

**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

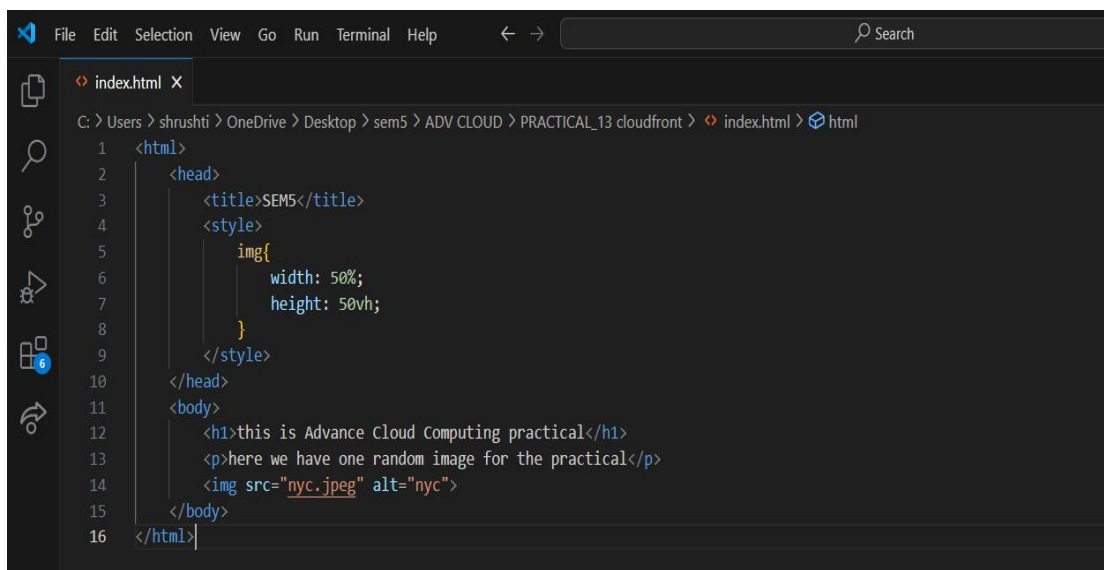
**Name of the Student:** Shrushti Krishna Shrivastav

**PRN:** 20220801024

**Title of Practicle :** Securely access S3 images using Amazon Cloud Front

**STEP1: Create Index.html**

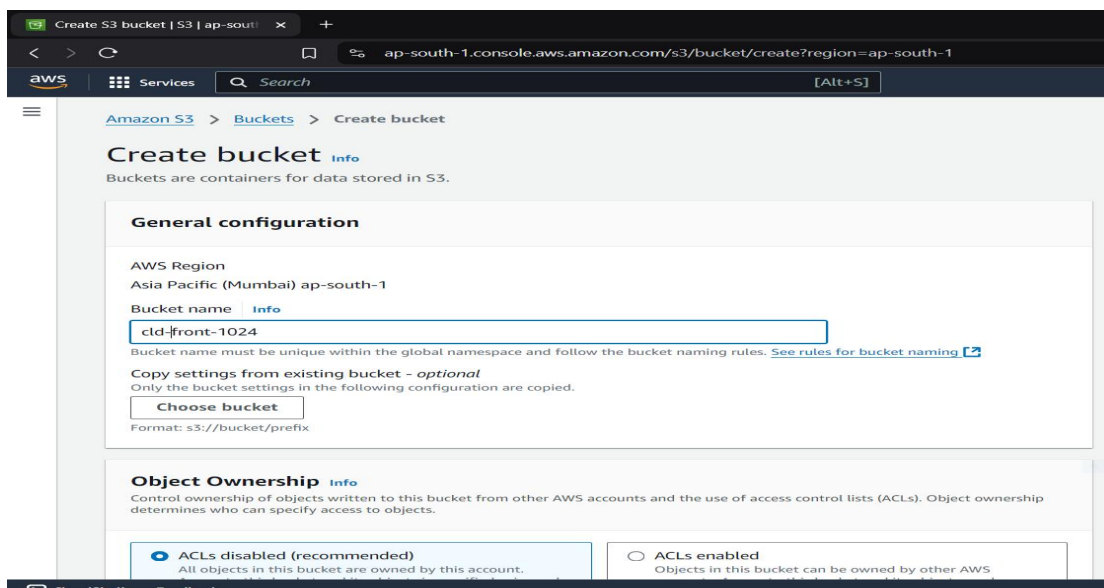
Create one html file



```
File Edit Selection View Go Run Terminal Help
index.html X
C:\Users> shrushti > OneDrive > Desktop > sem5 > ADV CLOUD > PRACTICAL_13 cloudfront > index.html > html
1 <html>
2   <head>
3     <title>SEMS</title>
4     <style>
5       img{
6         width: 50%;
7         height: 50vh;
8       }
9     </style>
10  </head>
11  <body>
12    <h1>this is Advance Cloud Computing practical</h1>
13    <p>here we have one random image for the practical</p>
14    
15  </body>
16 </html>
```

