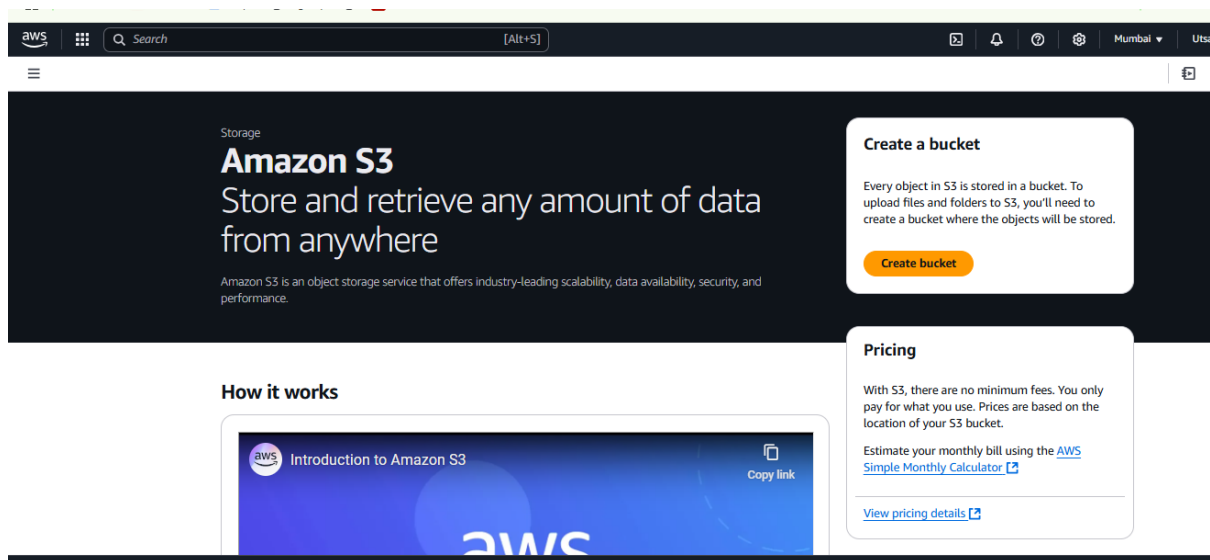


Name;- Utsav Sharma . Id:- CZT240357

A Static Website With S3 And CloudFront

Steps:-

1. Go to the [AWS Management Console](#) and sign in.
2. Make sure you are in the region where you want to create your S3 bucket.for this project.
- 3.Navigate to the **S3** service in the AWS Management Console.
- 4.Click on **Create bucket**.



5. Provide a **unique name** for your bucket and select the AWS Region where you want to create the bucket
6. Select Acls enabled (see above Image)
7. **Block all public access** settings. By default, all options under this setting are checked to prevent public access.
8. Click **Create bucket** to finalize the bucket creation process.
9. To allow public access, you'll need to add a bucket policy explicitly granting such permissions.

10. In the S3 dashboard, click on your newly created bucket's name.

Amazon S3 > Buckets

Successfully created bucket "utsavsharma"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Account snapshot - updated every 24 hours

All AWS Regions

[View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets

Directory buckets

General purpose buckets (1)

Info

All AWS Regions

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 >

Name	AWS Region	IAM Access Analyzer	Creation date
utsavsharma	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	January 2, 2025, 18:12:11 (UTC+05:30)

ap-south-1.console.aws.amazon.com/s3/upload/utsavsharma?region=ap-south-1&bucketType=general

Amazon S3 > Buckets > utsavsharma > Upload

Upload

Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

Files and folders (4 total, 16.0 KB)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	index.html	-	text/html	723.0 B
<input type="checkbox"/>	script.js	js/	text/javascript	6.3 KB
<input type="checkbox"/>	normalize.css	css/	text/css	7.5 KB
<input type="checkbox"/>	styles.css	css/	text/css	1.5 KB

