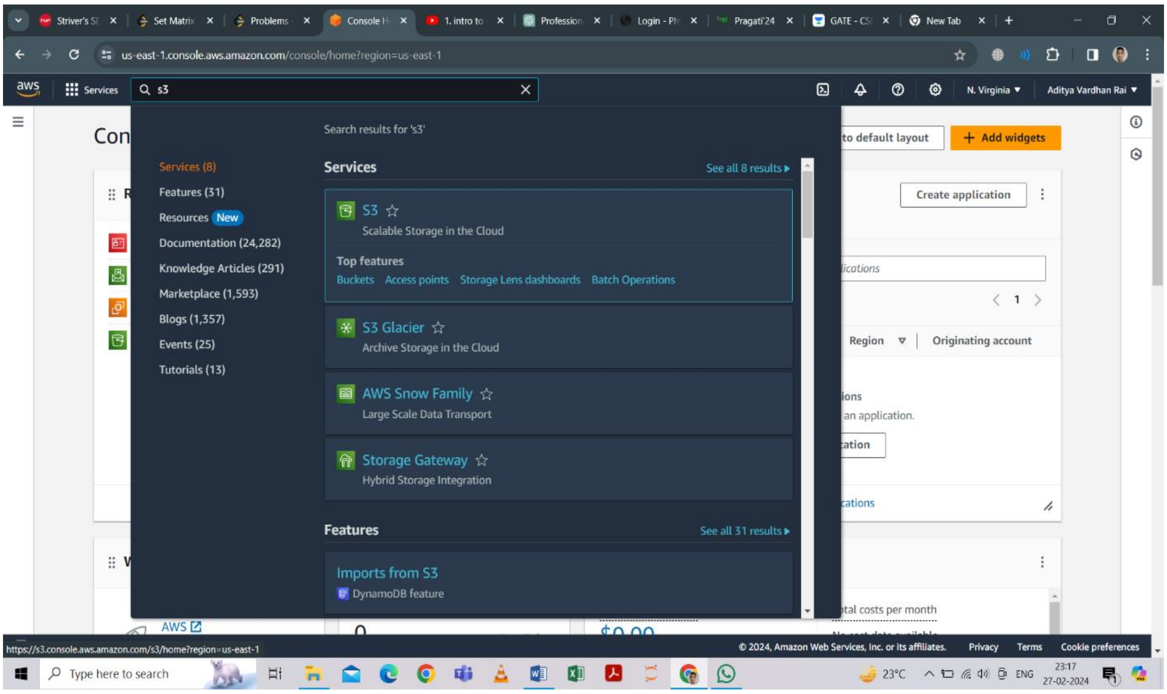
Assignment-6

PROBLEM STATEMENT :

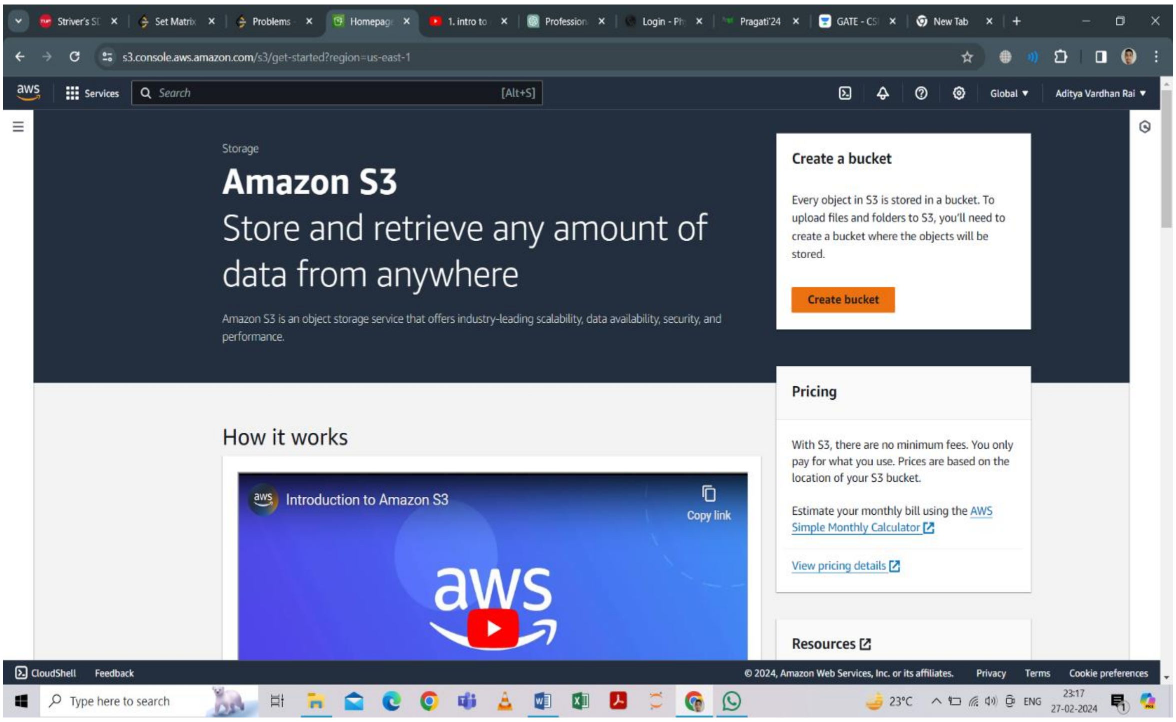
Upload a static website on S3.

