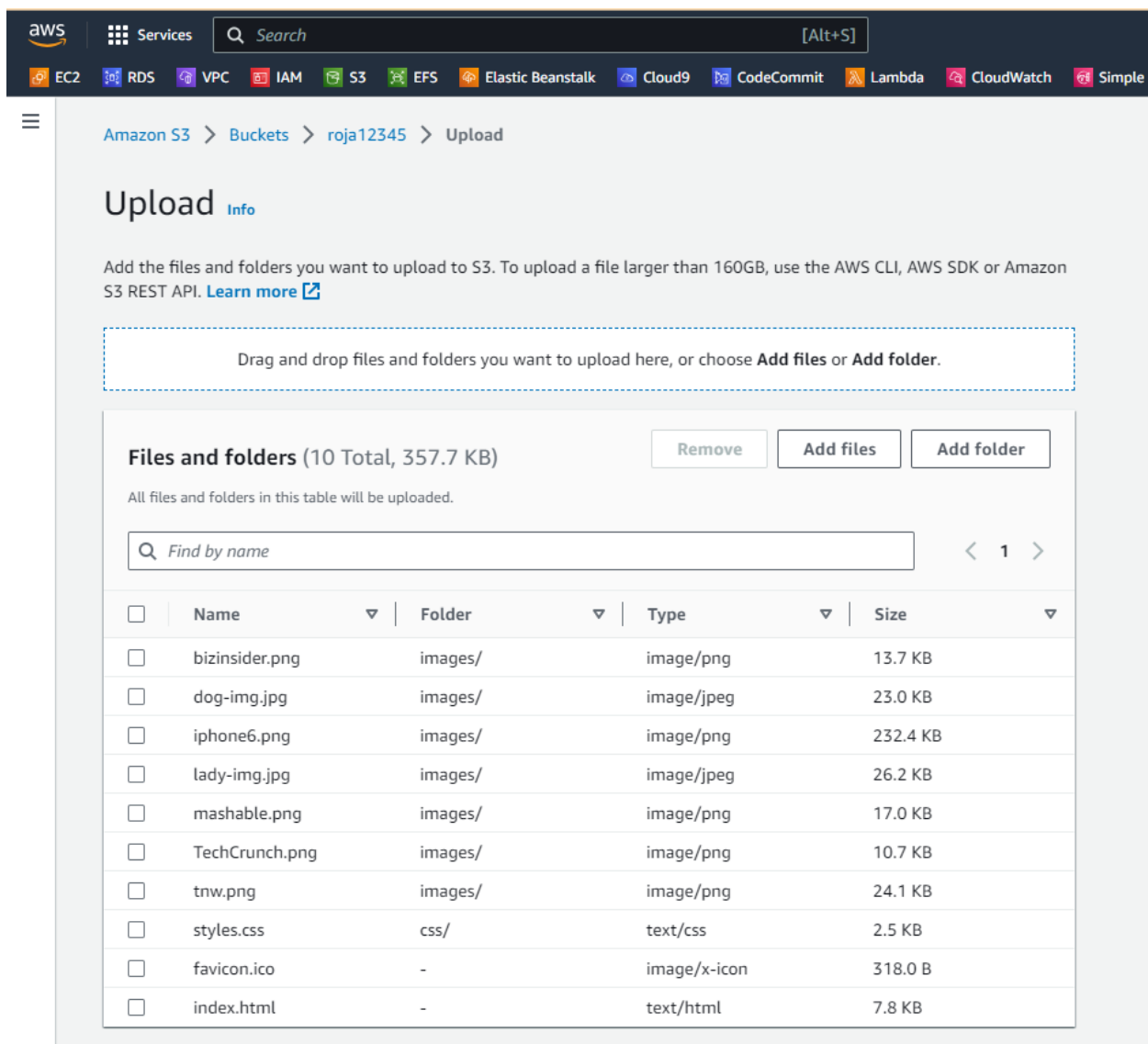
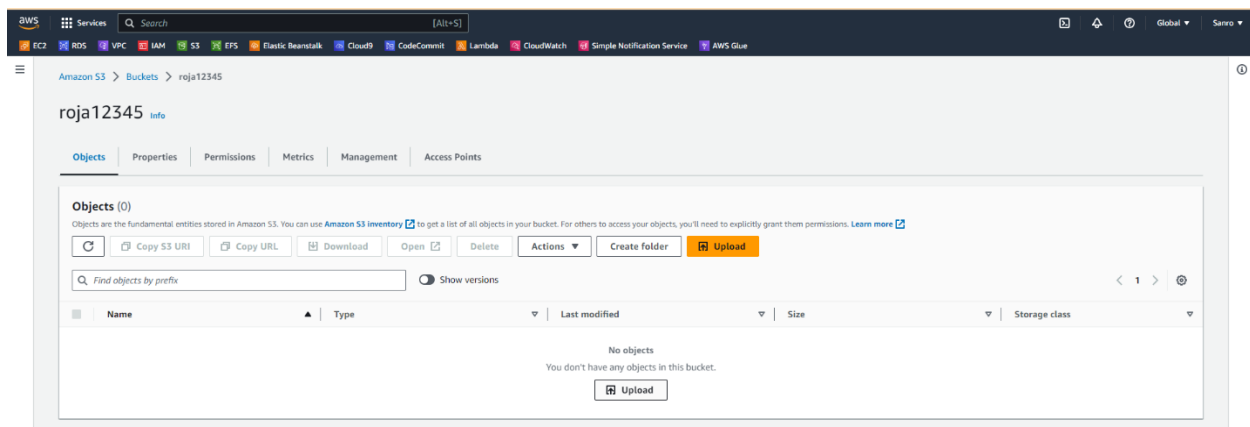
ⓘ

