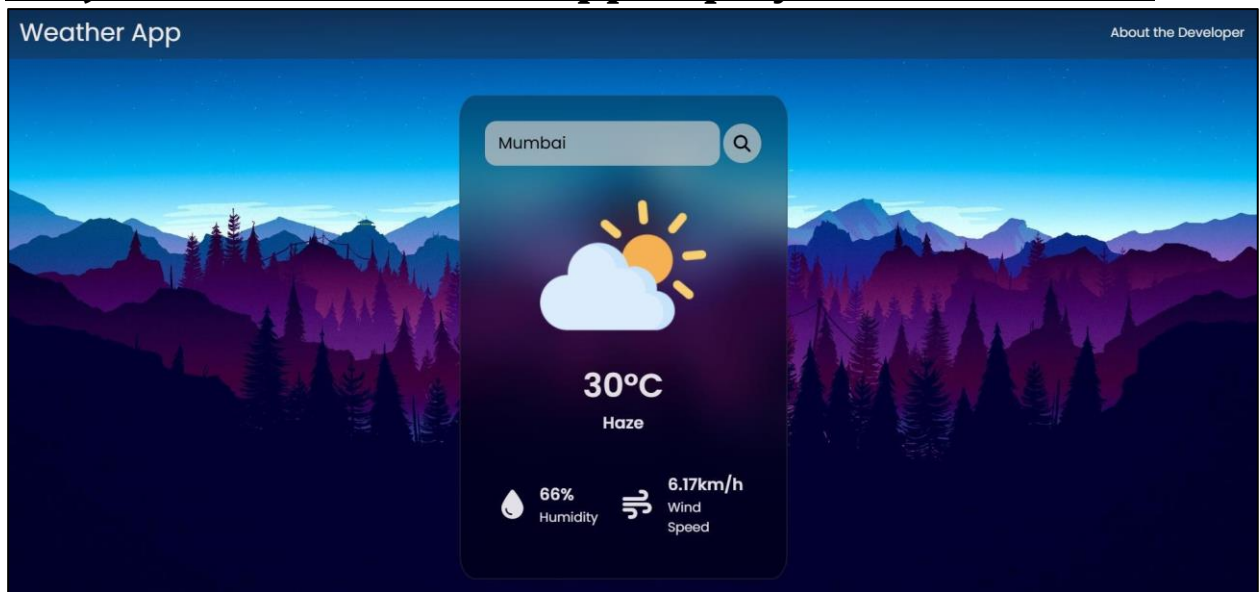


Project: Secure Weather App Deployment on AWS S3



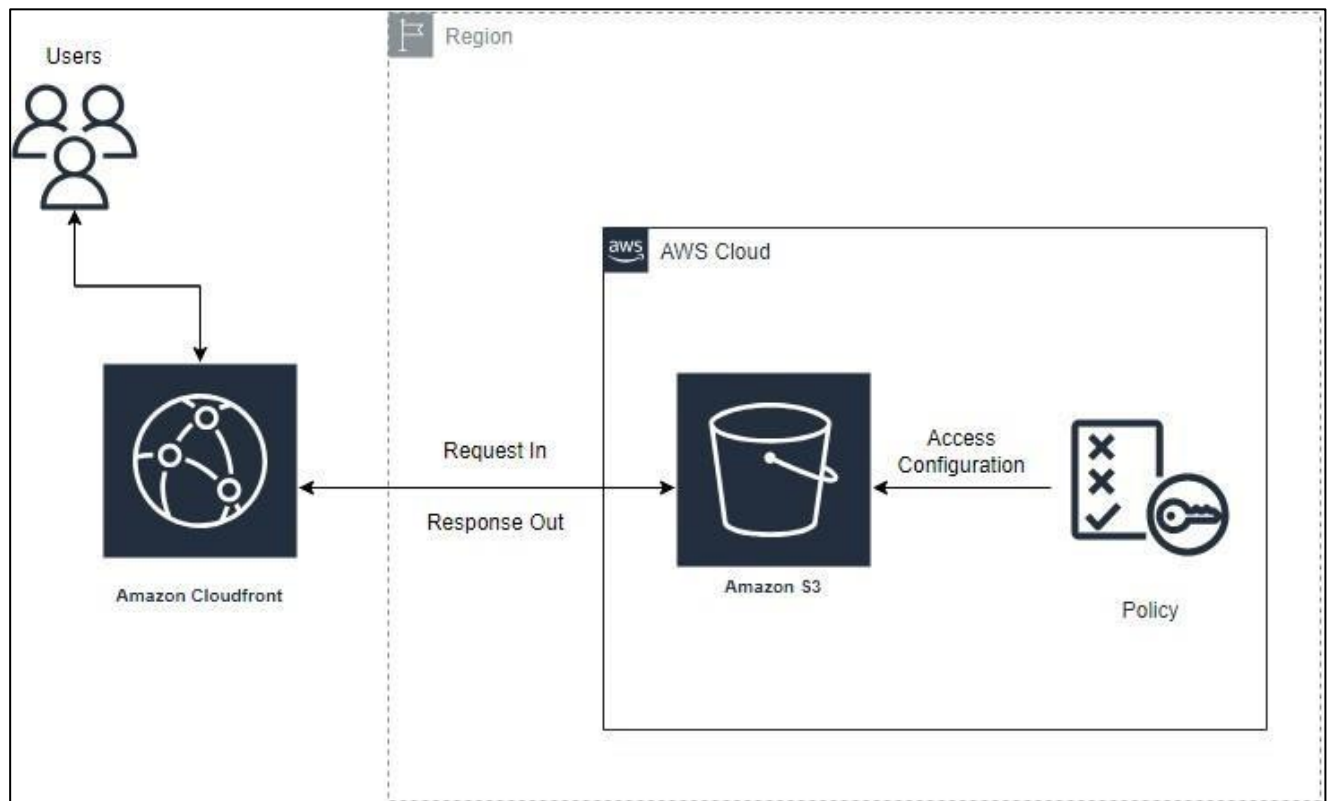
• Project Overview:

1. **Description:** This project involves deploying a static website (Weather App) on Amazon S3 to make it accessible over HTTP/HTTPS.
2. **Objective:** Set up static hosting on AWS S3, configure HTTP/HTTPS, and ensure the website is available publicly with the help of Amazon CloudFront.

• Technologies Used:

1. **AWS Services Used:**
 - Amazon S3 - Amazon CloudFront
2. **For WebApplication:**
 - HTML
 - CSS
 - JavaScript
 - OpenWeatherAPI

AWS Cloud Architecture:



- In this project, this is the architecture I have built for the website hosting.

Note: The main objective of this project is deploy the weather webapp securely on the Internet.

Part 1:

Website Creation:

- The Weather WebApp is one of my old project I built few months ago.
- As this project focuses on deployment, I will provide source code for the website.

Part 2:

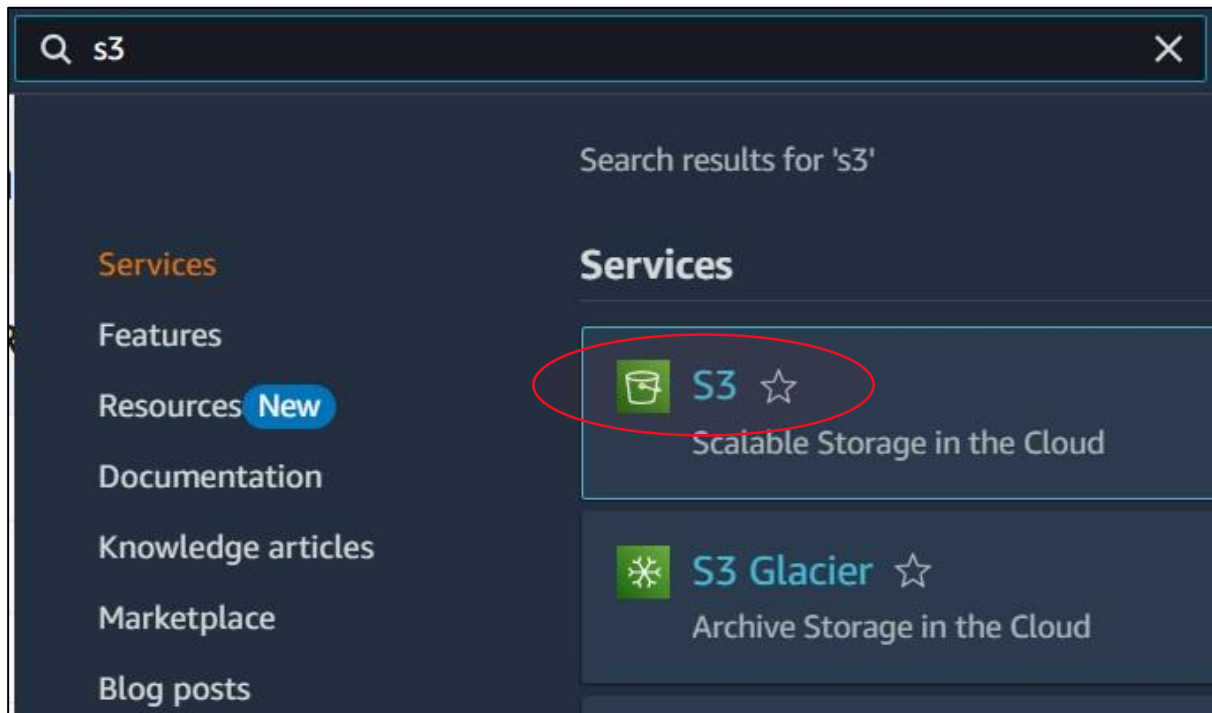
Deployment Process:

Note: if you don't have IAM user create one from the root user. with AmazonS3FullAccess and CloudFrontFullAccess policies.