Destination

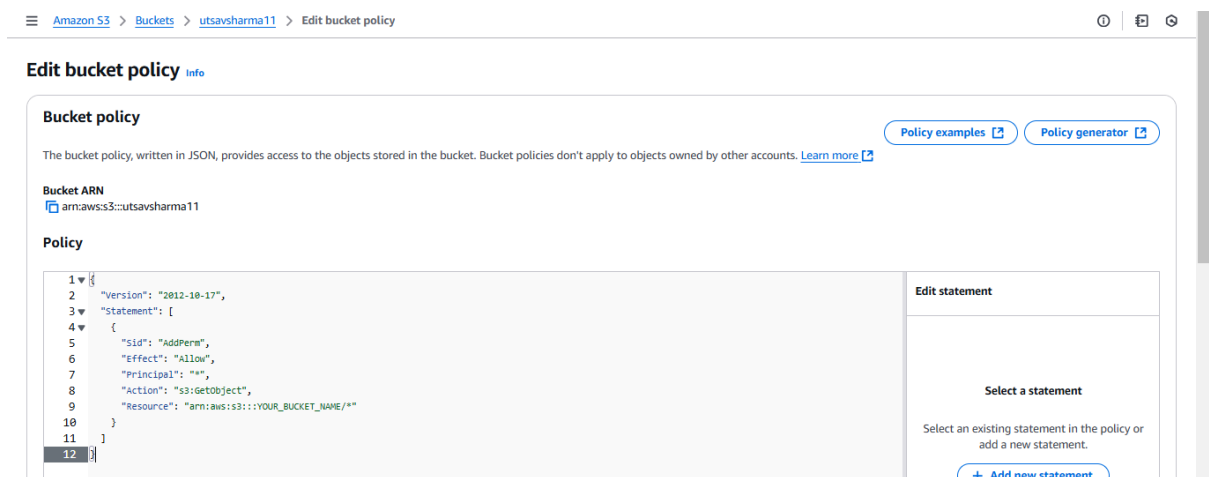
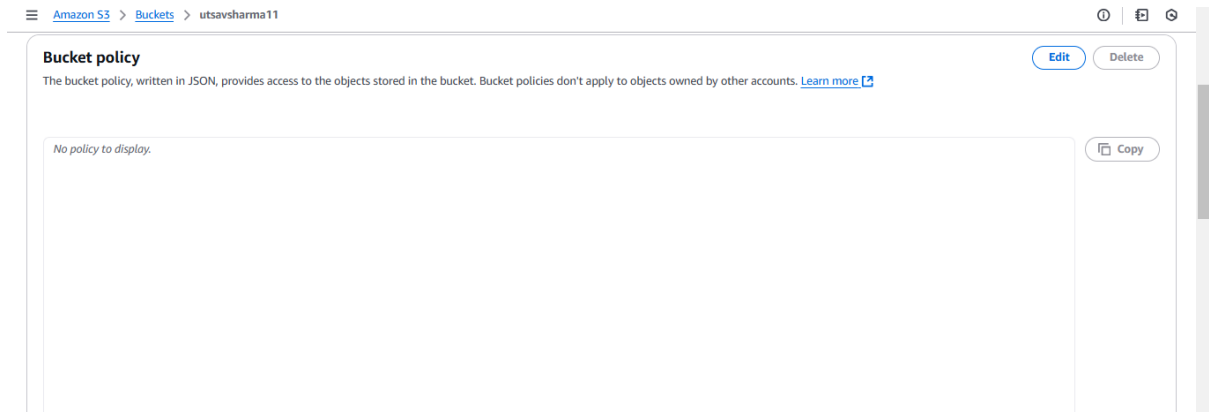
Info

Destination


```

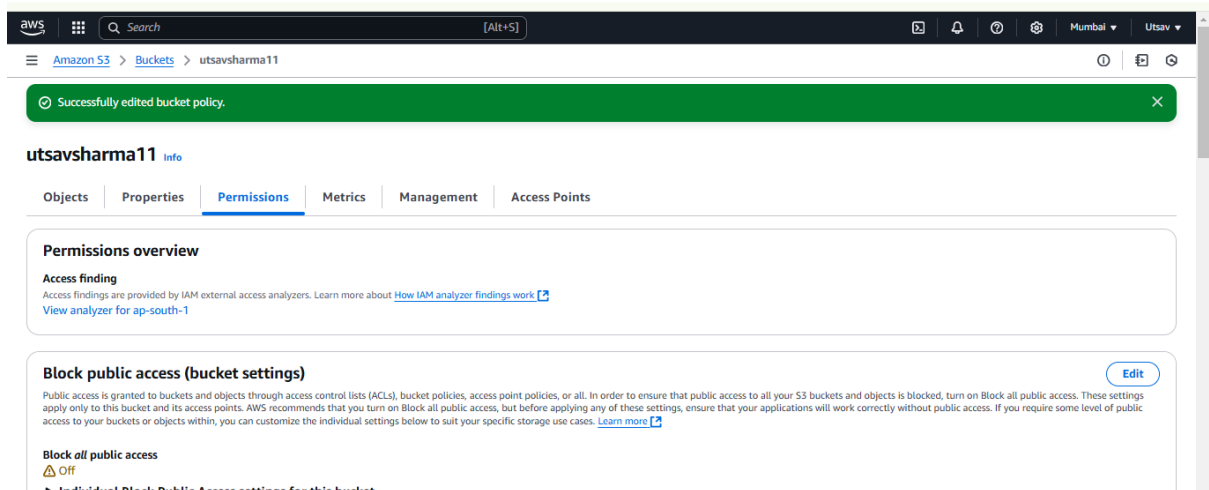
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::YOUR_BUCKET_NAME/*"
  }
]
}