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

Cancel

Create bucket

Step 3: Now upload the files of the website that you want to host in AWS into that bucket



### Destination

Destination

s3://roja12345

► Destination details

Bucket settings that impact new objects stored in the specified destination.

► Permissions

Grant public access and access to other AWS accounts.

► Properties

Specify storage class, encryption settings, tags, and more.

Cancel

Upload

Upload succeeded

View details below.

### Upload: status

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

Summary

Destination	Succeeded	Failed
s3://roja12345	10 files, 357.7 KB (100.00%)	0 files, 0 B (0%)

Step 4: After successfully uploading the files into the bucket now select all the files in the bucket and make public access using ACL (Access Control List)

Amazon S3 > Buckets > roja12345

roja12345

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (4)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Show versions

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	css/	Folder	-	-	-
<input checked="" type="checkbox"/>	favicon.ico	ico	August 7, 2023, 17:33:51 (UTC+05:30)	318.0 B	Standard
<input checked="" type="checkbox"/>	images/	Folder	-	-	-
<input checked="" type="checkbox"/>	index.html	html	August 7, 2023, 17:33:52 (UTC+05:30)	7.8 KB	Standard

aws

Services

Search

[Alt+S]

EC2RDSVPCIAMS3EFSElastic BeanstalkCloud9CodeCommitLambdaCloudWatchSimple Notification ServiceAWS Glue

Amazon S3 > Buckets > roja12345

roja12345

Info

ObjectsPropertiesPermissionsMetricsManagementAccess Points

Objects (4)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permis

Copy S3 URICopy URLDownloadOpenDelete

ActionsCreate folderUpload

Find objects by prefix

Show versions

<input checked="" type="checkbox"/>	Name	Type
<input checked="" type="checkbox"/>	css/	Folder
<input checked="" type="checkbox"/>	favicon.ico	ico
<input checked="" type="checkbox"/>	images/	Folder
<input checked="" type="checkbox"/>	index.html	html

Download as

Share with a presigned URL

Calculate total size

Copy

Move

Initiate restore

Query with S3 Select

Edit actions

Rename object

Edit storage class

Edit server-side encryption

Edit metadata

Edit tags

Make public using ACL

CloudShellFeedbackLanguage

aws

Services

Search

[Alt+S]

EC2RDSVPCIAMS3EFSElastic BeanstalkCloud9CodeCommitLambdaCloudWatchSimple Notific

Amazon S3 > Buckets > roja12345 > Make public

Make public

Info

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#)

⚠

- When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.
- This action applies to all objects within the specified folders. Objects added to these folders while the action is in progress might be affected.