Follow this guide for creating IAM User: [IAM User creation](#)

1. Creating S3 bucket using IAM user with following configurations:

a. Go to S3 Service → Create Bucket



Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name [Info](#)

Unique Bucket Name!

weather_webapp

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: s3://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.

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](#)

Allow Public Access

☐ 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.

▼ Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

☒ Disable

☐ Enable

Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

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

Cancel

Create bucket

b. after successfully creating bucket:

Go to buckets → Upload → Adding Required Files:

Amazon S3 > Buckets

Account snapshot - updated every 24 hours

View Storage Lens dashboard

General purpose buckets

Directory buckets

General purpose buckets (1)

Copy ARN

Empty

Delete

Create bucket

Find buckets by name

< 1 >

Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/> weather-webapp	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	September 14, 2024, 19:31:15 (UTC+05:30)

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 SDK 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 (13 Total, 620.8 KB)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 2 >

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	app-icon.jpg	-	image/jpeg
<input type="checkbox"/>	backg.jpg	-	image/jpeg
<input type="checkbox"/>	clear.png	-	image/png
<input type="checkbox"/>	cloud_def.png	-	image/png
<input type="checkbox"/>	clouds.png	-	image/png
<input type="checkbox"/>	drizzle.png	-	image/png
<input type="checkbox"/>	index.html	-	text/html
<input type="checkbox"/>	location-not-found.svg	-	image/svg+xml
<input type="checkbox"/>	mist.png	-	image/png
<input type="checkbox"/>	rain.png	-	image/png

Added Required Files!

After successfully adding the required files, I kept the properties default to Standard storage type as I need to access the file frequently.

For permissions I kept them default.

Now, click on upload.

c. go to bucket → properties → scroll to enable static web hosting:

Amazon S3 > Buckets > weather-webapp > 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

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

Static website hosting
Enabled

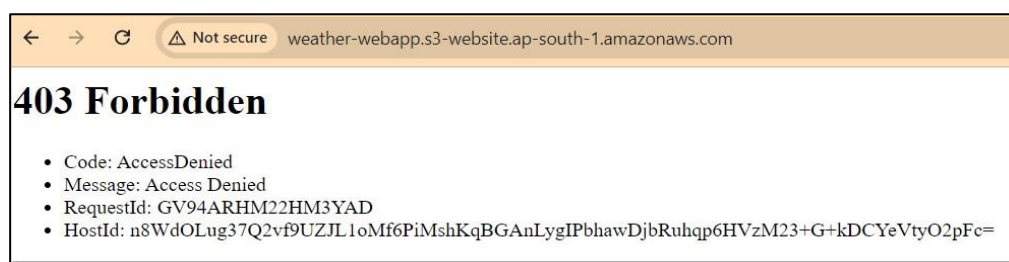
Hosting type
Bucket hosting

Bucket website endpoint copied

website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

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

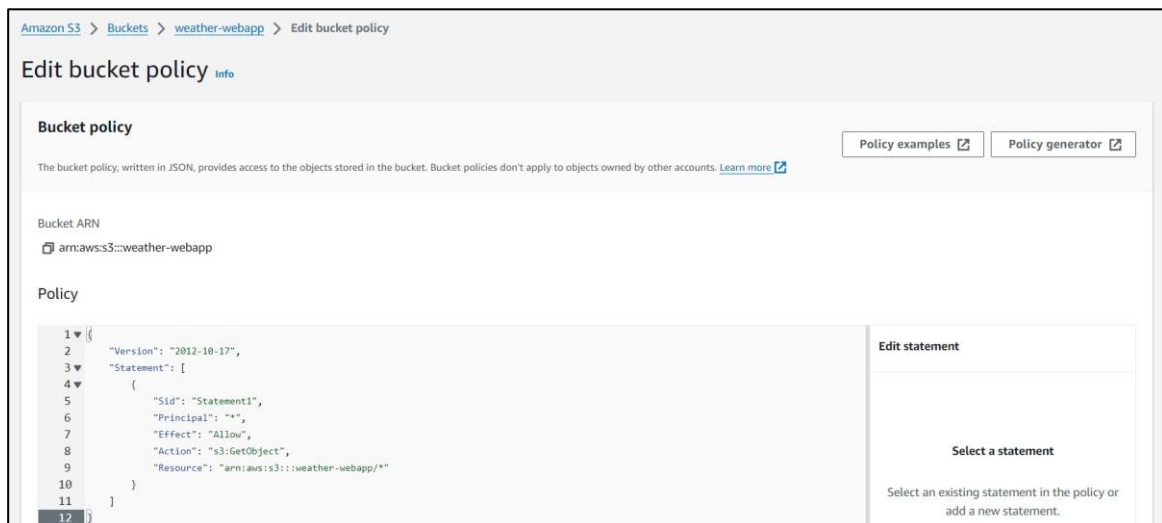
copy the given link to check whether website is working or not. paste it in new tab:



Access is Denied, as we have not configured the bucket policy.