```



14. To save your bucket policy, at the bottom of the page, click Save changes.

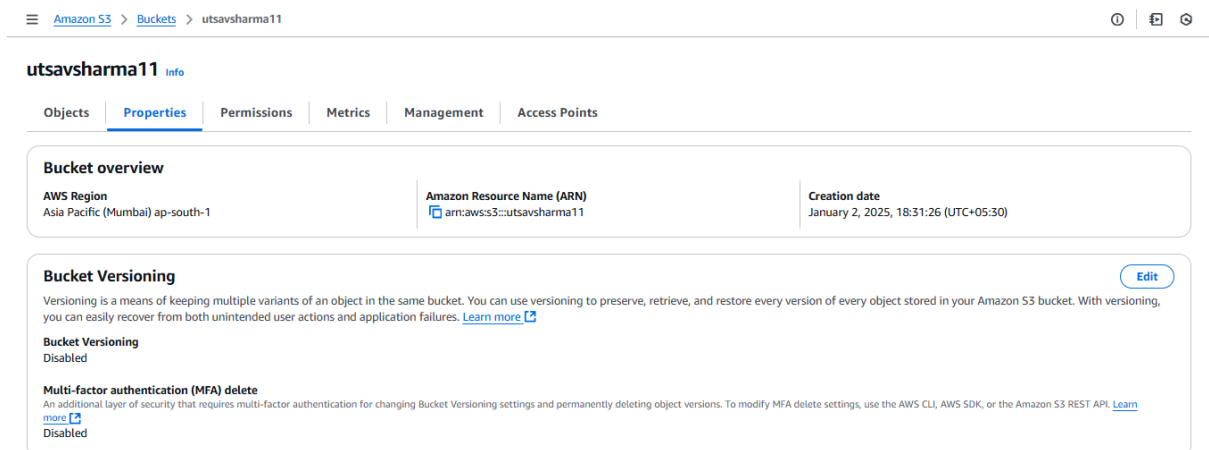
The bucket overview page will load and you will see a notification that the policy has been edited.



15. Let's Enable static website hosting, Click on the Properties tab

17. Select Enable to enable static website hosting &

1. Choose **Host a static website**. Here, you'll be prompted to enter:
 1. **Index document**: The name of your homepage document (e.g., index.html). This is the file served when visitors access the root URL of your website.
 2. **Error document** (optional): The name of the HTML file to show when an error occurs (e.g., error.html). This is not mandatory but recommended for handling HTTP errors gracefully.
2. (Optional) If you have a custom error document, fill in the **Error document** field.
3. Click **Save changes**.



Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays

Disabled

Edit

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

We recommend using AWS Amplify Hosting for static website hosting

Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

Create Amplify app

S3 static website hosting

Disabled

Amazon S3

Buckets

utsavsharma11

Edit static website hosting

Edit static website hosting

Info

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

Disable

Enable

Hosting type

Host a static website

Use the bucket endpoint as the web address. [Learn more](#)

Redirect requests for an object

Redirect requests to another bucket or domain. [Learn more](#)

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](#)

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Successfully edited static website hosting.

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays

Disabled

Edit

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

We recommend using AWS Amplify Hosting for static website hosting

Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

Create Amplify app

S3 static website hosting

Enabled

Hosting type

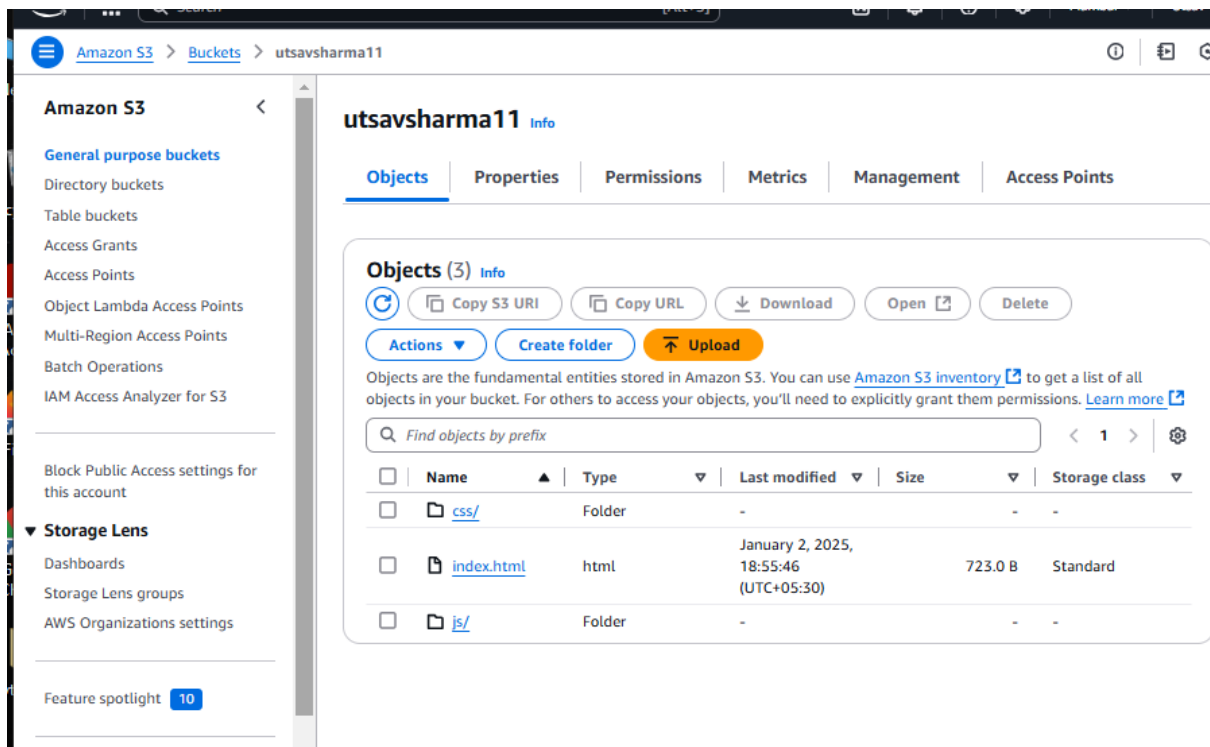
Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://utsavsharma11.s3-website.ap-south-1.amazonaws.com>