Specified objects

Find objects by name

< 1 >

Name	Type	Last modified	Size
css/	Folder	-	-
favicon.ico	ico	August 7, 2023, 17:33:51 (UTC+05:30)	318.0 B
images/	Folder	-	-
index.html	html	August 7, 2023, 17:33:52 (UTC+05:30)	7.8 KB

CancelMake public

## Step 5: Now go to properties and enable static website hosting

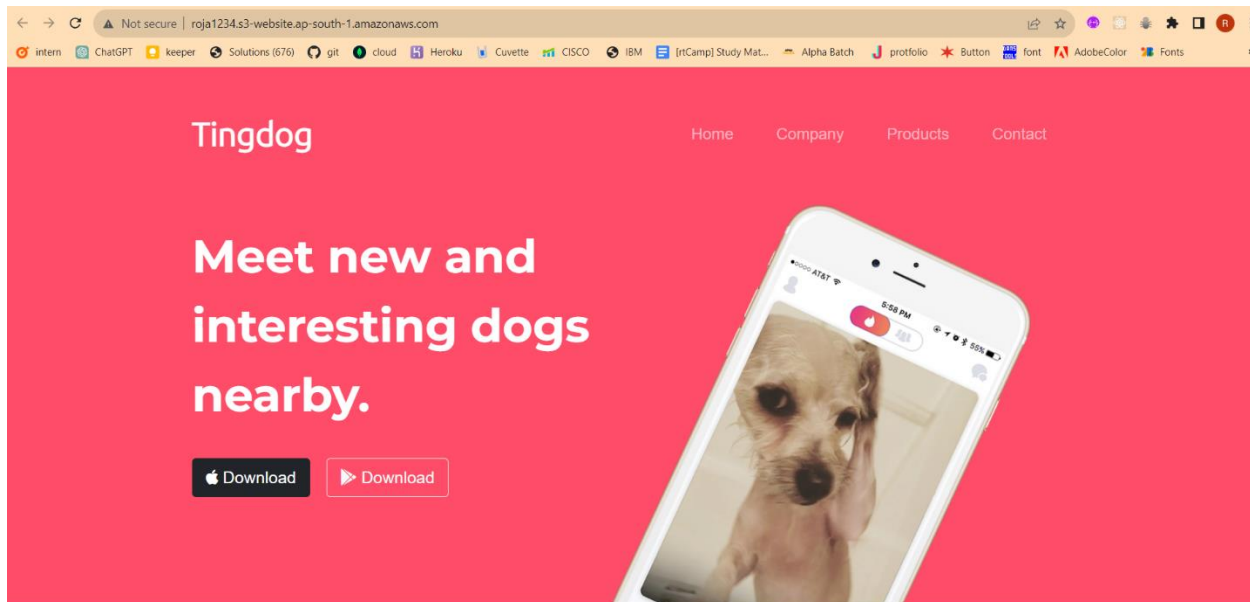
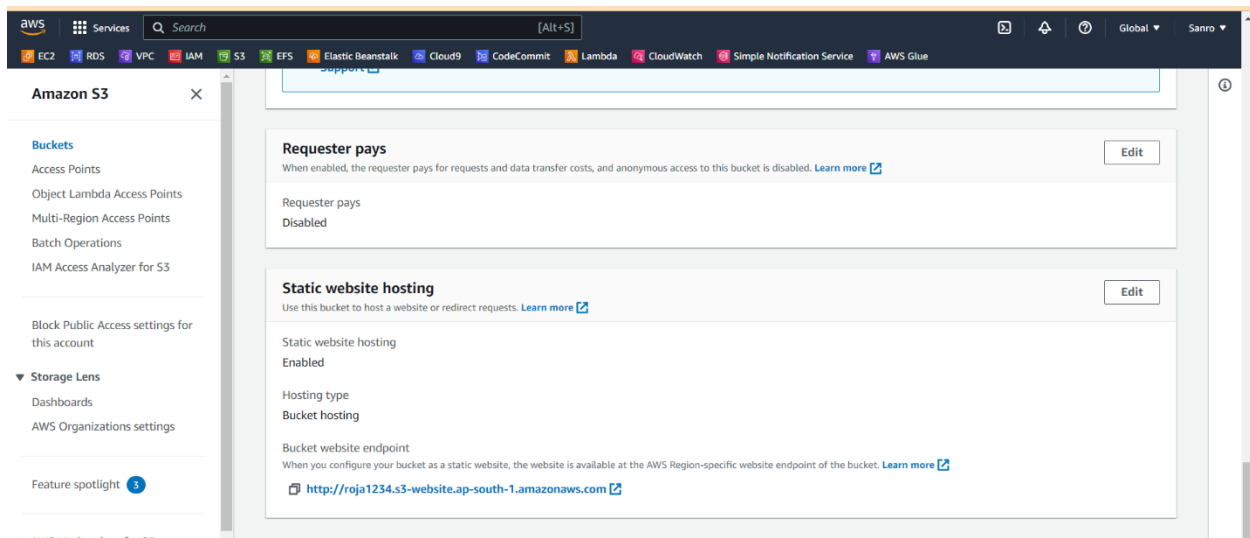
Both step 4 and 5 are permissions for providing the access of our website globally