**STEP2: Create S3 bucket and upload the file**

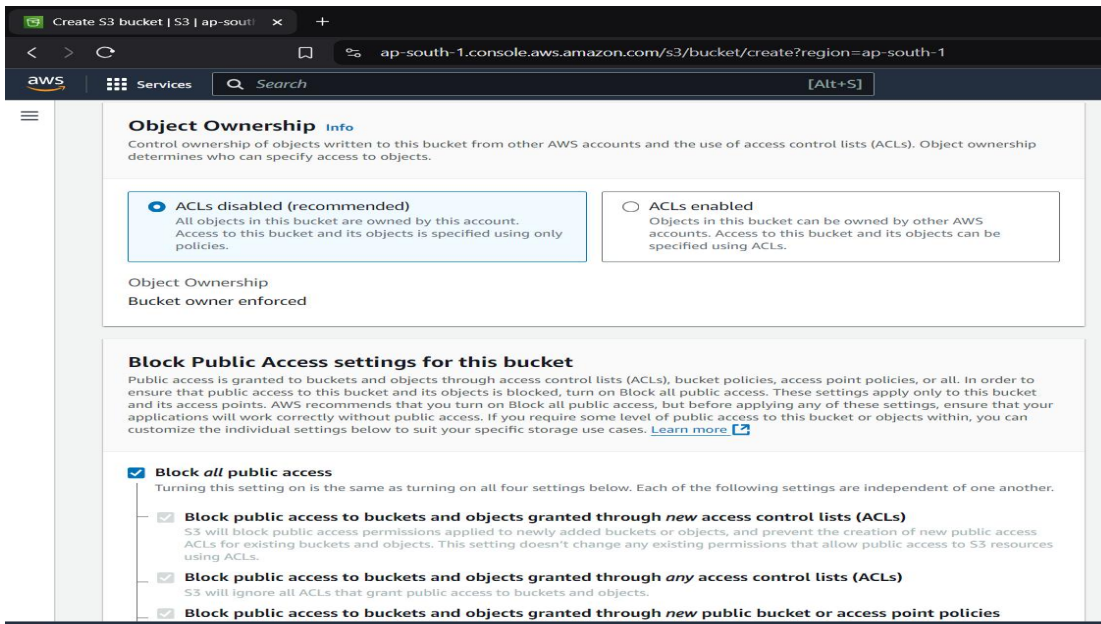
Create one bucket



**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (SCSEA)**  
**Subject: Advance Cloud Computing(ACC)**

**Name of the Student:** Shrushti Krishna Shrivastav **PRN:** 20220801024

**Title of Practicle :** Securely access S3 images using Amazon Cloud Front



**Create S3 bucket | S3 | ap-south-1**

ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1

**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 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.

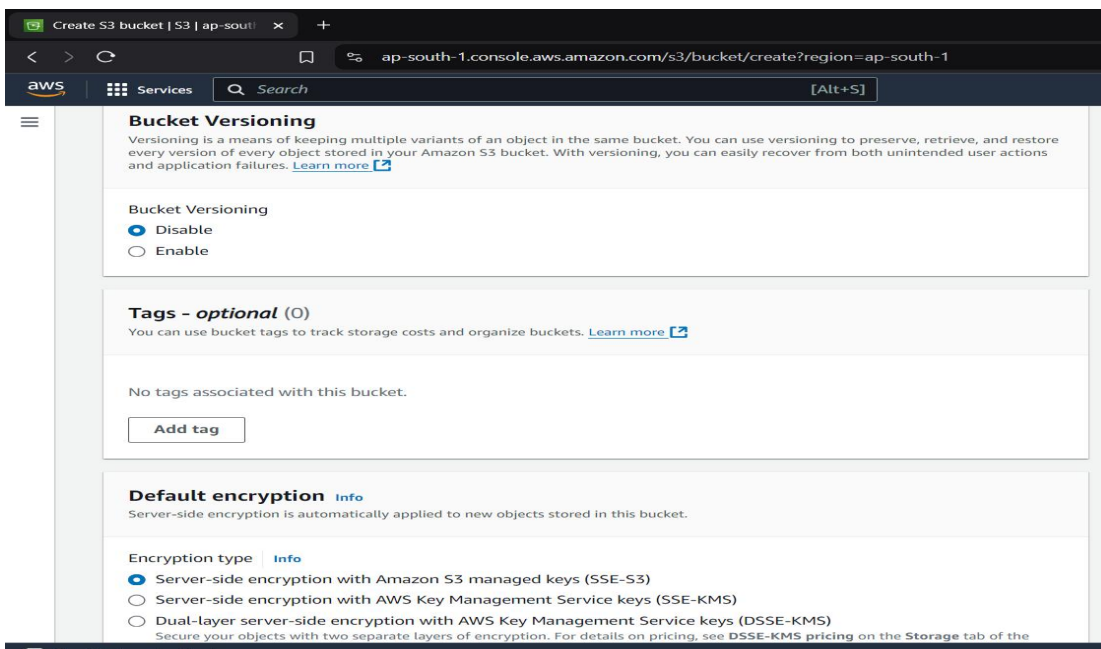
Object Ownership  
Bucket owner enforced