Steps to upload a static website on S3->

1. Sign up for an AWS account, search for ‘S3’ then click on it.



2. Click on ‘Create bucket’.



Amazon S3

Store and retrieve any amount of data from anywhere

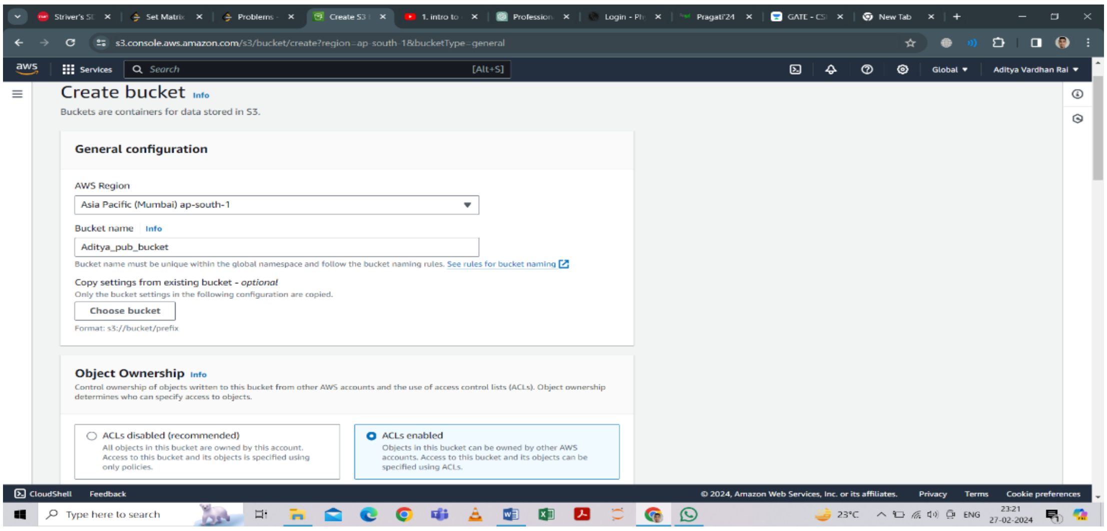
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

3. Fill up the required details: ’Aws Region’, ’Bucket name’. Click on ‘ACLs enabled’, uncheck ‘Block all public access’, tick ‘I acknowledge…’ and then click on ‘Create bucket’.



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

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name Info

Aditya_pub_bucket

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

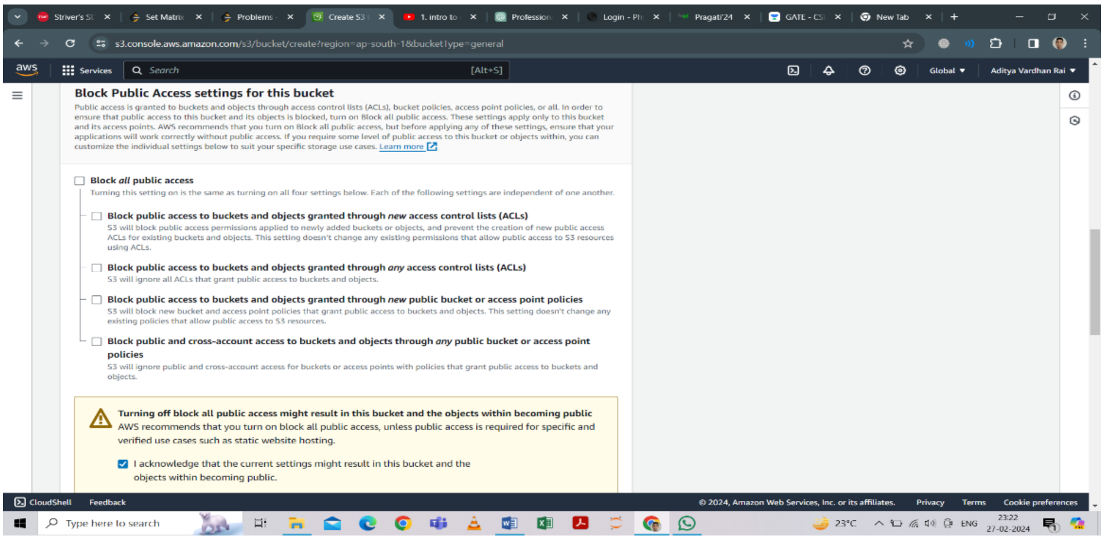
Format: s3://bucket/prefix

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.