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services' menu, a search bar, and a list of services including EC2, RDS, VPC, IAM, S3, EFS, Elastic Beanstalk, Cloud9, CodeCommit, Lambda, CloudWatch, and CloudFormation. Below the navigation bar, the breadcrumb trail reads 'Amazon S3 > Buckets > roja12345 > Edit static website hosting'. The main heading is 'Edit static website hosting' with an 'Info' link. The content area is titled 'Static website hosting' and includes a sub-header 'Use this bucket to host a website or redirect requests. Learn more'. There are two sections: 'Static website hosting' with radio buttons for 'Disable' and 'Enable' (selected), and 'Hosting type' with radio buttons for 'Host a static website' (selected) and 'Redirect requests for an object'. A blue information box states: 'For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access'. Below this, there's an 'Index document' section with a text input field containing 'index.html'. An 'Error document - optional' section has a text input field containing 'error.html'. Finally, a 'Redirection rules - optional' section has a text input field and a 'Learn more' link.

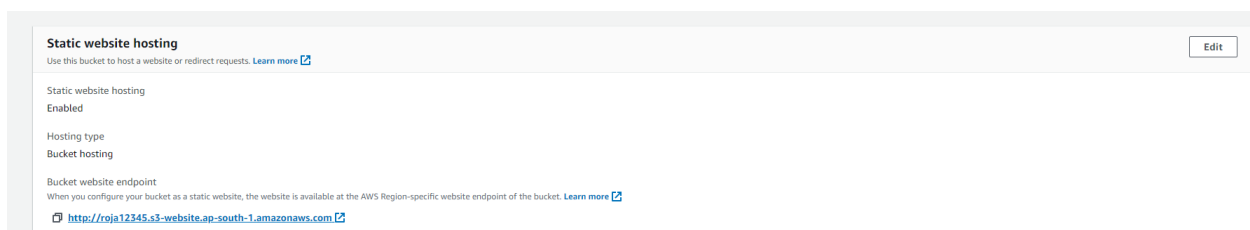
Step 6: Thus, our website is hosted on the AWS Cloud which can be accessed in many ways some of them are provided below