**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**



**Create S3 bucket | S3 | ap-south-1**

ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1

**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](#)

**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

**School of Computer Science, Engineering and Applications(SCSEA)**

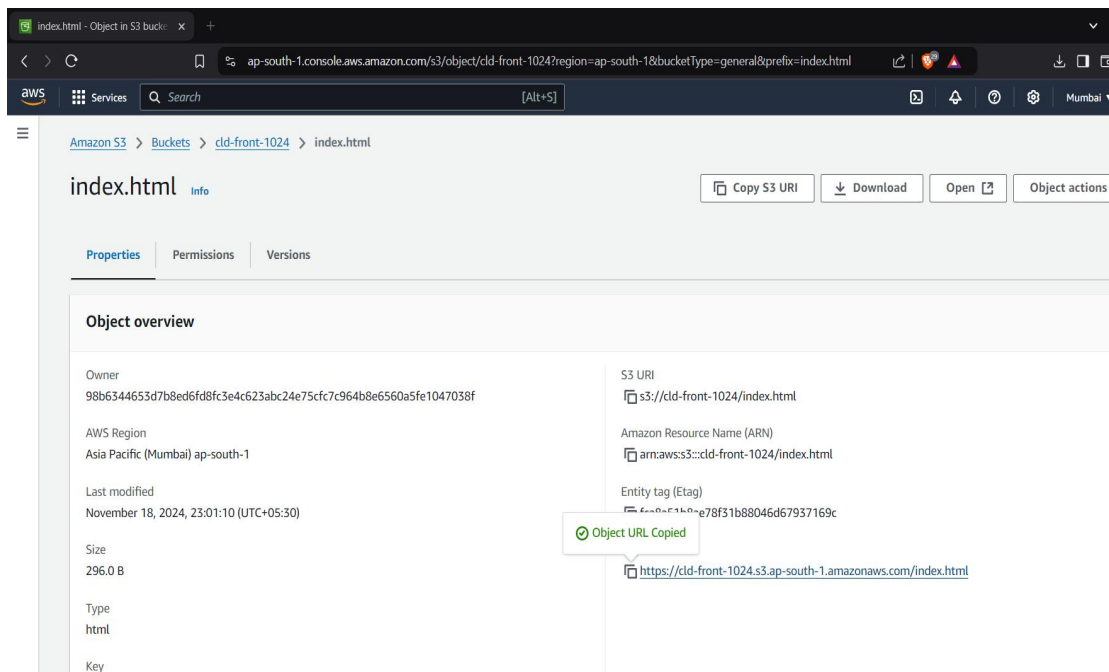
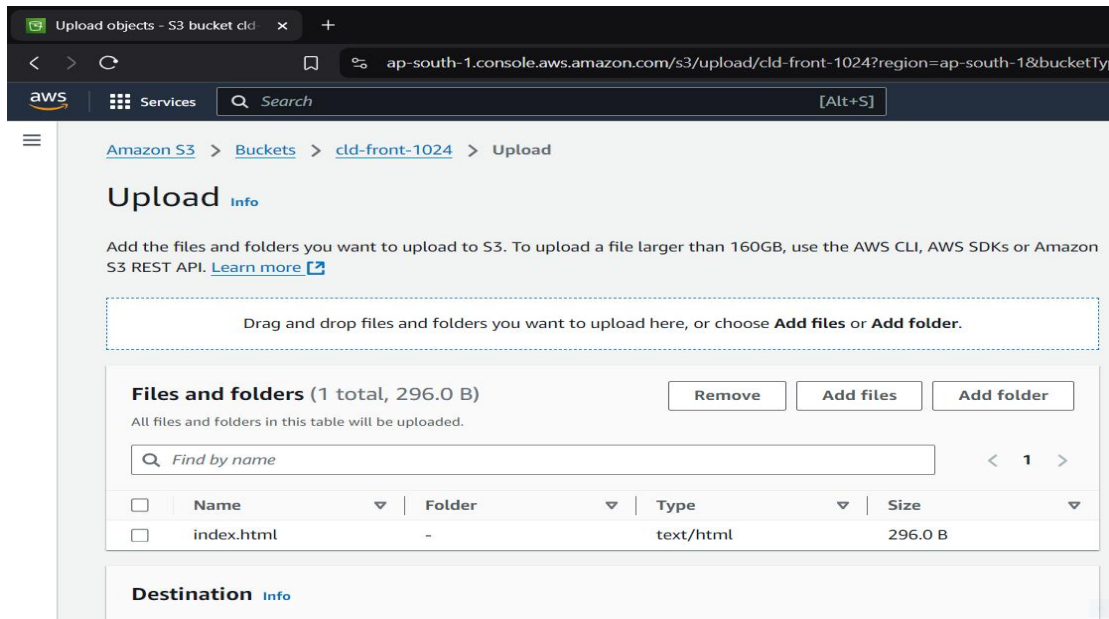
**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