17. Upload the Website Files.



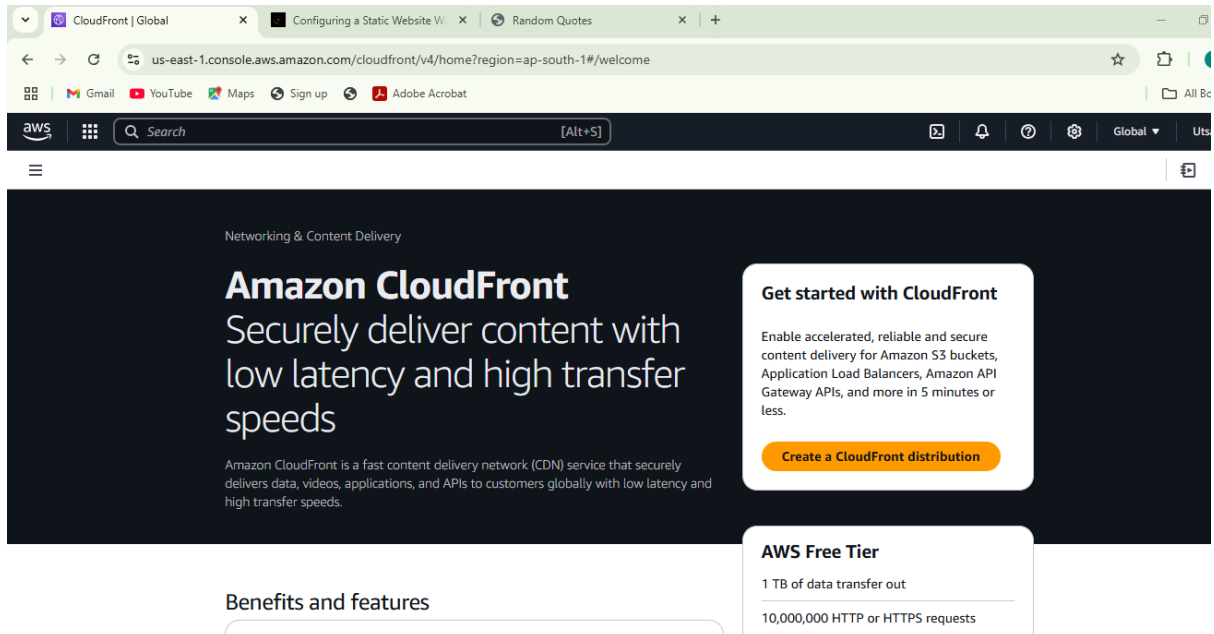
18 **Bucket website endpoint** URL. This URL is the public address of your static website.

19. Paste the endpoint into the address bar of a new browser tab.



CloudFront:-

1. In the AWS Management Console search bar, enter *CloudFront*, and click the CloudFront result under Services:



2. To start creating a distribution, click Create a CloudFront Distribution:

3. Under Origin, in the Origin Domain text-box, enter the Amazon S3 static website hosting endpoint that you created earlier:

A screenshot of the AWS CloudFront "Create distribution" form. The browser address bar shows the URL: us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=ap-south-1#/distributions/create. The form is titled "Create distribution" and has a breadcrumb trail: CloudFront > Distributions > Create. The "Origin" section is active, showing "Origin domain" with a text box containing "utsavsharma11.s3.ap-south-1.amazonaws.com". Below this, there is a warning message: "This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint." with a "Use website endpoint" button. The "Origin path - optional" section has a text box for "Enter the origin path". The "Name" section has a text box containing "utsavsharma11.s3.ap-south-1.amazonaws.com". The "Origin access" section has three radio buttons: "Public" (unselected), "Origin access control settings (recommended)" (selected), and "Legacy access identities" (unselected). The "Origin access control settings" option is highlighted with a blue border.

4. Under Origin, in the Origin access, select Origin access control settings and click Create new OAC:

5. Under Create control setting, enter the following values:

Name: by Default it will have

Signing behavior: Ensure Sign requests is selected

Origin path - optional
Enter a URL path to append to the origin domain name for origin requests.

Name
Enter a name for this origin.