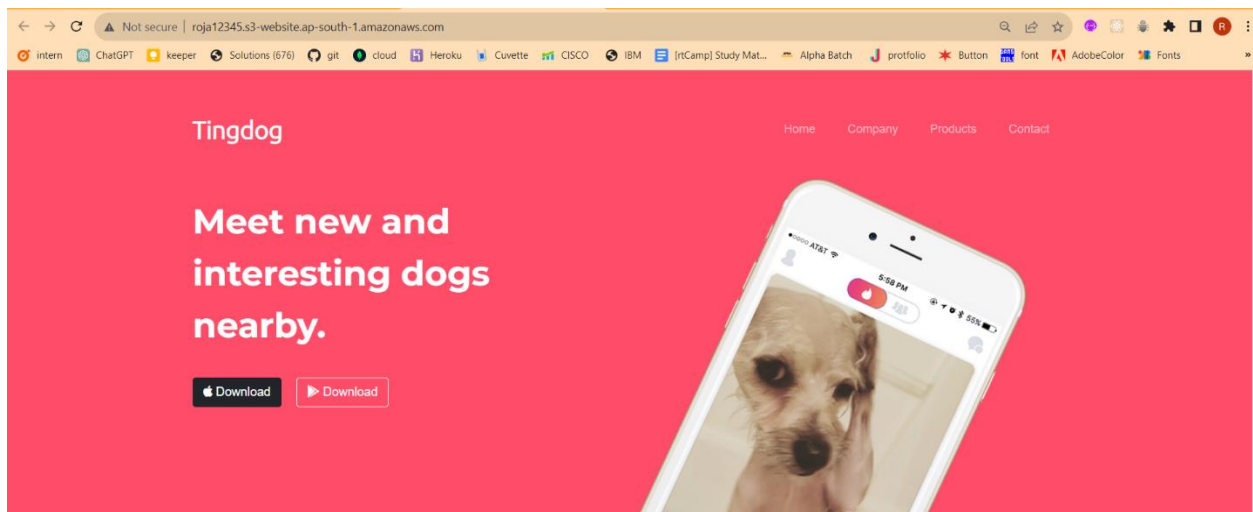
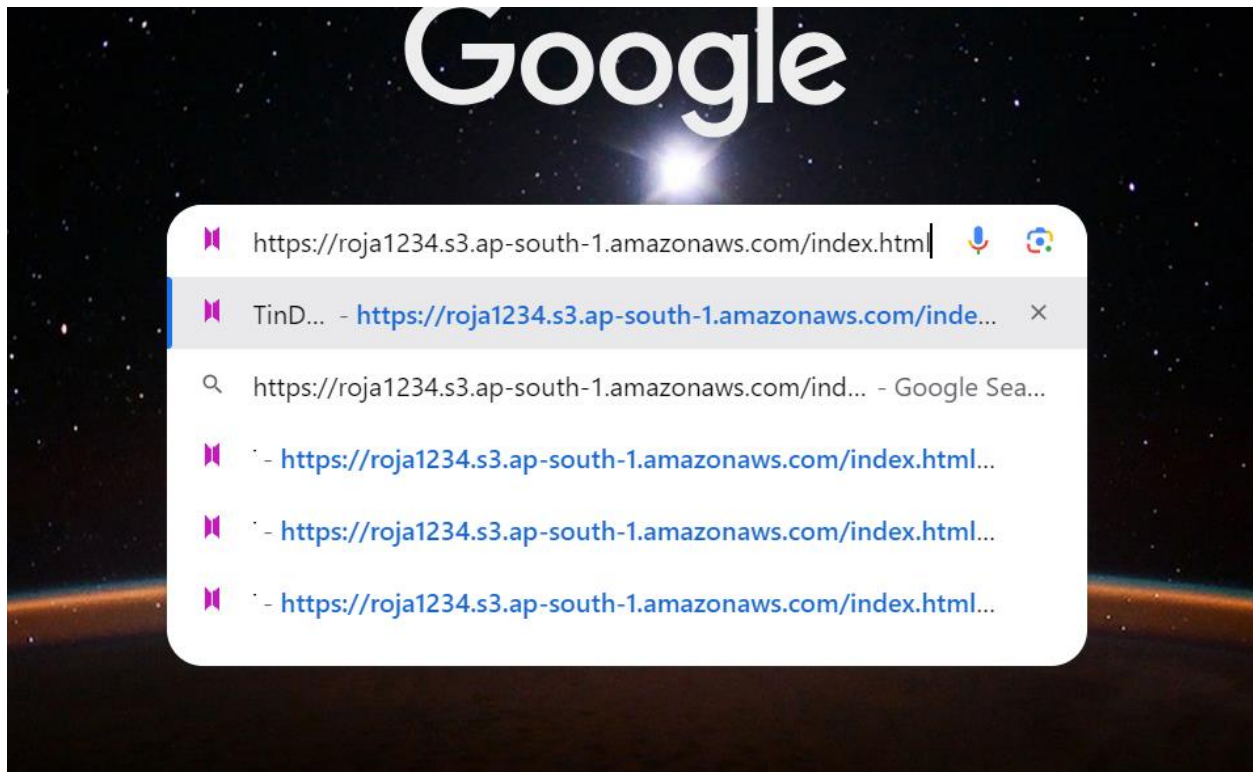
- We can simply click on the URL that is shown under 'static website hosting' in properties