**Name of the Student:** Shrushti Krishna Shrivastav

**PRN:** 20220801024

**Title of Practicle :** Securely access S3 images using Amazon Cloud Front



**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

**Name of the Student:** Shrushti Krishna Shrivastav

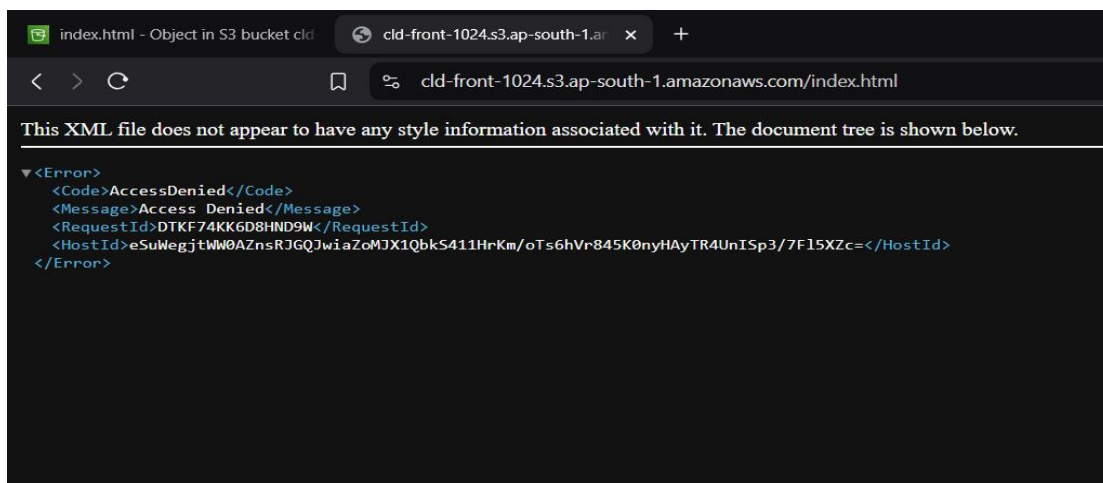
**PRN:** 20220801024

**Title of Practicle :**

Securely access S3 images using Amazon Cloud Front

**STEP3: try to access the file**

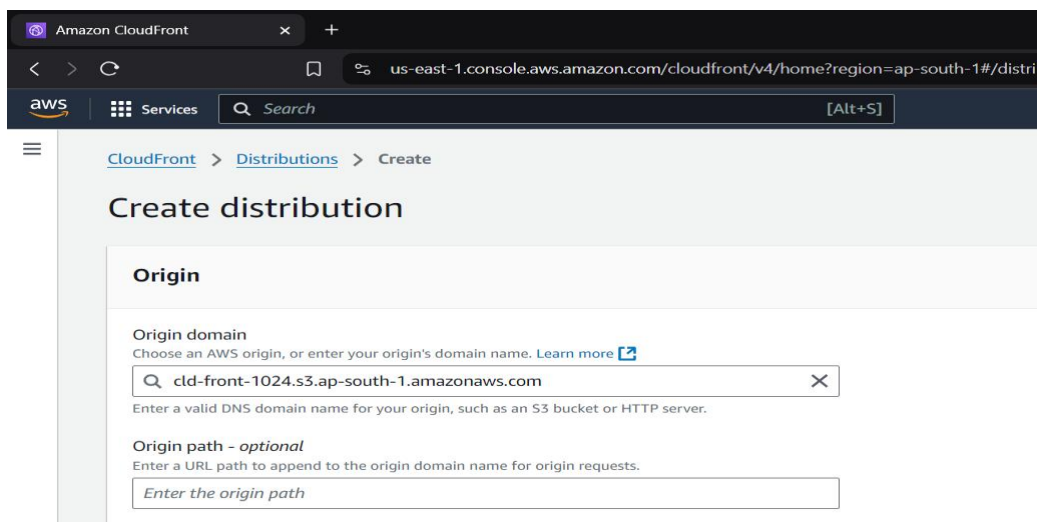
Copy paste the object url on browser--



We can't access this as we blocked all public access

**STEP4: cloudfront**

Go to cloudfront and create one distribution





**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

**Subject: Advance Cloud Computing(ACC)**

**Name of the Student:** Shrushti Krishna Shrivastav

**PRN:** 20220801024

**Title of Practicle :** Securely access S3 images using Amazon Cloud Front

Name  
Enter a name for this origin.

cld-front-1024.s3.ap-south-1.amazonaws.com

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.

[Alt+S]

**Create new OAC** ×

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

cld-front-1024.s3.ap-south-1.amazonaws.com

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

Enter description

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

S3

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

Cancel Create





## School of Computer Science, Engineering and Applications(SCSEA)

### B.C.A. TY (SCSEA)

### Subject: Advance Cloud Computing(ACC)

Name of the Student: Shrushti Krishna Shrivastav

PRN: 20220801024

Title of Practicle : Securely access S3 images using Amazon Cloud Front

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](#)

**You must update the S3 bucket policy**  
CloudFront will provide you with the policy statement after creating the distribution.

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

► Additional settings

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

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  
☐ Use North America, Europe, Asia, Middle East, and Africa

Alternate domain name (CNAME) - *optional*  
Add the custom domain names that you use in URLs for the files served by this distribution.

[Add item](#)

**To add a list of alternative domain names, use the [bulk editor](#).**

Custom SSL certificate - *optional*  
Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region.

[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.

## School of Computer Science, Engineering and Applications(SCSEA)

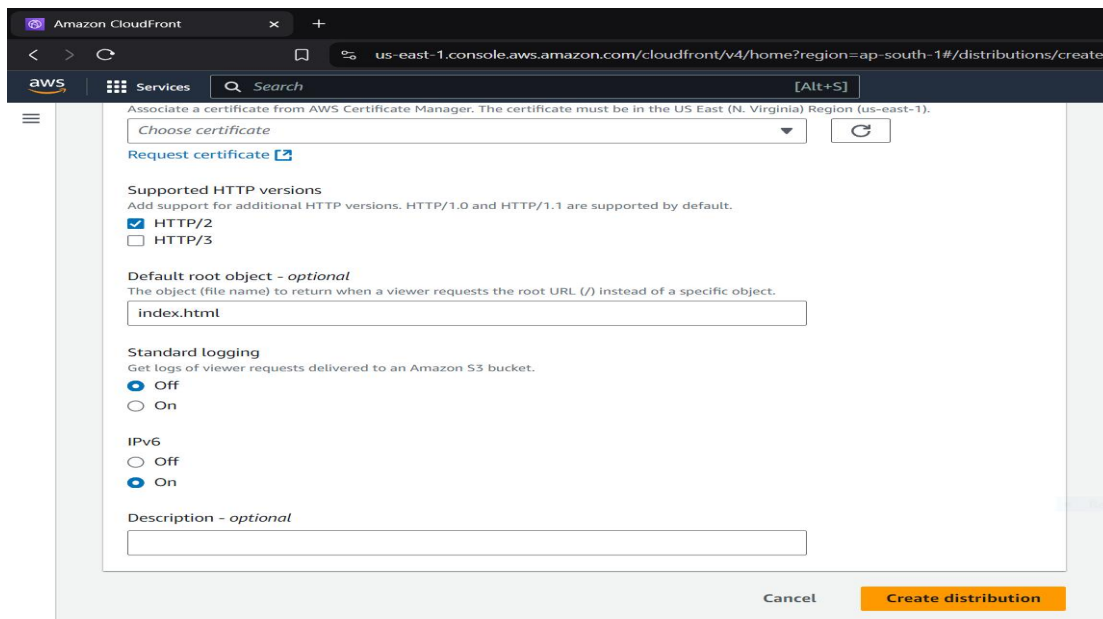
### B.C.A. TY (SCSEA)

