

**Computer Engineering Department**  
Program: Sem VI  
**Course: Cloud Computing Lab(CSL605)**  
**PART A**  
**(PART A: TO BE COMPLETED BY STUDENTS)**  
**Experiment No.5**

**A.1 Aim:**

**To demonstrate and implement Storage as a service using AWS S3 Service**

**A.2 Prerequisite:**

Knowledge of Networking, Distributed Computing and knowledge of Software architectures.

**A.3 Objective:**

Objectives this experiment is to provide students overview of AWS storages, its Features and Services.

**A.4 Outcome: (LO3)**

After successful completion of this experiment student will be able to; Implement IAAS deployment model of cloud.

**A.5 Theory:**



**Amazon Elastic Block storage (EBS):** Storage in the form of blocks, each of these blocks associated with one particular instance, so when to access this block make sure that you have an instant connected to it and storage is accessed through that instant only.

**Amazon Elastic File System (EFS):** It is shared file system; hence it is not attached to a particular system or operating system.

**Amazon S3 Glacier:** Need to store archive data, certain data that we would not want to retrieve or access on daily basis or frequently, such data you can put on **S3 Glacier**. That is it locks data for certain time during which you cannot access it, once you clear that duration you are free to access that data.

This storage is very cheap as compared to other data storage.

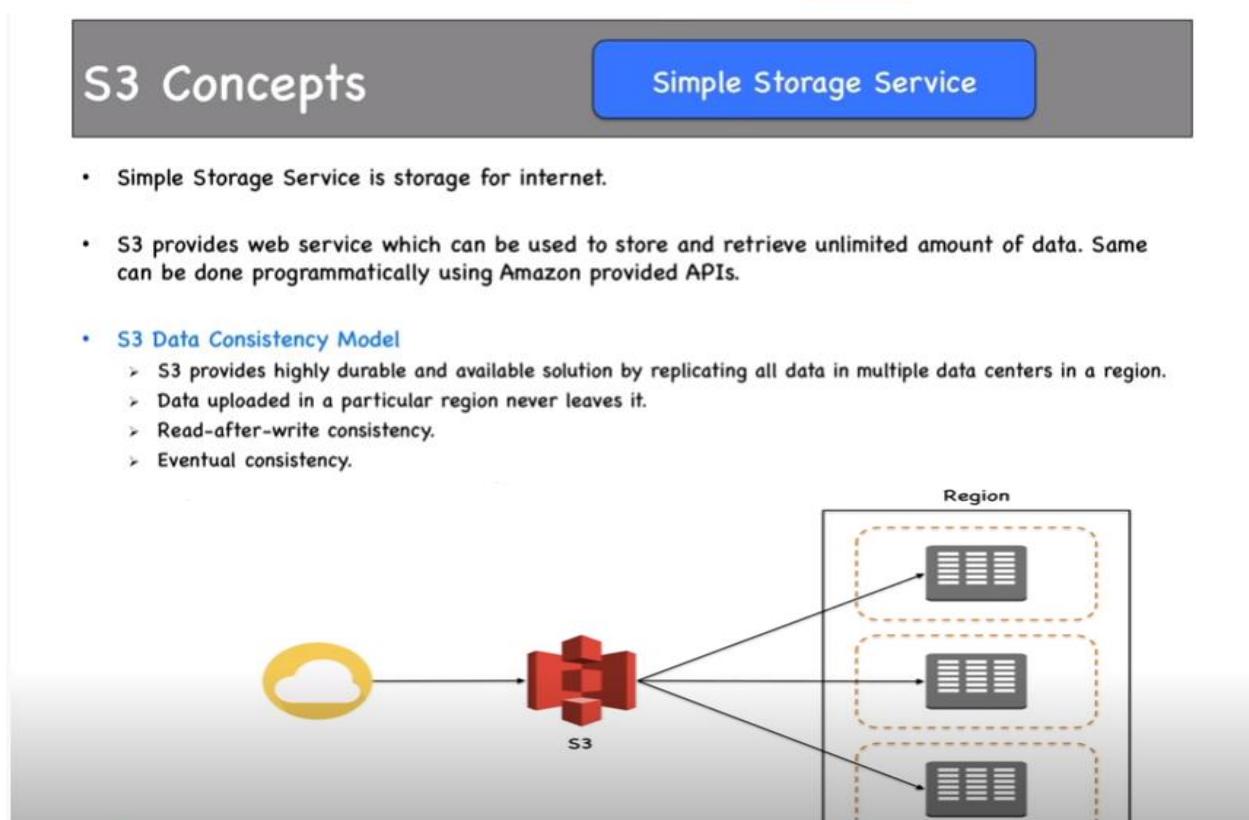
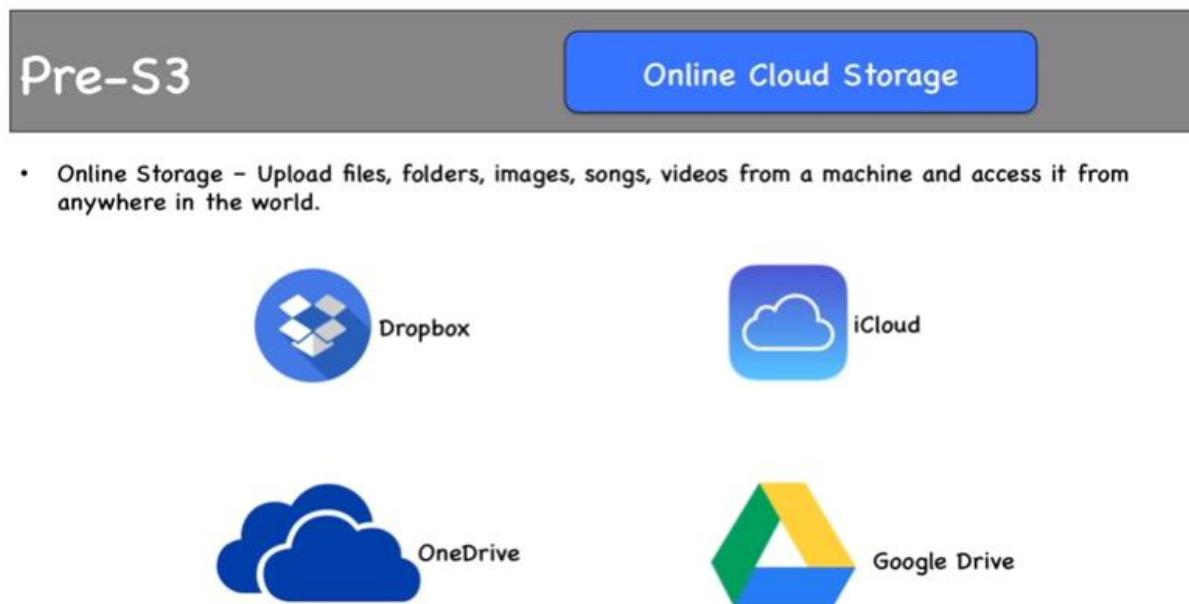
Example: Hospital System (birth certificate data): Birth certificate given by hospital once