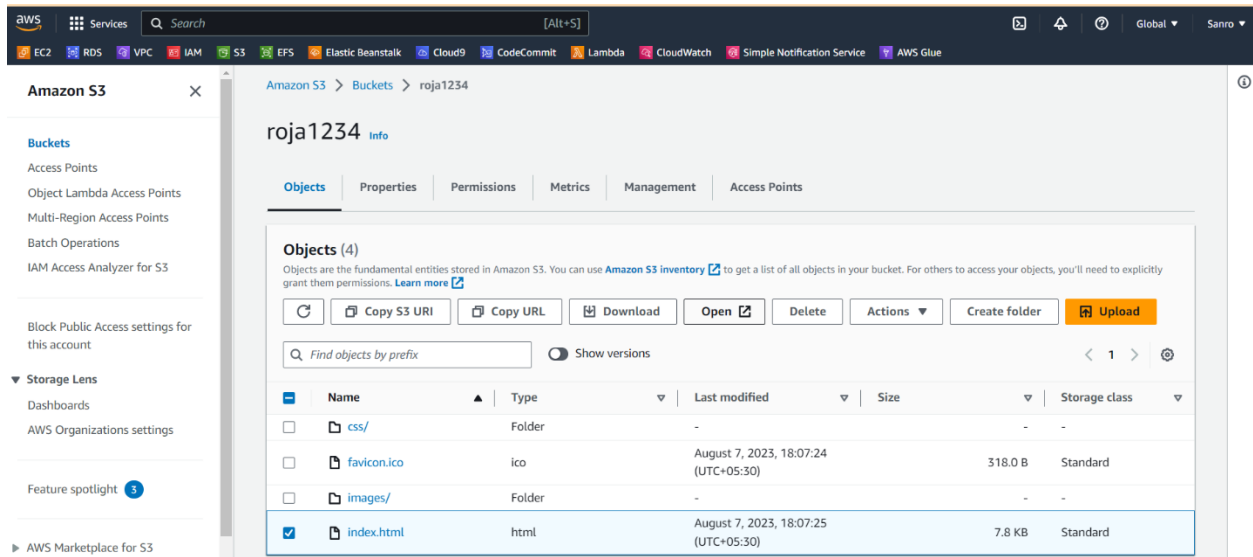


b. We can copy the website URL and paste it on the browser

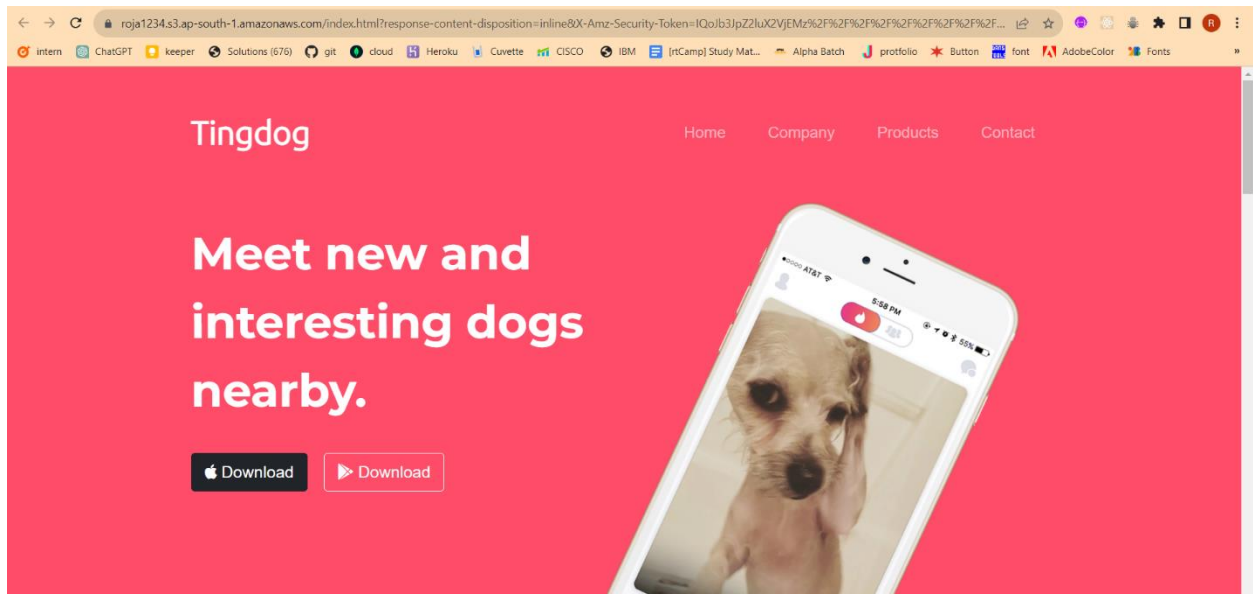