### Subject: Advance Cloud Computing(ACC)

Name of the Student: Shrushti Krishna Shrivastav

PRN: 20220801024

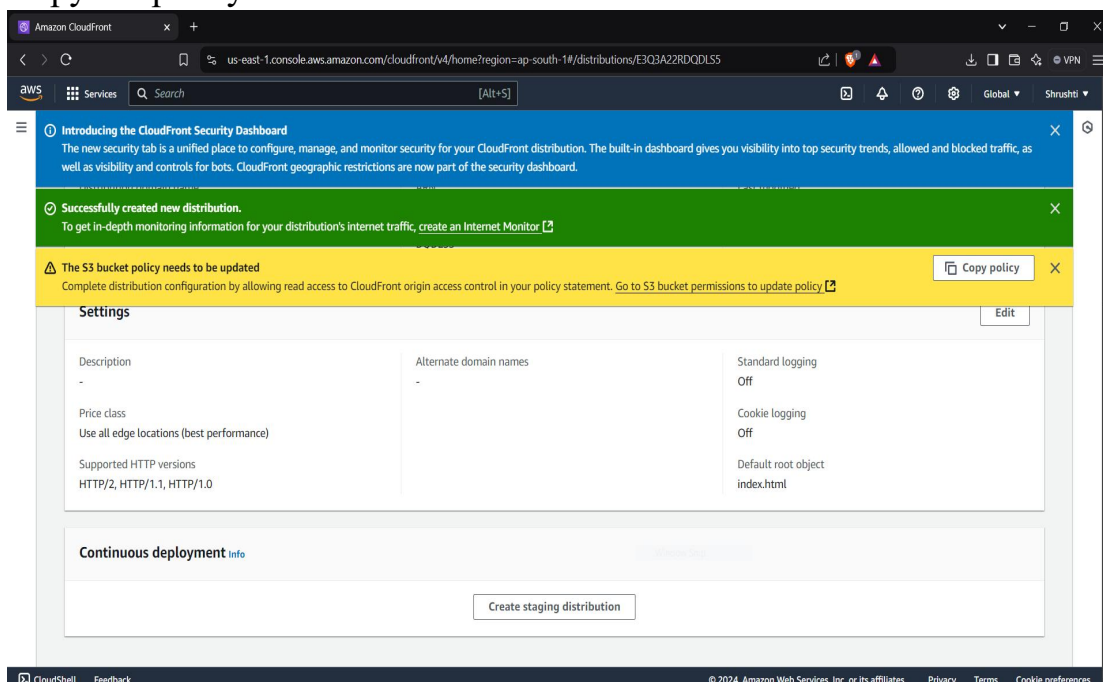
Title of Practicle : Securely access S3 images using Amazon Cloud Front



The screenshot shows the 'Create distribution' page in the Amazon CloudFront console. The URL is `us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=ap-south-1#/distributions/create`. The page includes a 'Choose certificate' dropdown, a 'Request certificate' link, and a 'Supported HTTP versions' section with checkboxes for HTTP/2 (checked) and HTTP/3. The 'Default root object - optional' section has a text input field containing 'index.html'. The 'Standard logging' section has radio buttons for 'Off' (selected) and 'On'. The 'IPv6' section has radio buttons for 'Off' and 'On' (selected). There is a 'Description - optional' text input field at the bottom. At the bottom right, there are 'Cancel' and 'Create distribution' buttons.

### STEP5: edit policy

#### Copy the policy



The screenshot shows the 'Settings' page for a CloudFront distribution in the Amazon CloudFront console. The URL is `us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=ap-south-1#/distributions/E3Q3A22RDQDL55`. The page displays various settings: 'Description' (empty), 'Alternate domain names' (empty), 'Standard logging' (Off), 'Price class' (Use all edge locations (best performance)), 'Supported HTTP versions' (HTTP/2, HTTP/1.1, HTTP/1.0), 'Cookie logging' (Off), and 'Default root object' (index.html). There is a 'Continuous deployment info' section with a 'Create staging distribution' button. A yellow warning banner at the top states 'The S3 bucket policy needs to be updated' and includes a 'Copy policy' button. The page footer includes 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc.