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

Block Public Access settings for this bucket

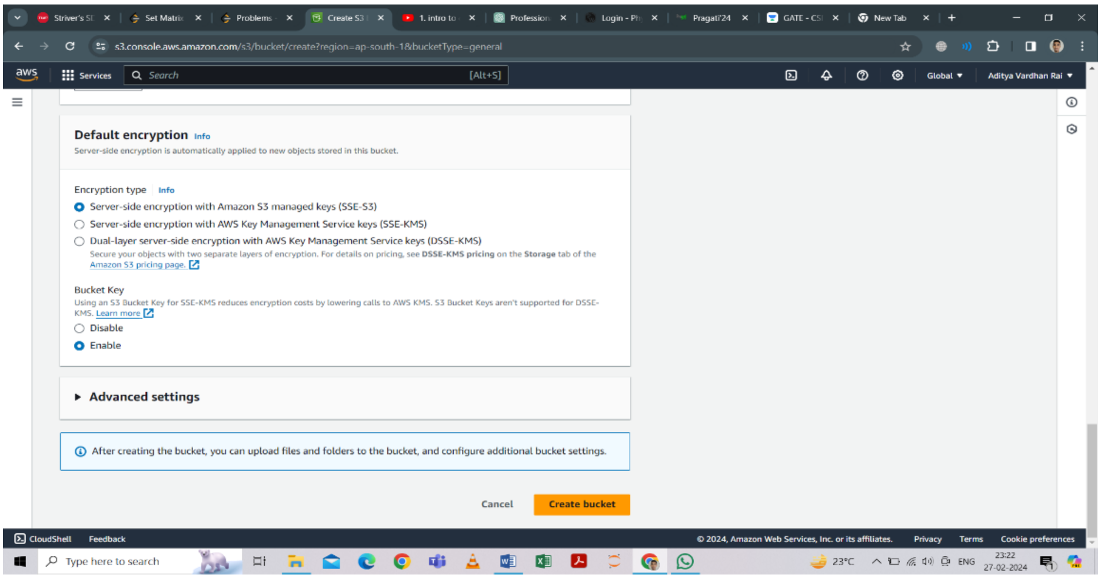
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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.



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

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

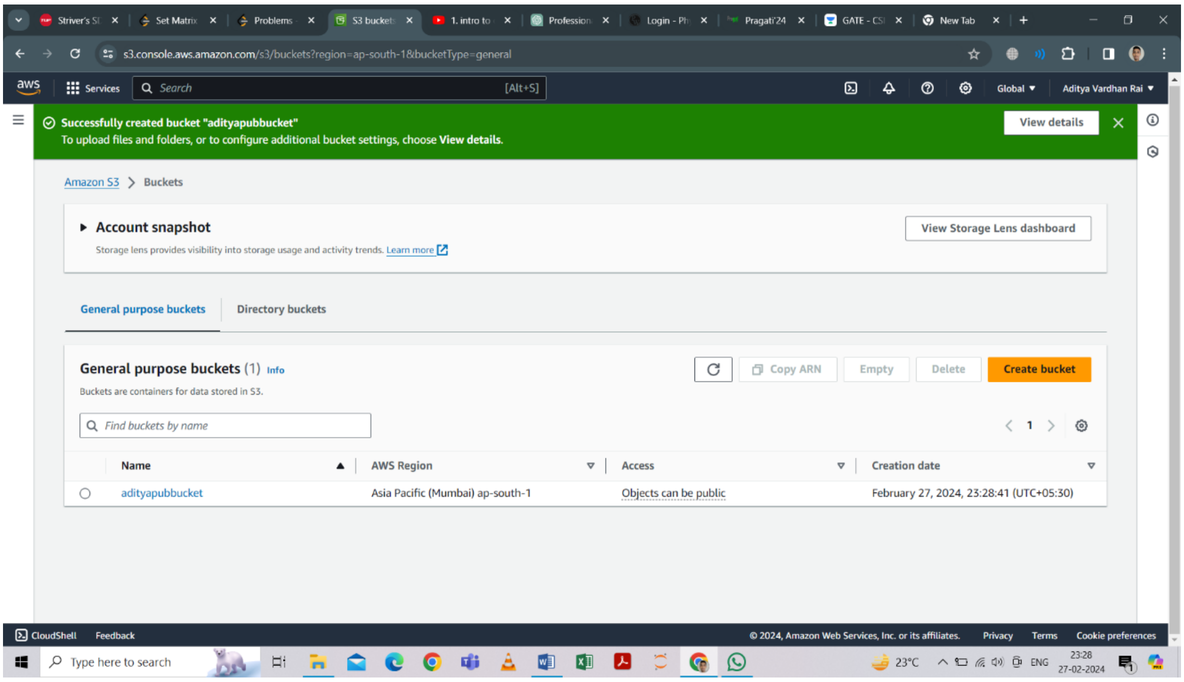
○ Disable
● Enable

▸ Advanced settings

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

Cancel | Create bucket

4. The bucket is created successfully. Click on the bucket name.



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

Successfully created bucket "adityapubbucket"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