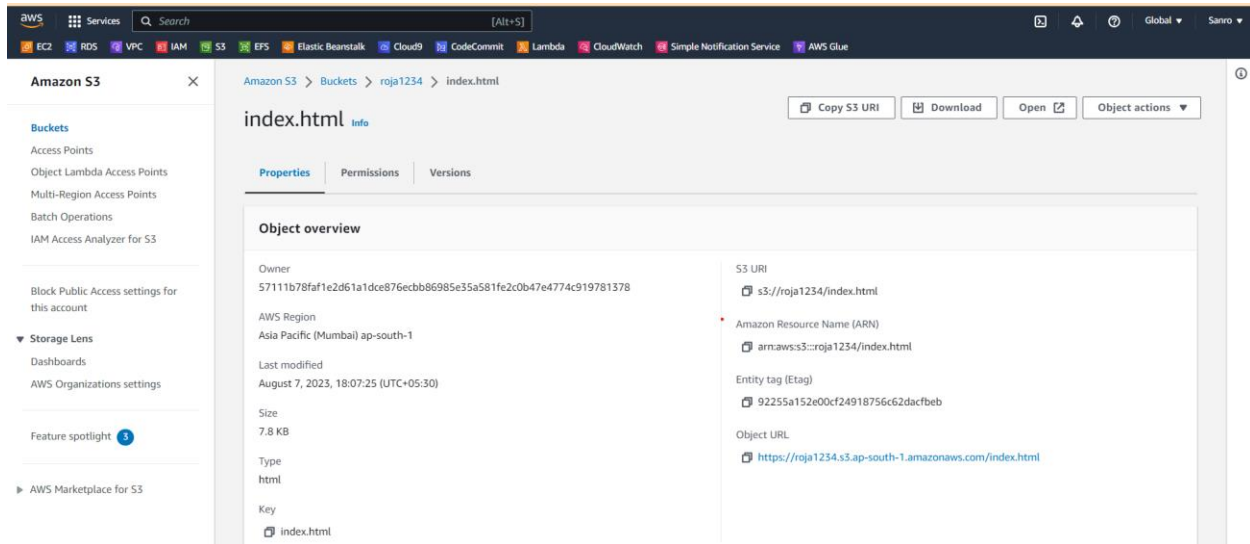
- c. Go to the bucket and to the main file of our website which is `index.html`, select it then we can click on 'open URL'