**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

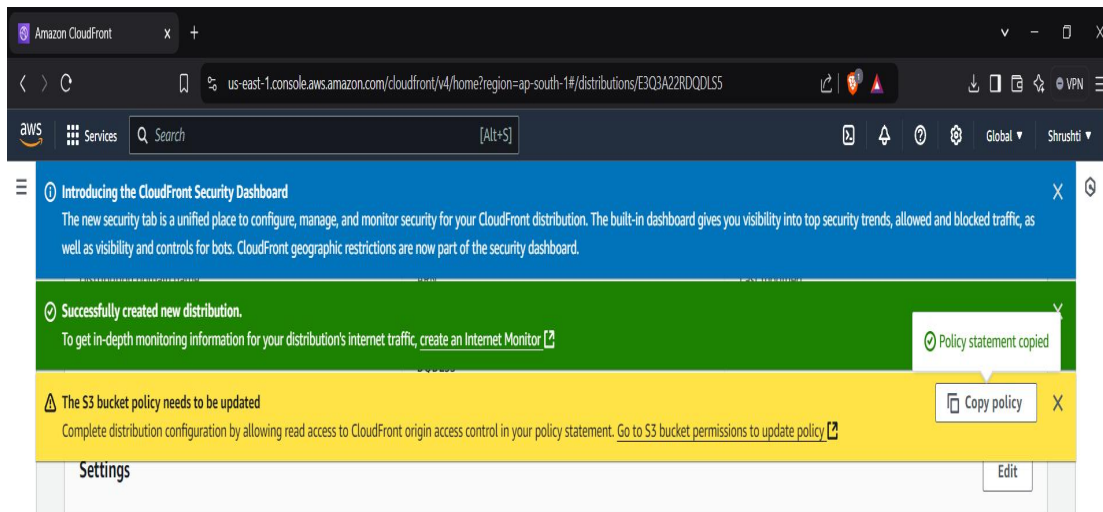
**Subject: Advance Cloud Computing(ACC)**

**Name of the Student:** Shrushti Krishna Shrivastav

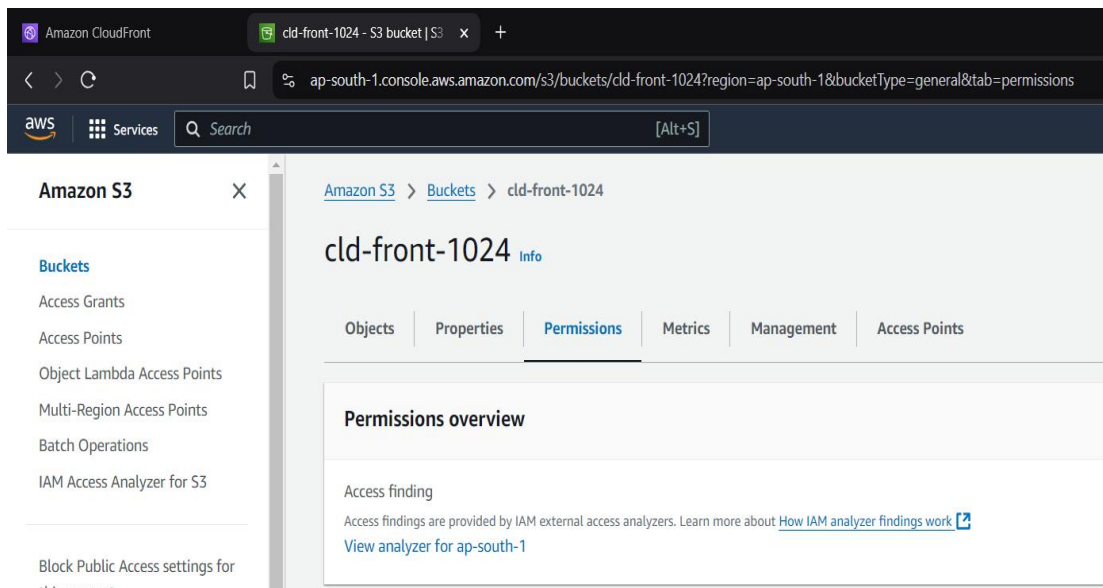
**PRN:** 20220801024

**Title of Practicle :** Securely access S3 images using Amazon Cloud Front

(yellow box)



Go to s3 bucket--permission--





**School of Computer Science, Engineering and Applications(SCSEA)**

**B.C.A. TY (SCSEA)**

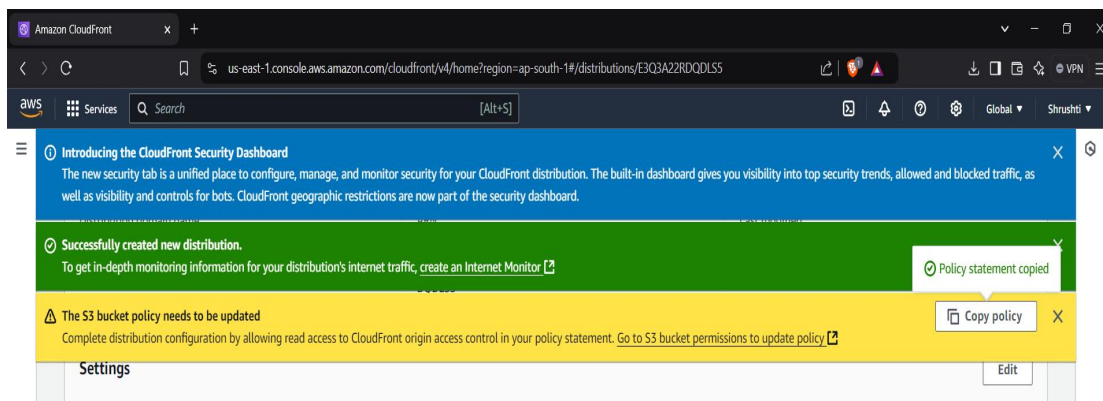
**Subject: Advance Cloud Computing(ACC)**