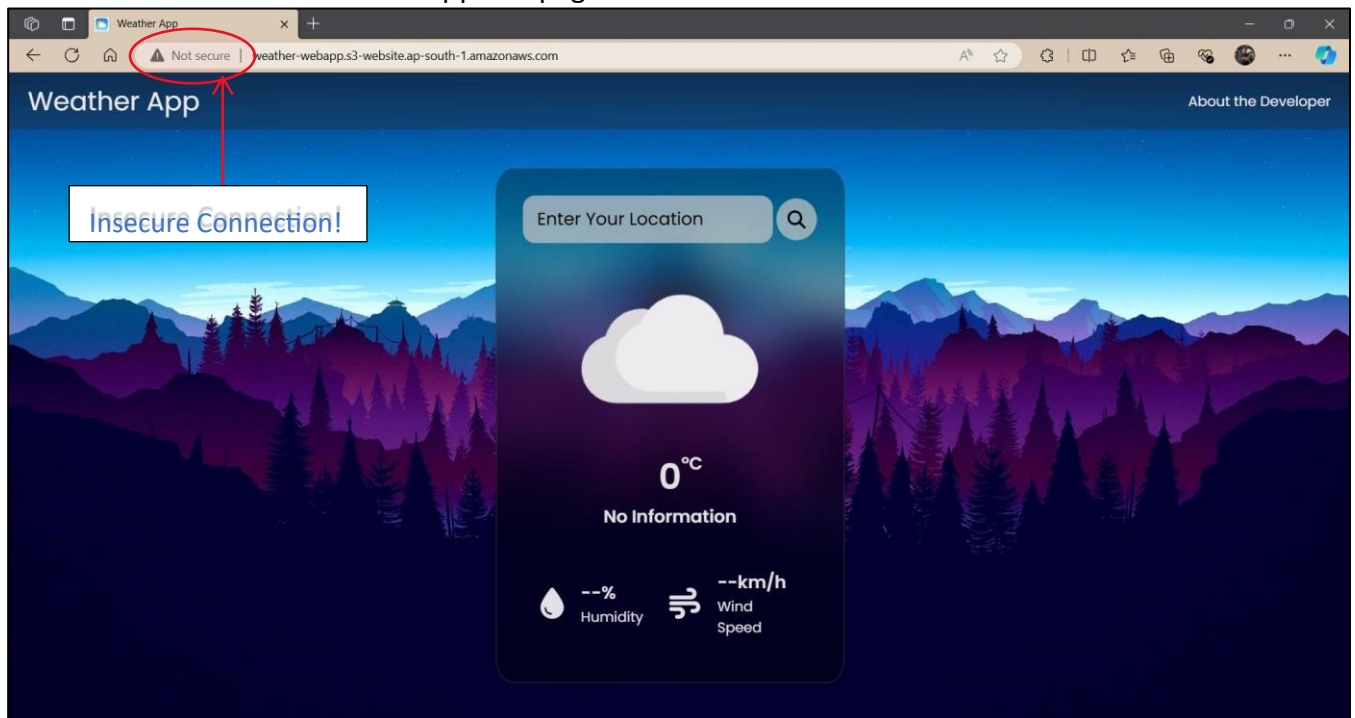
Configure bucket policy in Bucket's permissions tab and Add following Statement:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "Statement1",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::weather-webapp/*"  
    }  
  ]  
}
```



Save changes.

Now refresh the tab of Weather App webpage:



Successfully deployed the website on Amazon S3 but it is still insecure.

2. Securing the website using Amazon CloudFront:

- Go to Services → CloudFront → Create Distribution

CloudFront > Distributions > Create

Create distribution

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name.