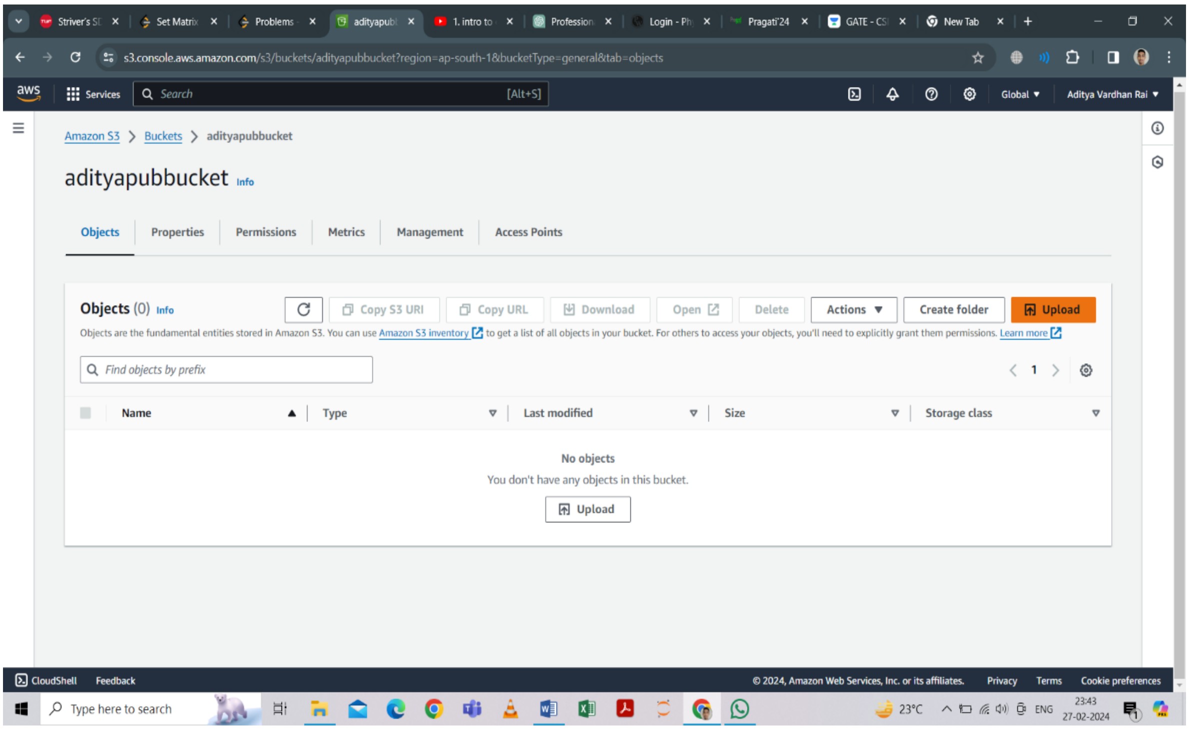
General purpose buckets (1) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Access	Creation date
○ adityapubbucket	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 27, 2024, 23:28:41 (UTC+05:30)

© 2024, Amazon Web Services, Inc. or its affiliates.

5. Click on 'Upload' then choose the three html files and upload those.



s3.console.aws.amazon.com/s3/buckets/adityapubbucket?region=ap-south-1&bucketType=general&tab=objects

Amazon S3 > Buckets > adityapubbucket

adityapubbucket Info

Objects (0) Info

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

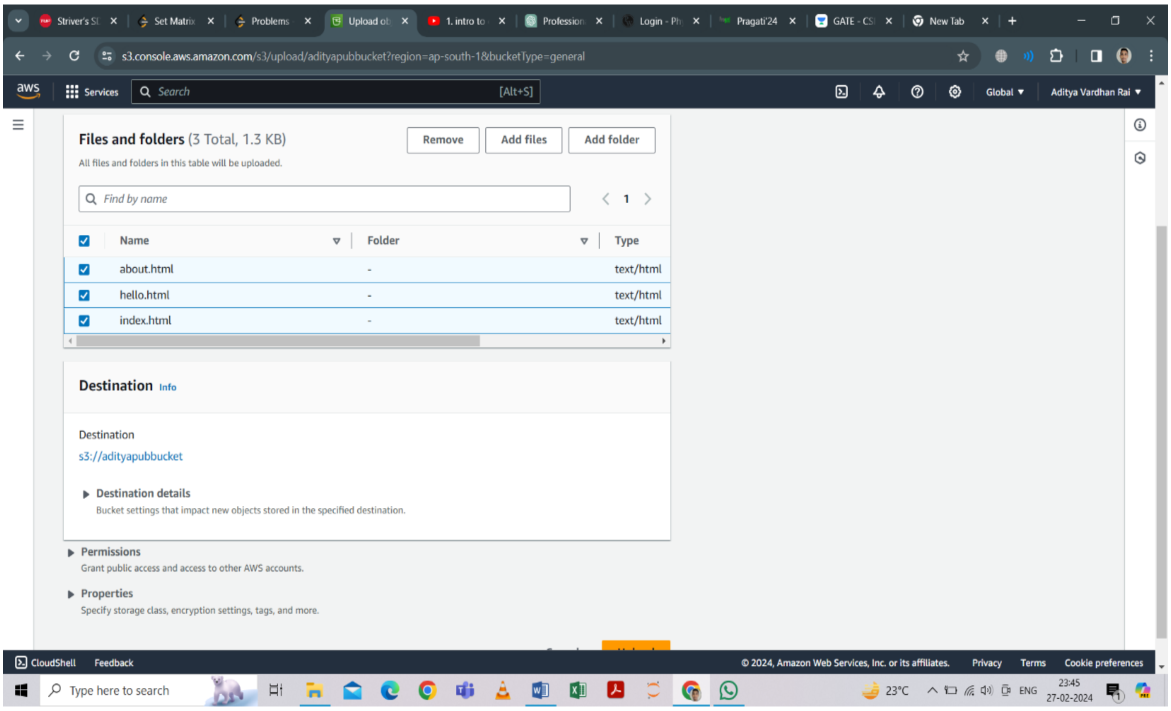
Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

© 2024, Amazon Web Services, Inc. or its affiliates.

6. Click on ‘Add files’ and add the three html files.



Files and folders (3 Total, 1.3 KB)

All files and folders in this table will be uploaded.