**Name of the Student:** Shrushti Krishna Shrivastav

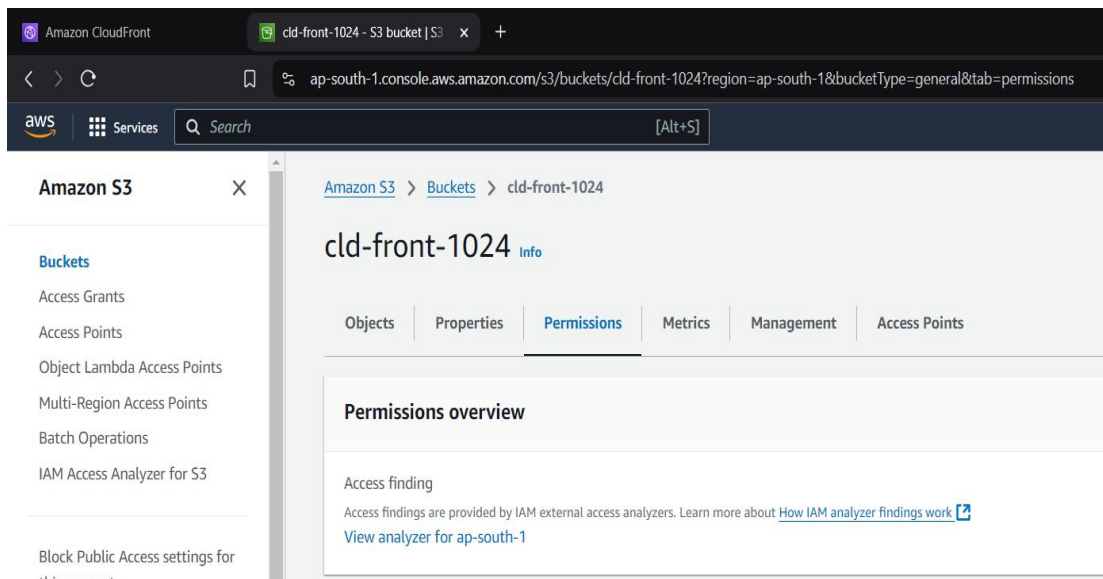
**PRN:** 20220801024

**Title of Practicle :** Securely access S3 images using Amazon Cloud Front

(yellow box)



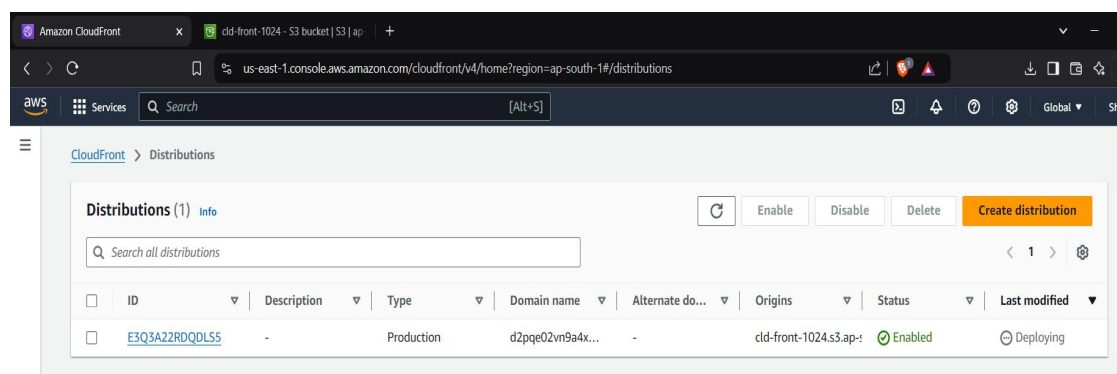
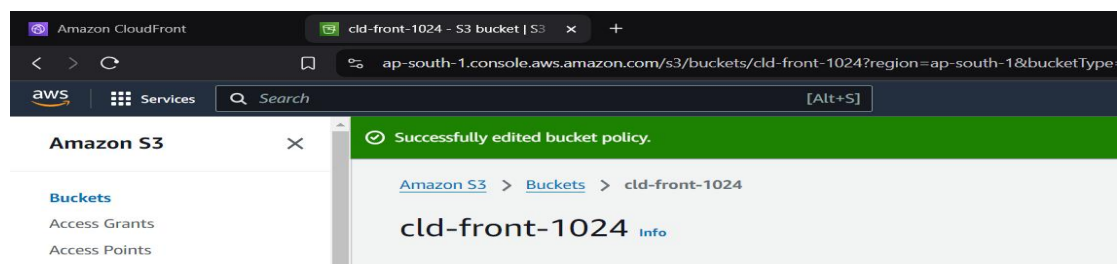
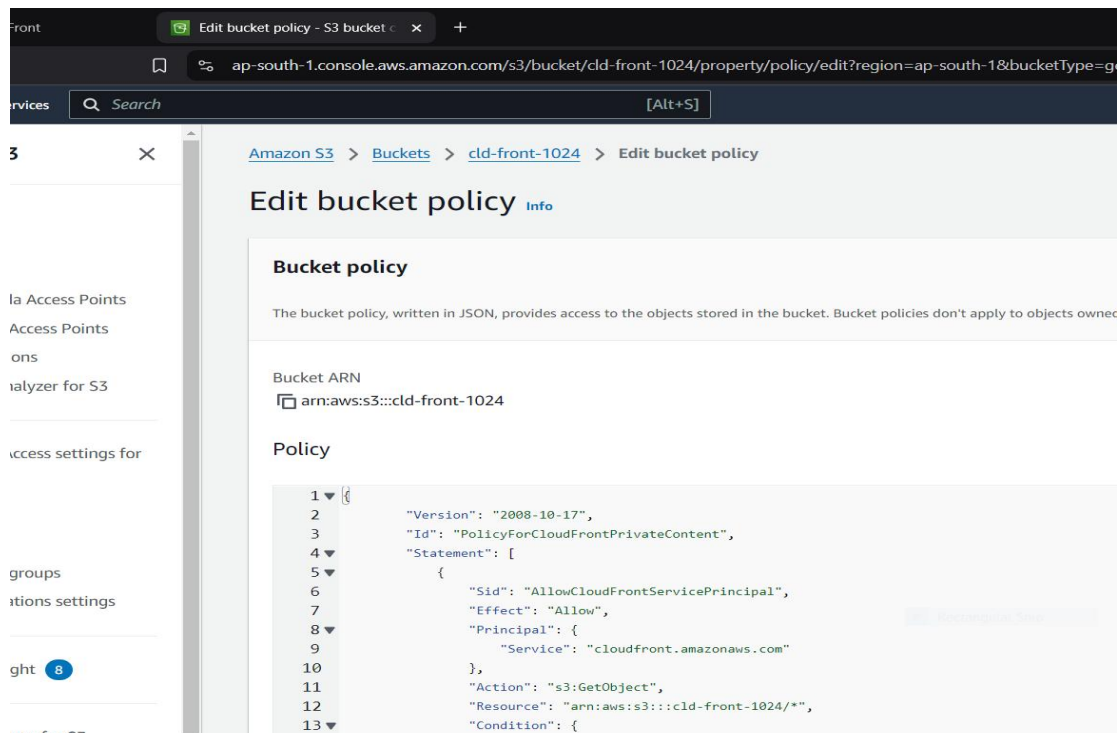
Go to s3 bucket--permission--