Origin access | Info
☐ Public
Bucket must allow public access.
☒ **Origin access control settings (recommended)**
Bucket can restrict access to only CloudFront.
☐ Legacy access identities
Use a CloudFront origin access identity (OAI) to access the S3 bucket.

Origin access control
Select an existing origin access control (recommended) or create a new control.
 [Create new OAC](#)

Add custom header - optional
CloudFront includes this header in all requests that it sends to your origin.
[Add header](#)

Enable Origin Shield
Origin shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.
☒ No
☐ Yes

Create new OAC

Name
The name must be unique. Valid characters: letters, numbers and most special characters. Use up to 64 characters.

Description - optional
The description can have up to 256 characters.

Signing behavior
☐ Do not sign requests
☒ **Sign requests (recommended)**
☒ Do not override authorization header
Do not sign if incoming request has authorization header.

Origin type

The origin type must be the same type as origin domain.

[Cancel](#) [Create](#)

6. Select *Do not enable security protections* under Web Application Firewall (WAF):

Viewer request	No association
Viewer response	No association
Origin request	No association
Origin response	No association

Web Application Firewall (WAF) [Info](#)

☐ Enable security protections
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

☒ Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.

Settings

Anycast static IP list - optional [Info](#)
Deliver traffic from a small set of IP addresses
There are no Anycast static IP lists available
[Create an Anycast static IP list](#)
There are no Anycast static IP lists available

Price class [Info](#)
Choose the price class associated with the maximum price that you want to pay.
☐ Use all edge locations (best performance)
☒ Use only North America and Europe

[Request certificate](#)

Supported HTTP versions

Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.

- ☒ HTTP/2
☐ HTTP/3

Default root object - optional

The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

index.html

IPv6

- ☐ Off
☒ On

Description - optional

Standard logging [Info](#)

Additional charges may apply. See [Info](#) for more details.

Log delivery

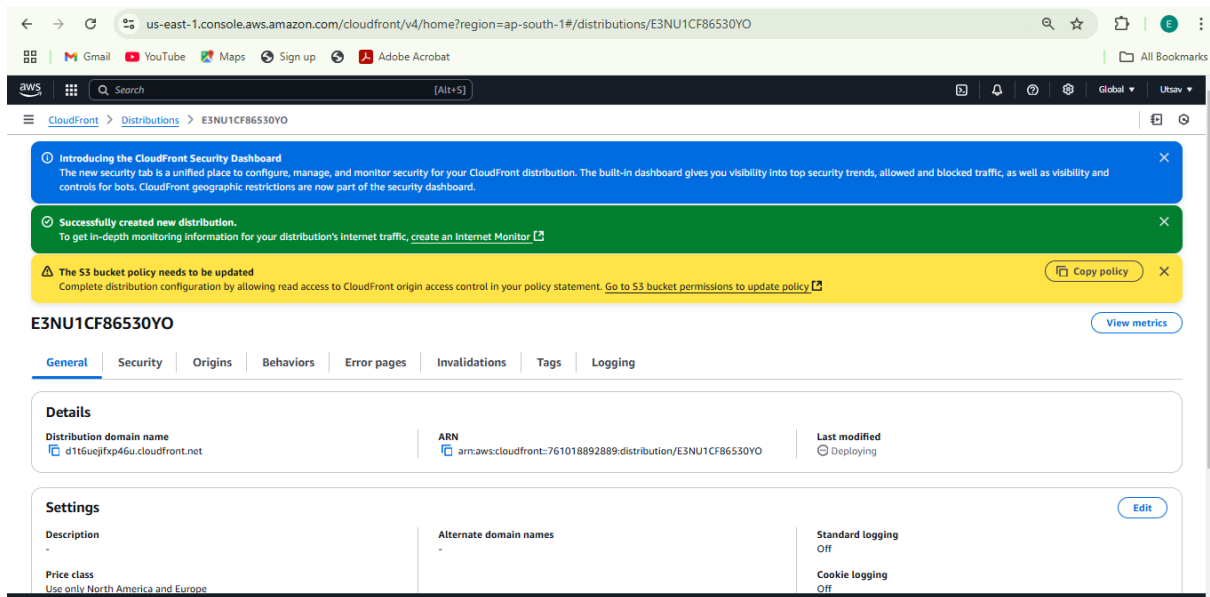
Get logs of viewer requests to CloudWatch, Amazon S3 or Firehose