☑	Name	Folder	Type
☑	about.html	-	text/html
☑	hello.html	-	text/html
☑	index.html	-	text/html

Destination Info

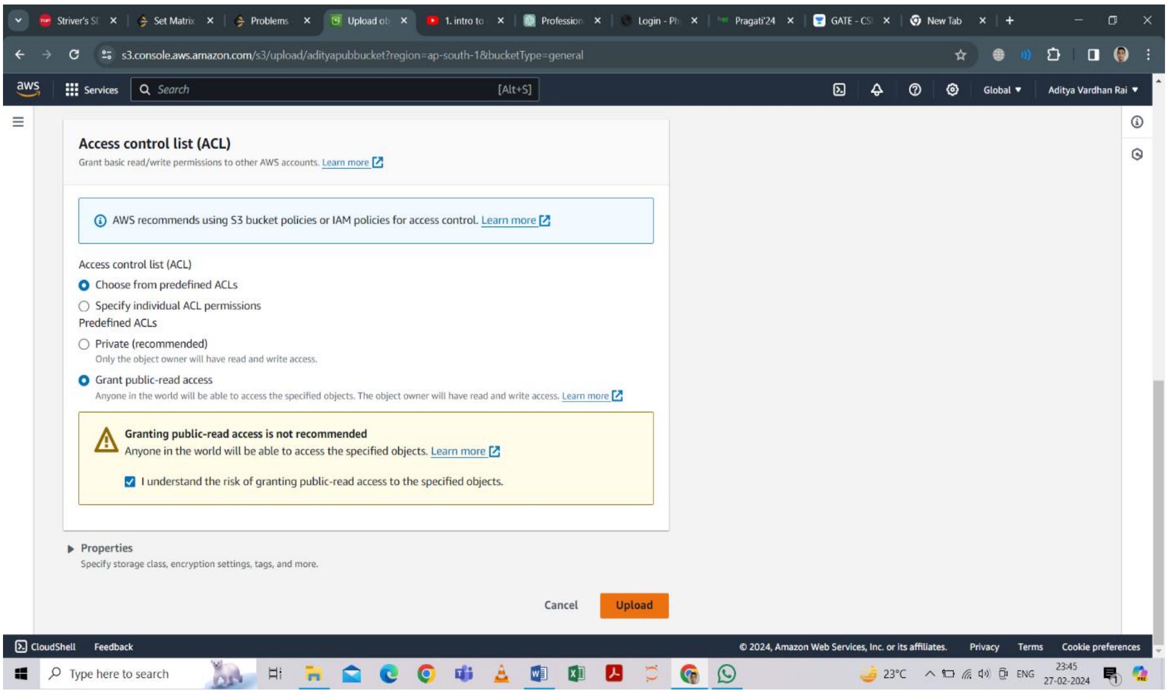
Destination
s3://adityapubbucket

▸ 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.

7. After selecting all these files go to ‘Permissions’. Do as shown. Then Upload.



Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

AWS recommends using S3 bucket policies or IAM policies for access control. Learn more

Access control list (ACL)
● Choose from predefined ACLs
○ Specify individual ACL permissions

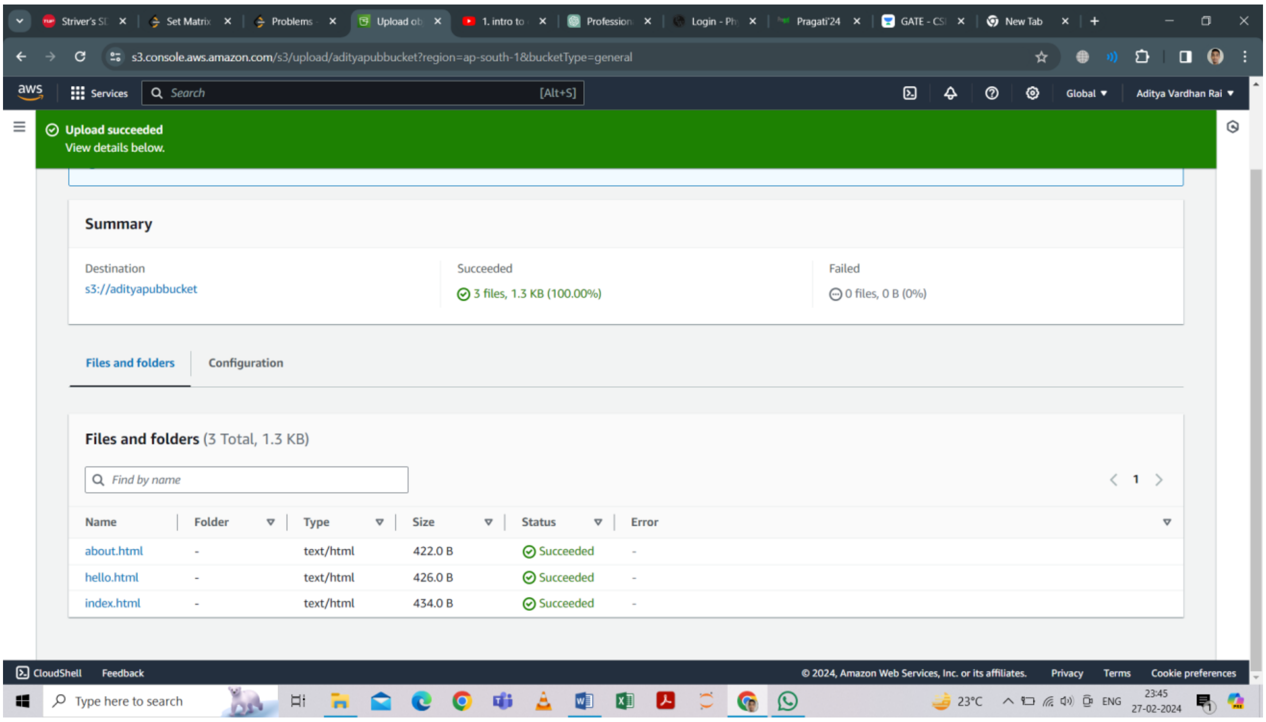
Predefined ACLs
○ Private (recommended)
Only the object owner will have read and write access.
● Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. Learn more

Granting public-read access is not recommended
Anyone in the world will be able to access the specified objects. Learn more

☑ I understand the risk of granting public-read access to the specified objects.