**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (SCSEA)**  
**Subject: Advance Cloud Computing(ACC)**

**Name of the Student:** Shrushti Krishna Shrivastav **PRN:** 20220801024

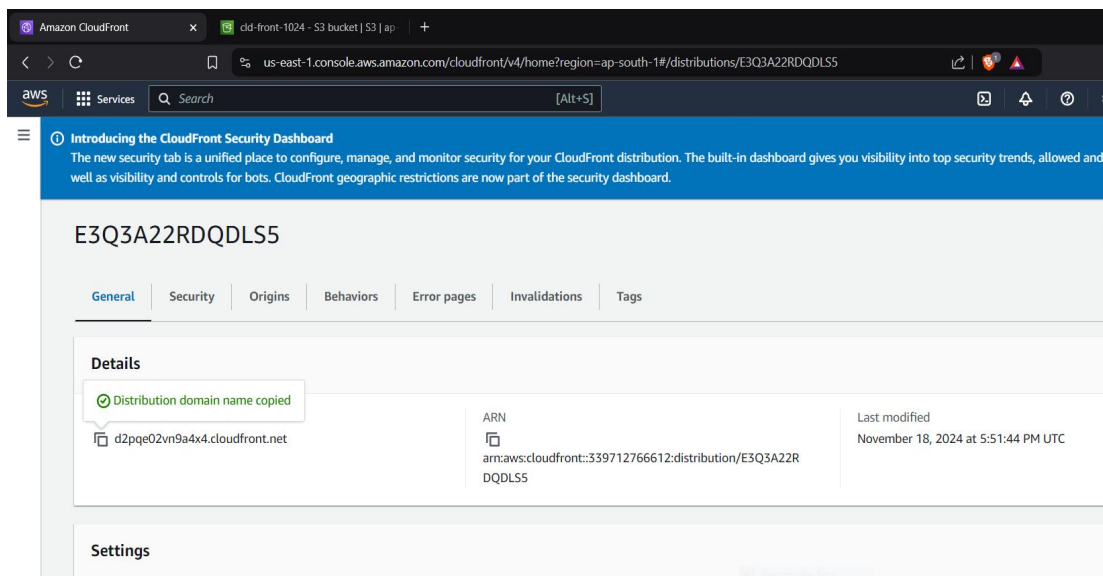
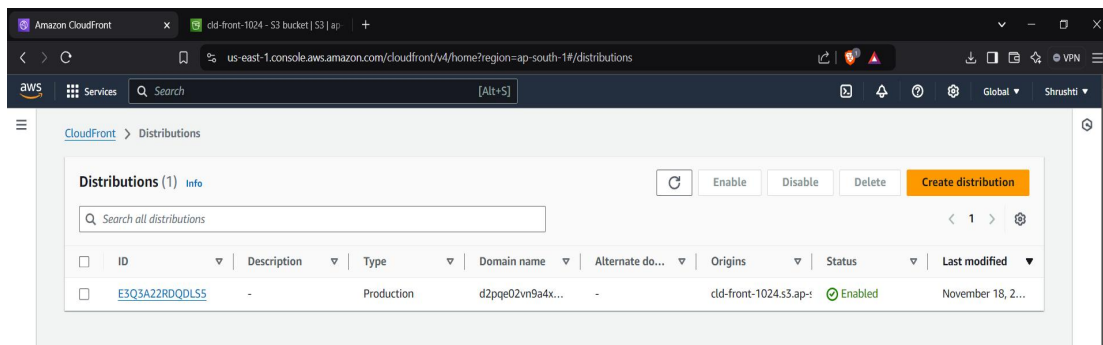
**Title of Practicle :** Securely access S3 images using Amazon Cloud Front



**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (SCSEA)**  
**Subject: Advance Cloud Computing(ACC)**

**Name of the Student:** Shrushti Krishna Shrivastav **PRN:** 20220801024

**Title of Practicle :** Securely access S3 images using Amazon Cloud Front



Now we are able to access (due to edited policy with cloudfront)