- ☒ Off
☐ On

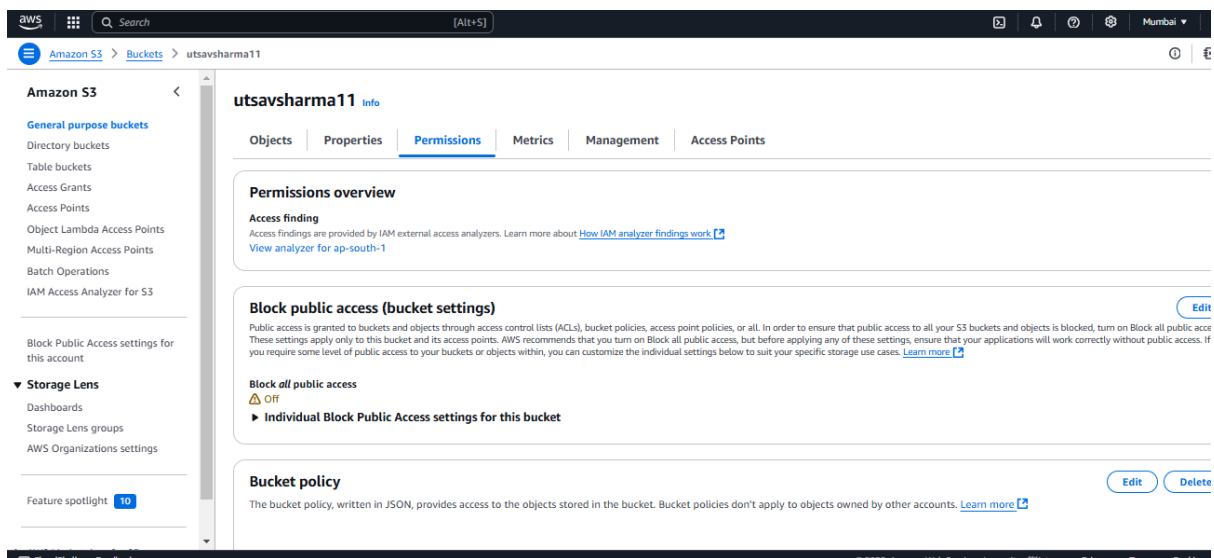
7 In the Default root object field, enter *index.html*.

8 To finish configuring your distribution, at the bottom of the page, click Create distribution:

9. Click Copy policy at the top of the page:



10 To implement the policy, return to the bucket you created, click the Permissions tab, scroll down to the Bucket policy section, click Edit, paste the policy you copied, and click Save changes:



11 Go to Bucket policy & click on Edit

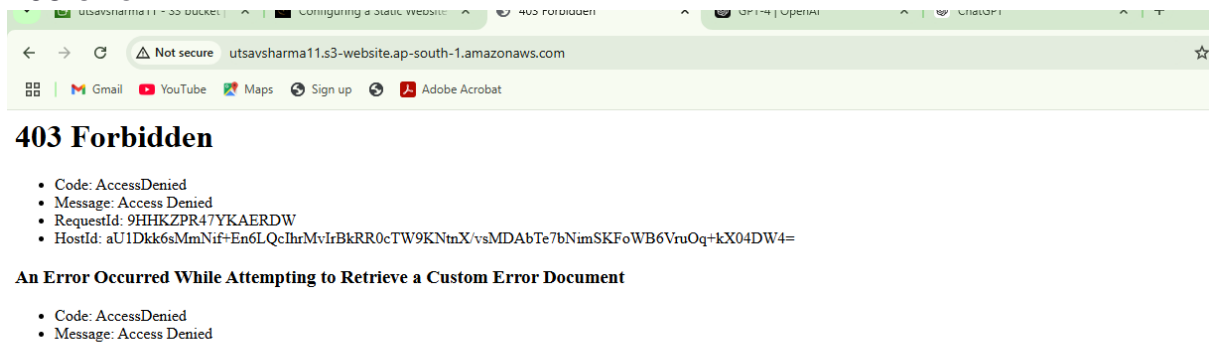
The screenshot shows the AWS Management Console interface. The left sidebar contains the navigation menu with categories like 'General purpose buckets', 'Storage Lens', and 'IAM Access Analyzer for S3'. The main content area is titled 'Edit bucket policy' and includes a 'Bucket policy' section. It displays the 'Bucket ARN' as 'arn:aws:s3::utsavsharma11' and a JSON policy. The policy allows the 'cloudfront.amazonaws.com' service to perform the 's3:GetObject' action on the bucket. On the right, there is an 'Edit statement' panel with a 'Select a statement' section and an 'Add new statement' button.

12. Update the Copied Policy from Cloudfront & click on Save Changes

13. Under the Block public access (bucket settings) section click Edit,

The screenshot shows the 'Edit Block public access (bucket settings)' page in the AWS Management Console. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Edit Block public access (bucket settings)'. It contains a section for 'Block public access (bucket settings)' with a description and a list of settings. The 'Block all public access' setting is checked. Below it, there are four unchecked settings: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. At the bottom right, there are 'Cancel' and 'Save changes' buttons.

14 .The previous Bucket website endpoint will no longer work and will return a 403 error.