weather-webapp.s3.ap-south-1.amazonaws.com

Warning: 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.

Use website endpoint

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

Enter the origin path

Name
Enter a name for this origin.

weather-webapp.s3.ap-south-1.amazonaws.com

Selecting my origin domain name, i.e. same as static web url of the bucket.

Viewer protocol policy

☐ HTTP and HTTPS

☒ Redirect HTTP to HTTPS

☐ HTTPS only

Allowed HTTP methods

☒ GET, HEAD

☐ GET, HEAD, OPTIONS

☐ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Restrict viewer access
If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.

☒ No

☐ Yes

Cache key and origin requests

We recommend using a cache policy and origin request policy to control the cache key and origin requests.

☒ Cache policy and origin request policy (recommended)

☐ Legacy cache settings

Cache policy
Choose an existing cache policy or create a new one.

CachingOptimized Recommended for S3

Policy with caching enabled. Supports Gzip and Brotli compression.

Create cache policy View policy

Origin request policy - *optional*
Choose an existing origin request policy or create a new one.

Select origin policy

Create origin request policy

For default root object, give the name of homepage.

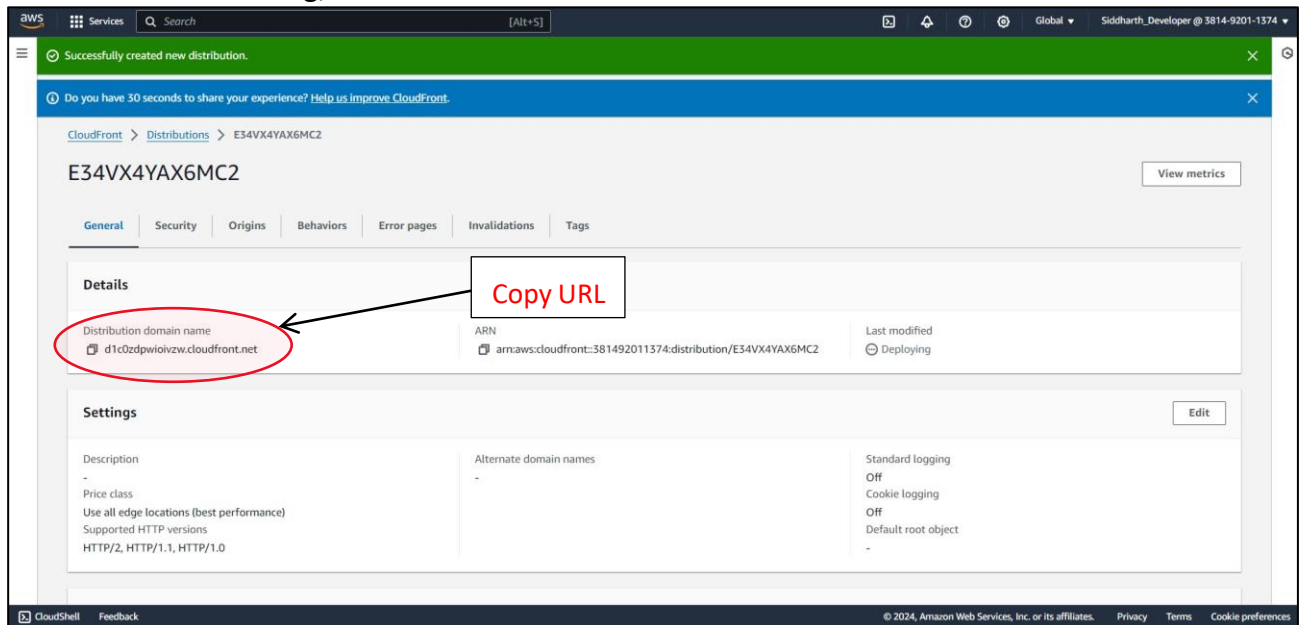
Default root object - optional

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

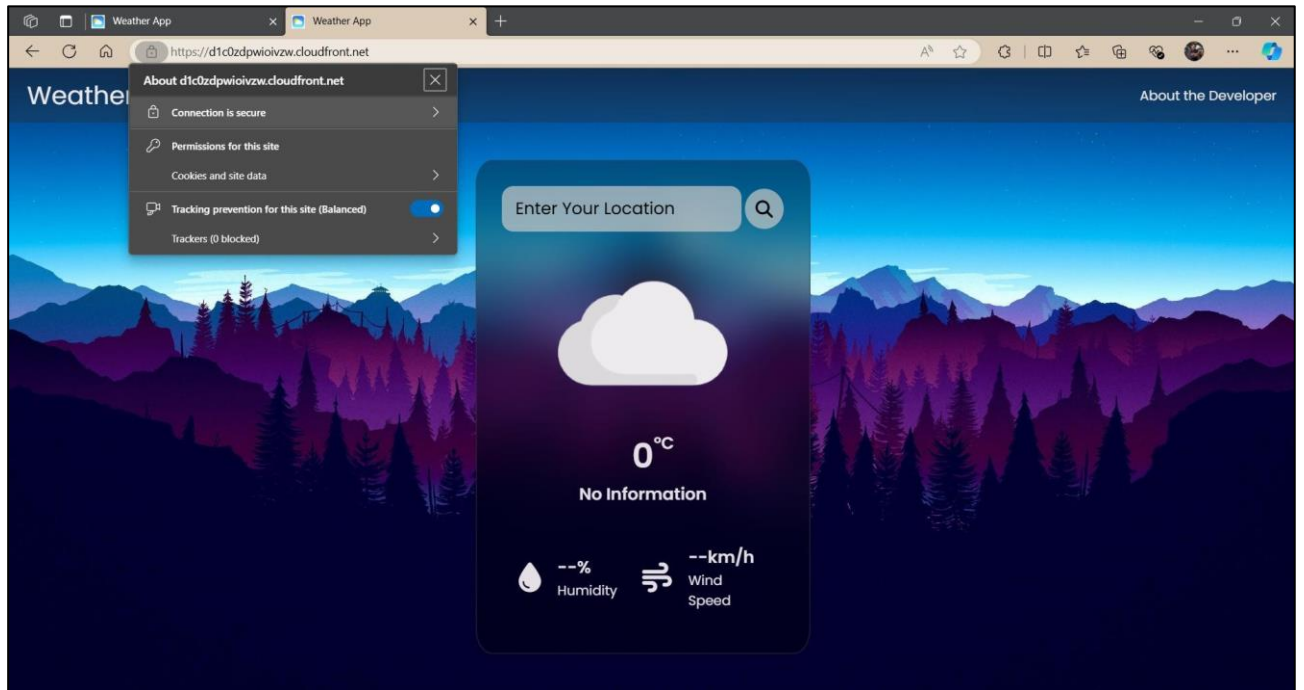
index.html

For WAF protection disable it and Create the Distribution.

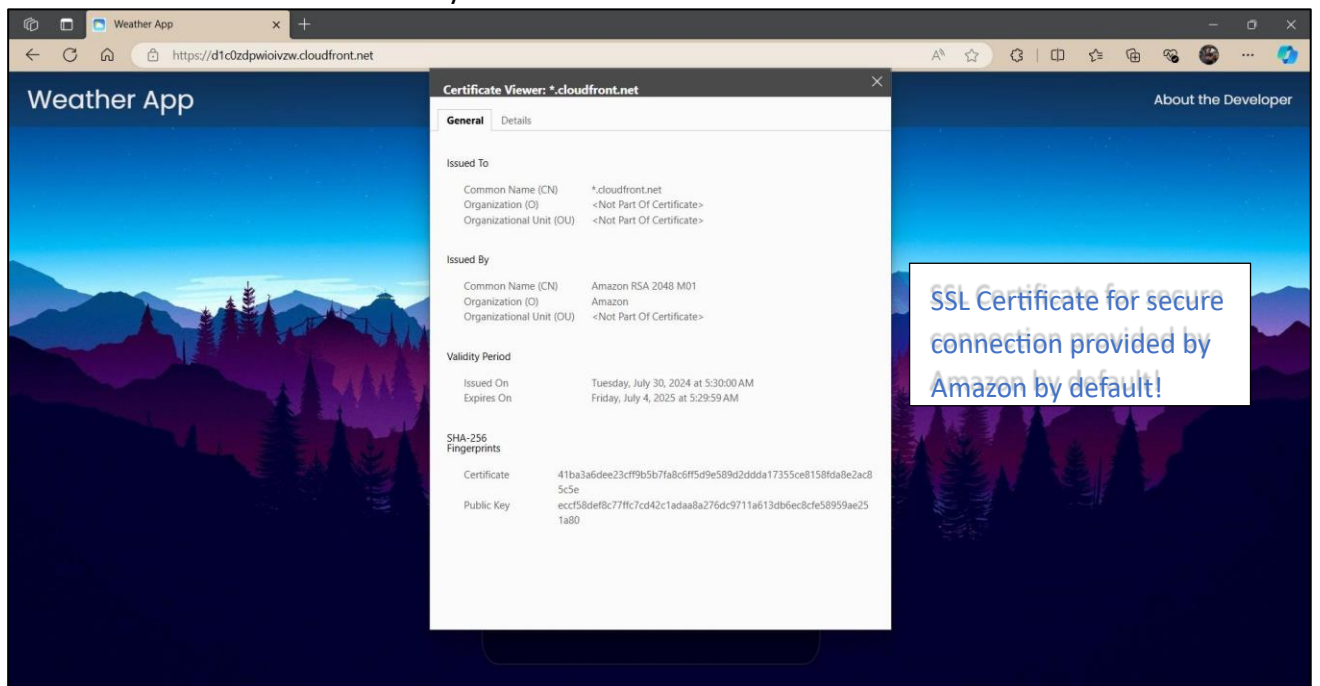
After successful creating, wait for the distribution to be available.



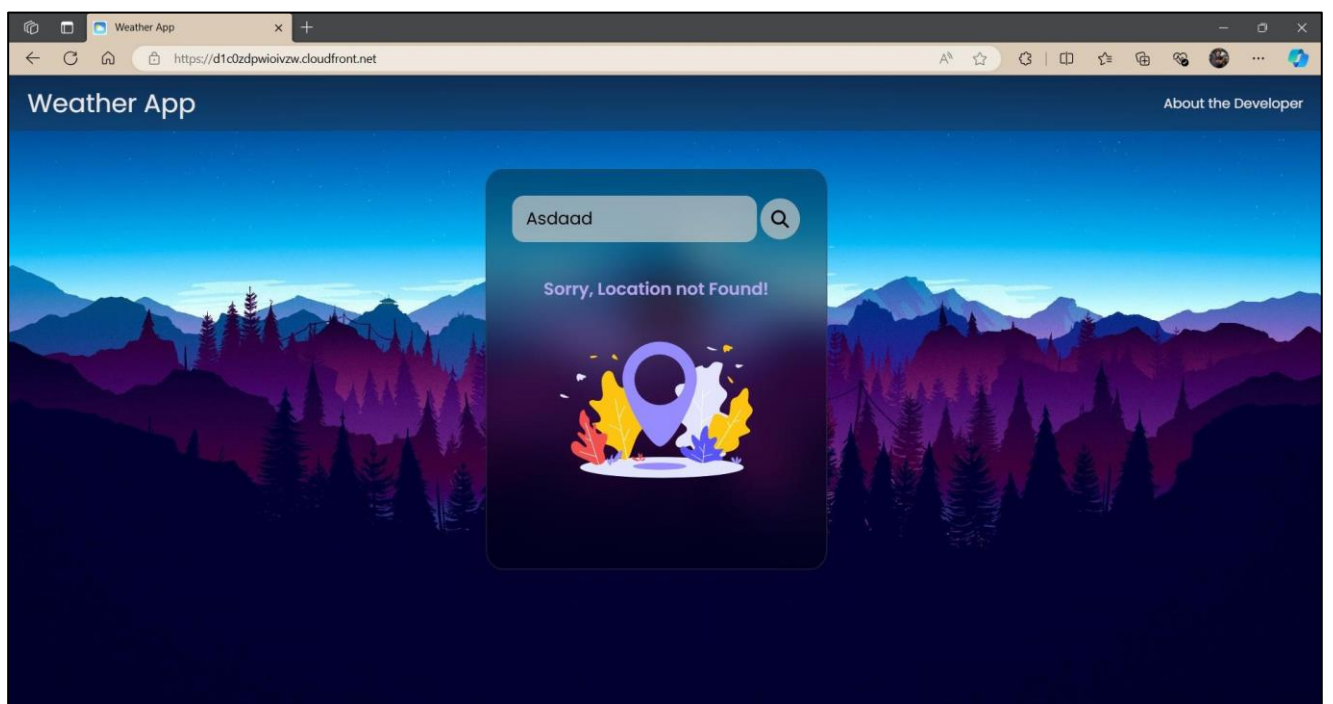
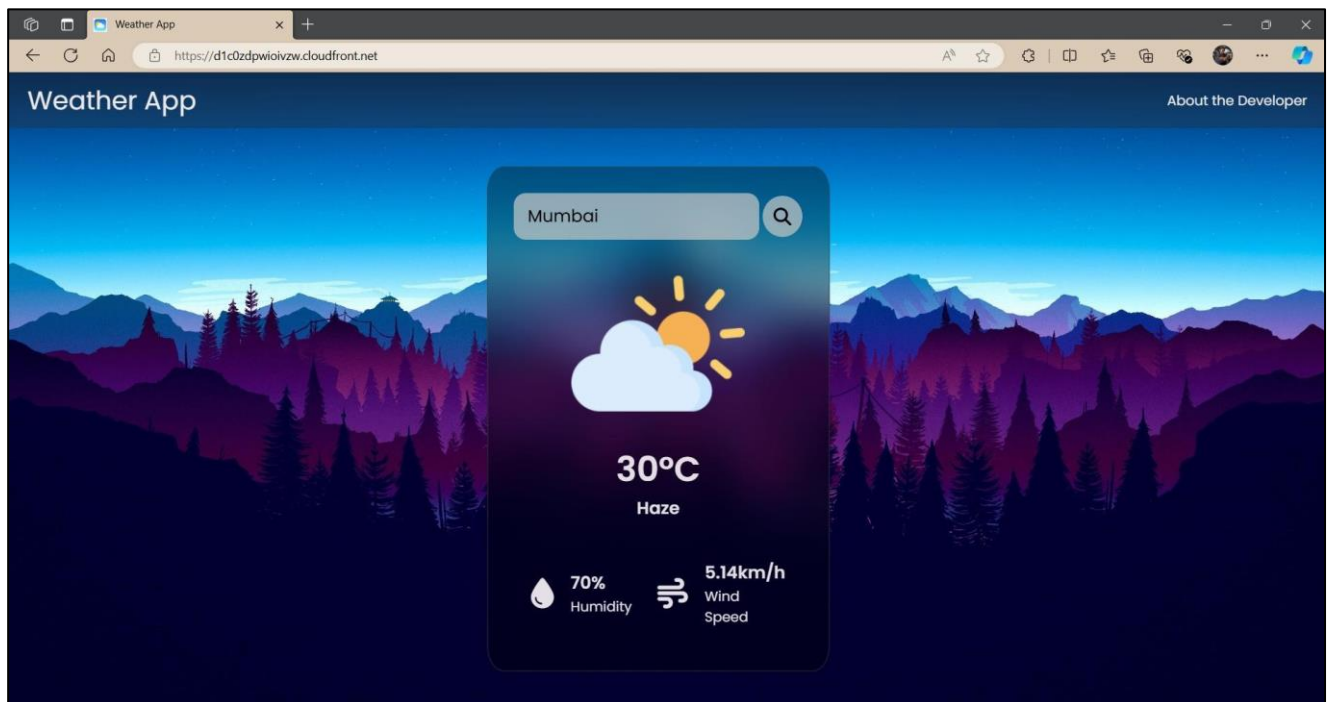
Copy the URL and paste in new tab:

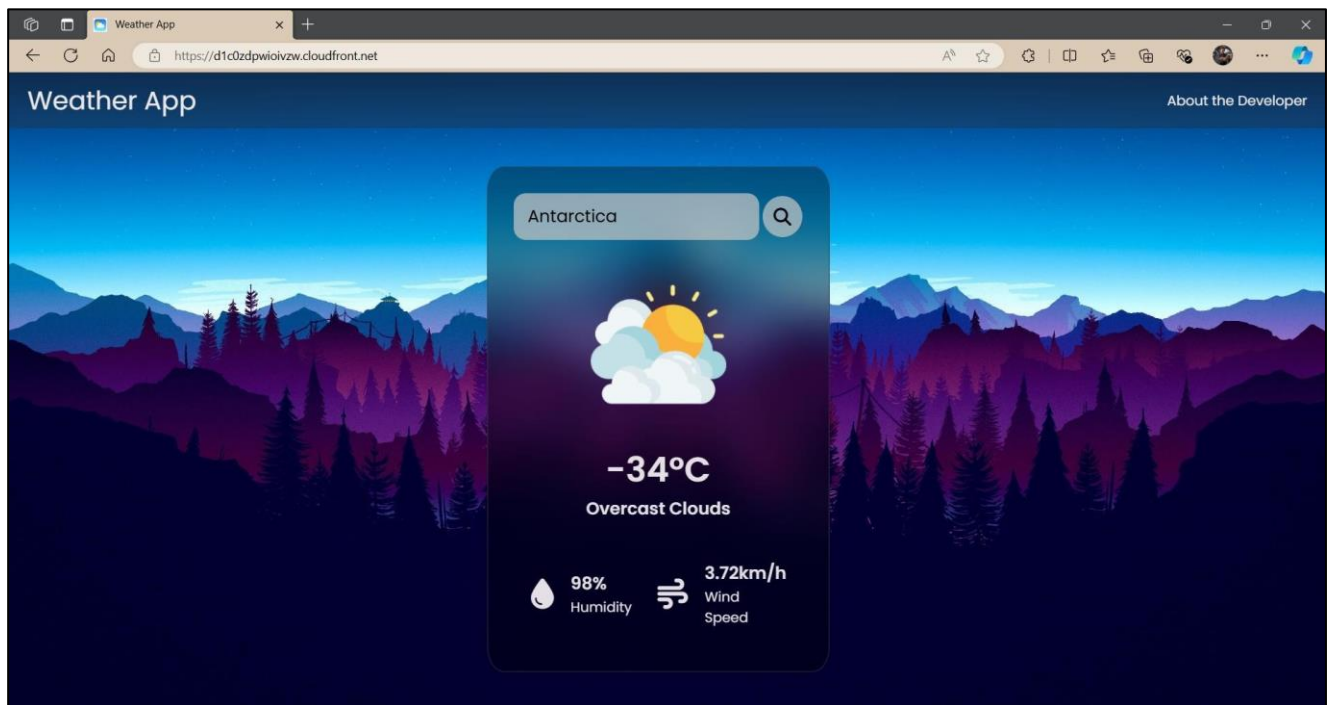


The has been launched successfully with secure HTTPS connection.



Part 3: Testing of the Weather WebApp





Limitations:

- As you can see the domain name is by default of the AWS CloudFront, so as a free tier user with no Domain Name owning this is one of the limitations I faced.
- But to counter it we can use Amazon Route53 service to purchase/transfer owned domain to completely make website your but for that we also require SSL/TLS certificate which can be generated using Amazon ACM.
- For further implementation of Route53 and ACM certification you can visit:
- [Website hosting using CloudFront and Route53](#)
- [Know more about generating certificate](#)