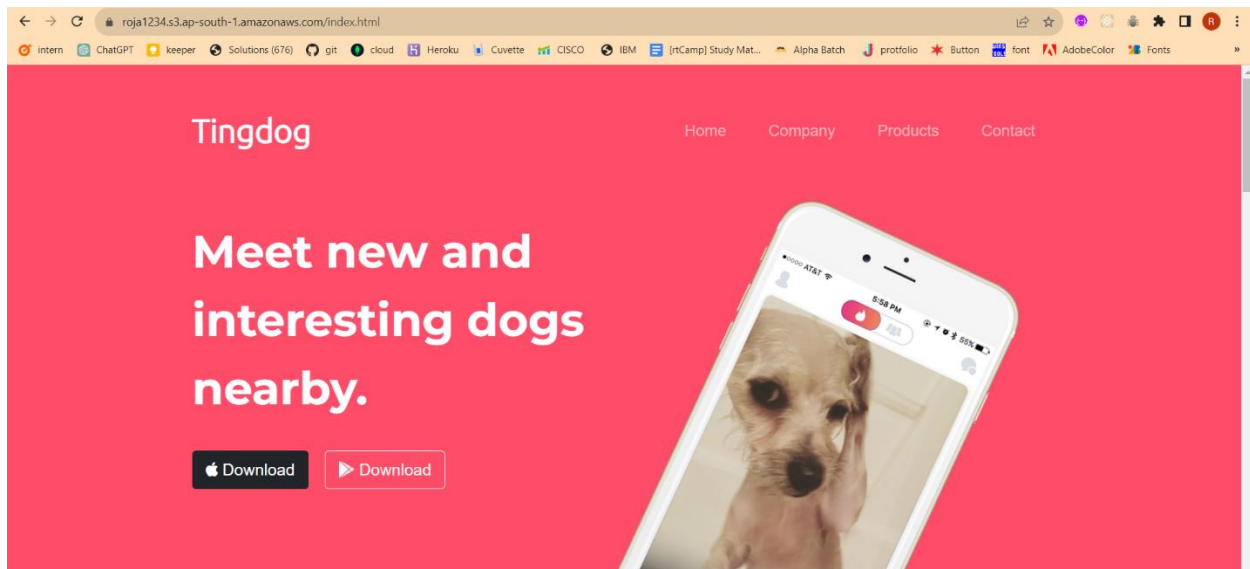
- Observe the URL on the browser to know the change on how we are accessing in different ways



- d. The last way is by clicking on the index.html file and then go to properties there we can find a URL , click on it which redirects to the website



- We can observe the URL Path which end point is shown as /index.html



These has been the steps for hosting a static website in AWS s3

## Step 7: Go to permissions and edit bucket policies (optional)

In addition to these we can add few more steps to the above process in order to provide much security and accessibility restrictions through bucket policies . They are

**Bucket Policy for Public Access Control:** To prevent accidental public access to your static website content, you can use a bucket policy that denies public access by default and then grants access to specific AWS services and resources.

**Website Hosting Permissions:** Allow public read access to your website's objects so that they can be accessed by visitors.

The first screenshot shows the 'Permissions' tab for the bucket 'roja1234'. It displays the 'Block public access (bucket settings)' section, which is currently set to 'Off'. Below this, there is a section for 'Block all public access' with a warning icon and the text 'Off'. A link to 'Individual Block Public Access settings for this bucket' is provided.

The second screenshot shows the 'Bucket policy' tab for the same bucket. It displays the bucket ARN 'arn:aws:s3::roja1234' and the policy JSON. The policy is a 'DenyPublicAccess' policy that denies all public access to the bucket. The JSON is as follows:

```
1 {
2   "Version": "2012-10-17",
3   "Id": "DenyPublicAccess",
4   "Statement": [
5     {
6       "Sid": "DenyAllPublicAccess",
7       "Effect": "Deny",
8       "Principal": "*",
9       "Action": "s3:GetObject",
10      "Resource": "arn:aws:s3::roja1234/*"
11    },
12    {
13      "Sid": "PublicReadGetObject",
14      "Effect": "Deny",
15      "Principal": "*",
16      "Action": "s3:GetObject",
17      "Resource": "arn:aws:s3::roja1234/*"
18    }
19  ]
20 }
```

On the right side of the console, there is an 'Edit statement' section with a 'Select a statement' dropdown and an 'Add new statement' button.

Done! here's my website <http://roja1234.s3-website.ap-south-1.amazonaws.com> hosted in AWS s3