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

8. Successfully uploaded.



s3.console.aws.amazon.com/s3/upload/adityapubbucket?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Global
Aditya Vardhan Rai
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Upload succeeded
View details below.

Summary

Destination	Succeeded	Failed
s3://adityapubbucket	✓ 3 files, 1.3 KB (100.00%)	0 files, 0 B (0%)

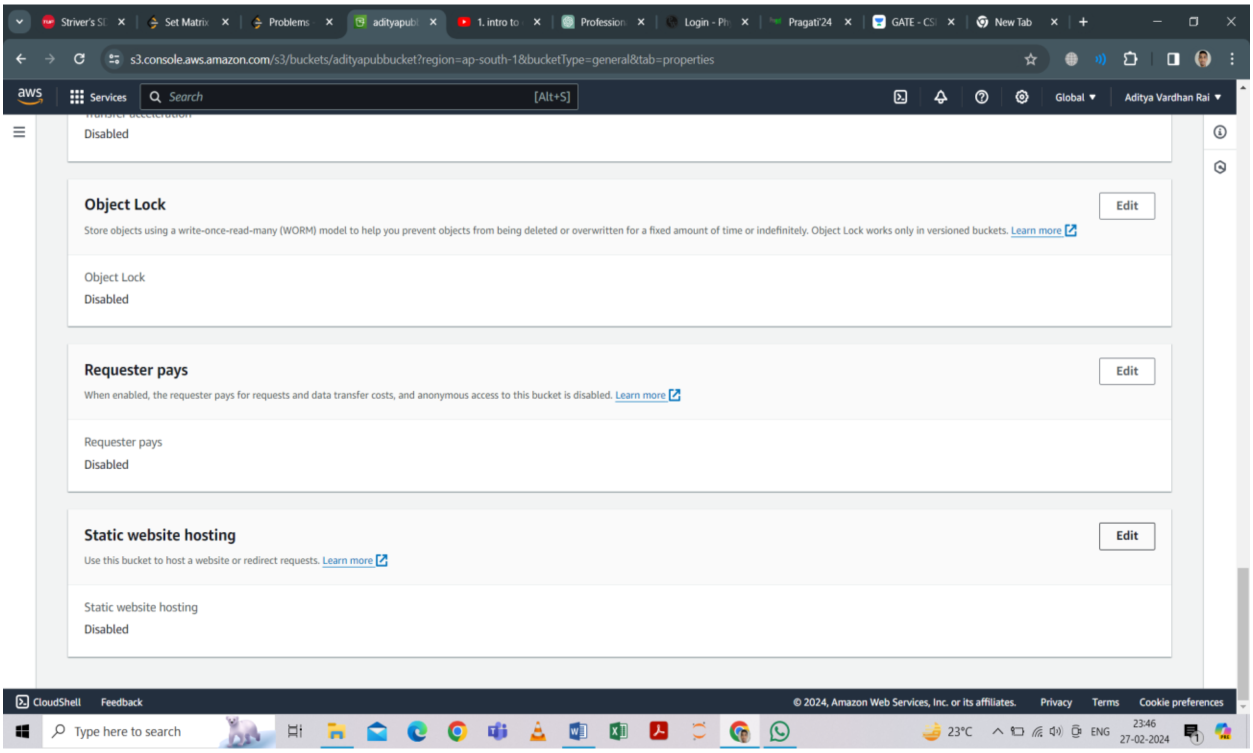
Files and folders | Configuration

Files and folders (3 Total, 1.3 KB)

Find by name

Name	Folder	Type	Size	Status	Error
about.html	-	text/html	422.0 B	✓ Succeeded	-
hello.html	-	text/html	426.0 B	✓ Succeeded	-
index.html	-	text/html	434.0 B	✓ Succeeded	-

9. Viewing the bucket, go to properties and select Static website hosting.



s3.console.aws.amazon.com/s3/buckets/adityapubbucket?region=ap-south-1&bucketType=general&tab=properties
Services
Search
[Alt+S]
Global
Aditya Vardhan Rai
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Disabled