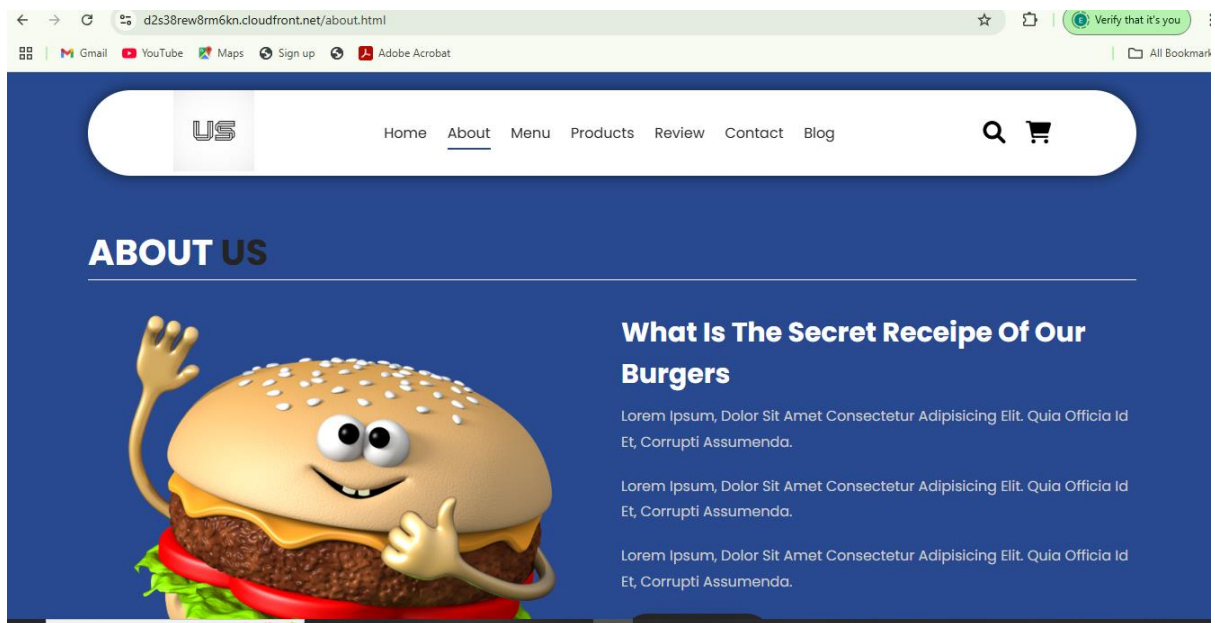
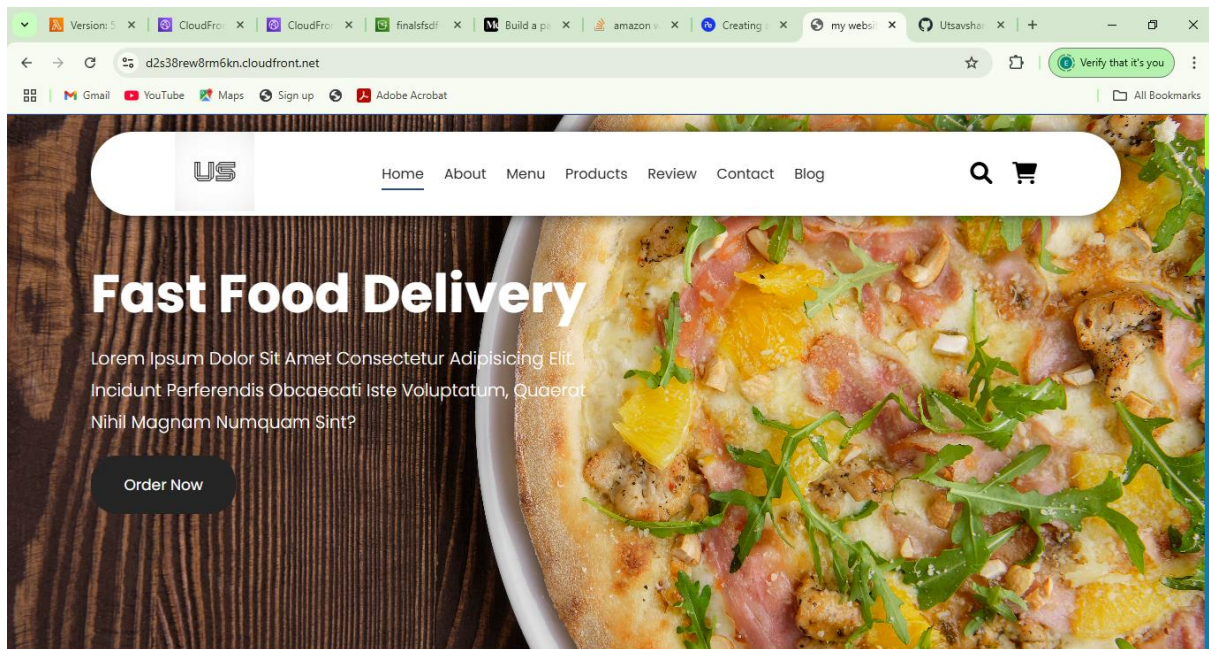