Object Lock Edit

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

Object Lock
Disabled

Requester pays Edit

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

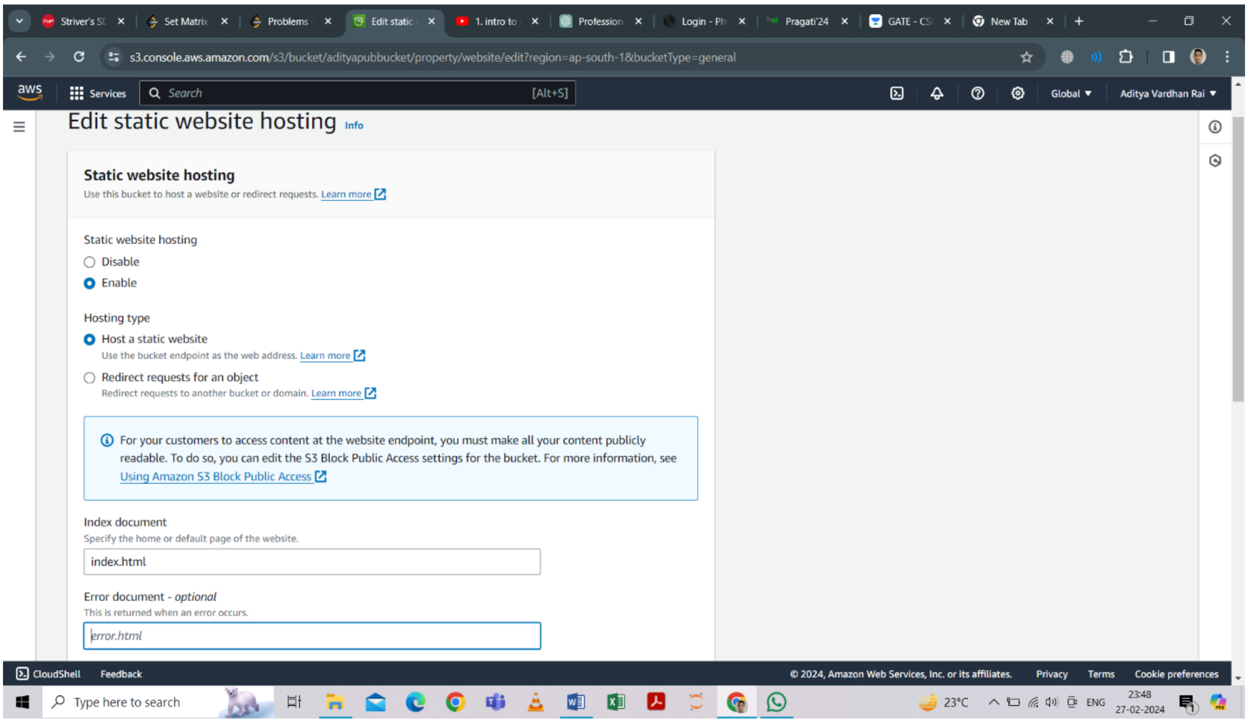
Requester pays
Disabled

Static website hosting Edit

Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Disabled

10. Under ‘Static website hosting’, click on ‘Enable’, then fill in the name of index document and click on ‘Save changes’.



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.

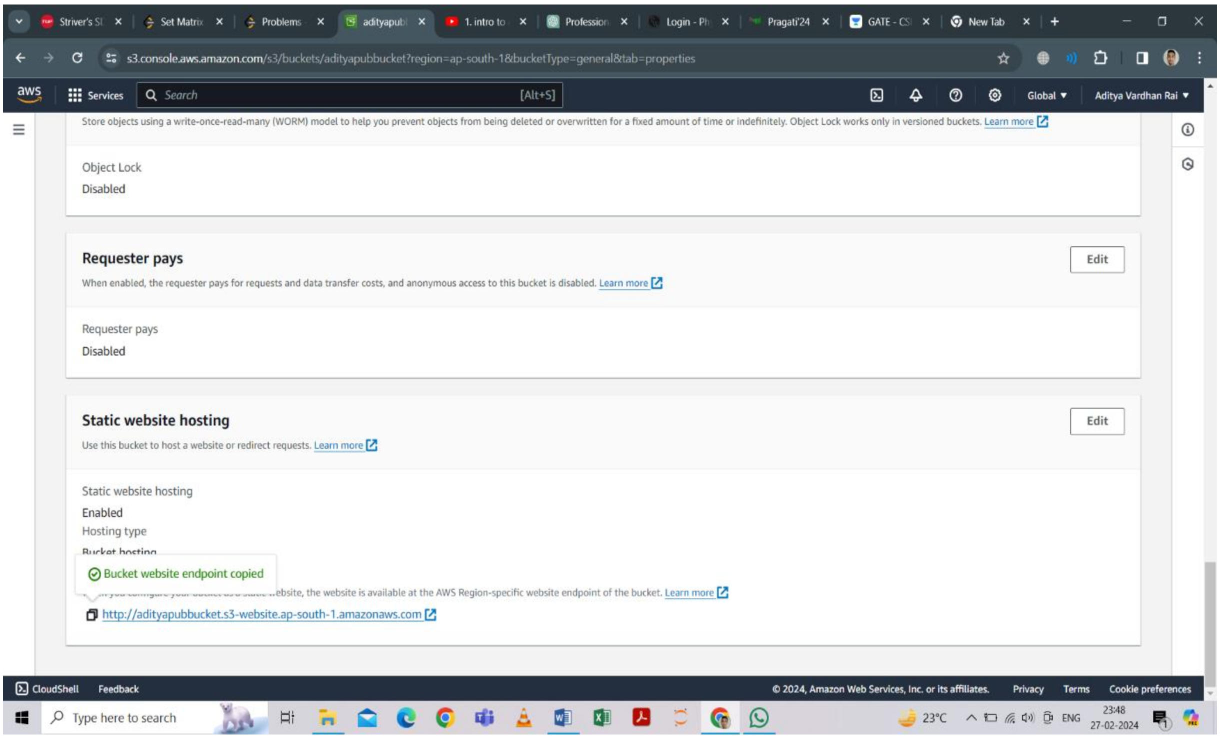
index.html

Error document - *optional*

This is returned when an error occurs.

error.html

11.The ‘Static website hosting’ is successfully edited. Now under ‘Staticwebsite hosting’, copy the ‘Bucket website endpoint’.