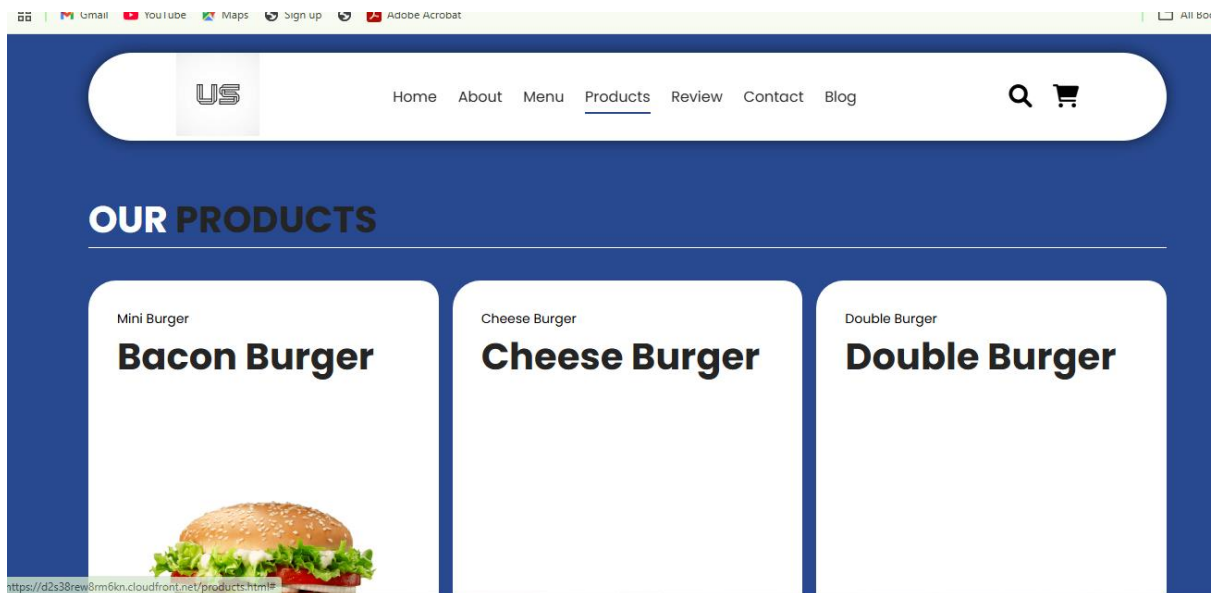
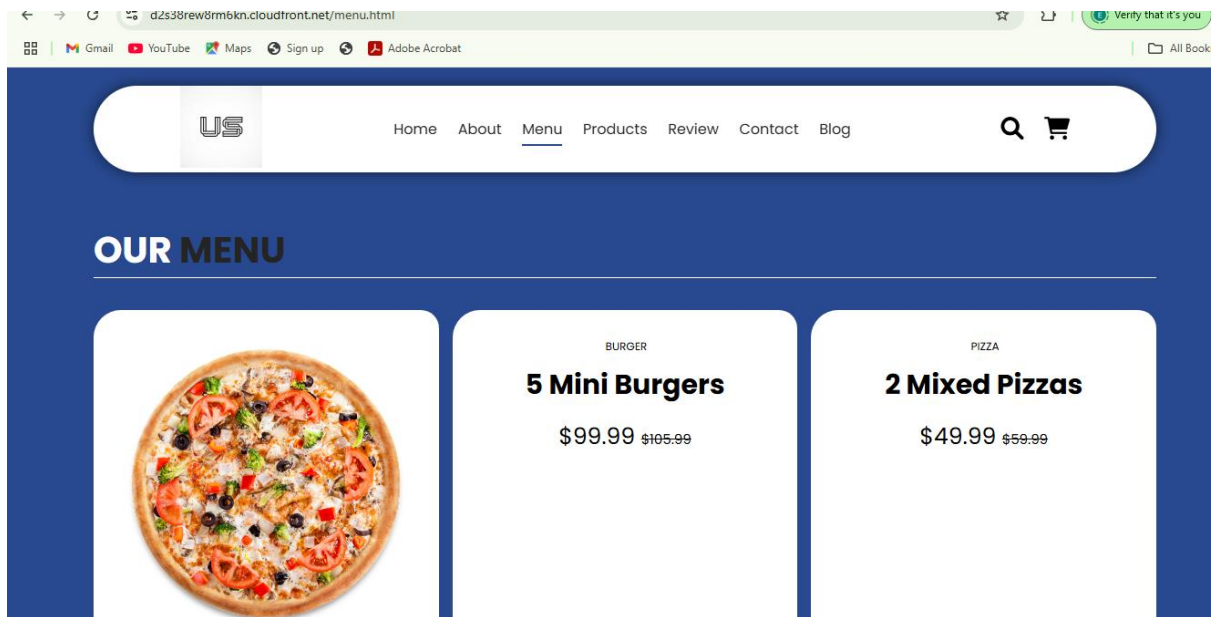
15. Return to the [CloudFront Distributions](#) table:

16. Enter into Cloudfront Distributions to copy the Domain name

17. Paste the domain name into the address bar of a new browser tab. You will see the website that you uploaded to your Amazon S3 bucket display:

Output:-





Website link:- <https://d12odjbato9p57.cloudfront.net>