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

Object Lock

Disabled

Requester pays

Edit

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

Requester pays

Disabled

Static website hosting

Edit

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

Enabled

Hosting type

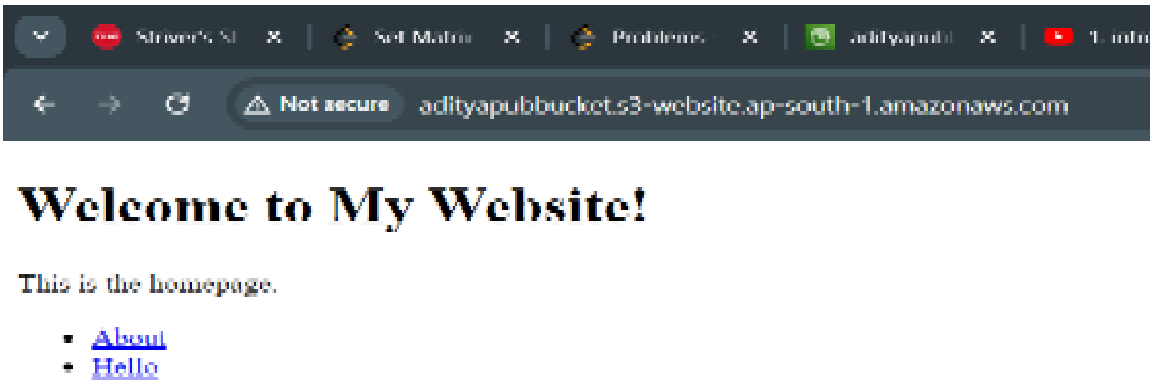
Bucket hosting

Bucket website endpoint copied

website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more

http://adityapubbucket.s3-website.ap-south-1.amazonaws.com

12.Open a new browser and paste the ‘Bucket website endpoint’ on the address bar. The results are as expected.

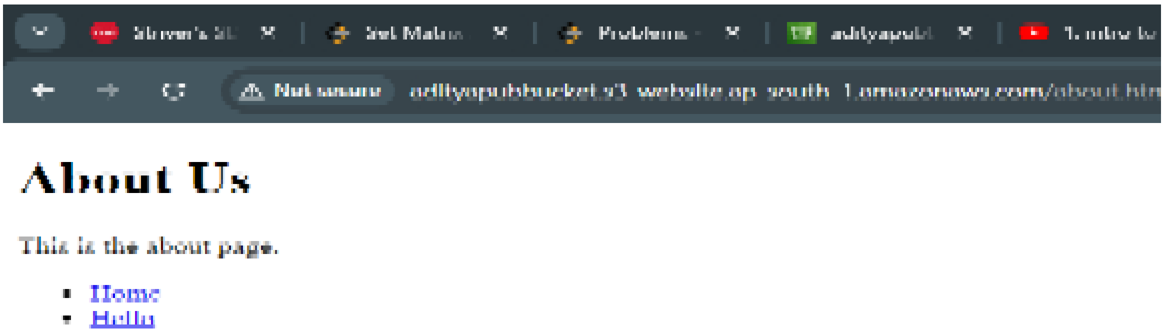


adityapubbucket.s3-website.ap-south-1.amazonaws.com

Welcome to My Website!

This is the homepage.

- About
- Hello

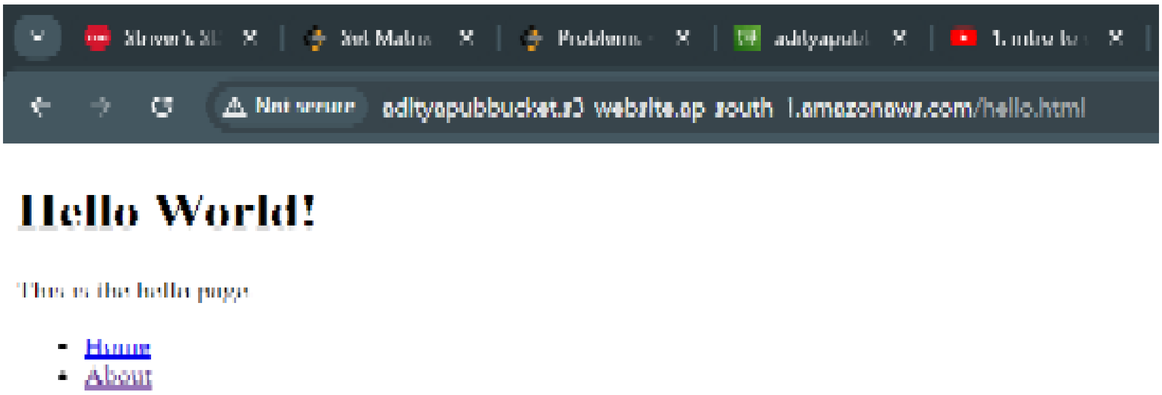


adityapubbucket.s3-website.ap-south-1.amazonaws.com/about.htm

About Us

This is the about page.

- Home
- Hello



adityapubbucket.s3-website.ap-south-1.amazonaws.com/hello.html

Hello World!

This is the hello page

- Home
- About