baby takes birth, so once you get it you are not requesting it again and again and hospital need to maintain it. That is data which is important but not needed on daily basis.

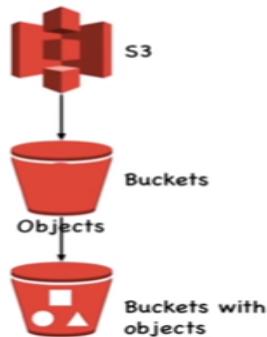
AWS Storage Gateway: Act as middle ware to move data from one system to another system.

### ⊕ What is Amazon S3 (Simple Storage Service)

- 1) Amazon s3 has a simple web service interface that you can use to store and retrieve any amount of data, at anytime from anywhere on the web.
- 2) **S3 works on objects and buckets** (Bucket is an container and an object (doc, image, file etc) is an file, which you can stored in container)
- 3) Online cloud storage



- S3 follows a storage hierarchy in keeping data (documents, images, videos, files etc.).



- Management console or S3 APIs can be used to manage buckets and objects.
- Bucket names have to be Globally unique irrespective of which region they are created in.
- Max 100 buckets can be created per account.

Amazon S3 (Simple Storage Service) provides object storage which is built for storing and recovering any amount of information or data from anywhere over the internet



4)

- ✓ Amazon S3 provides storage through web services interface
- ✓ It is designed for developers where web-scale computing can be easier for them
- ✓ It provides 99.999999999% durability and 99.99% availability of objects
- ✓ It can store computer files up to 5 terabytes in size

5)

## Object & Bucket in Amazon S3

An object consists of data, key(assigned name) and metadata

A bucket stores objects

When data is added to the bucket, Amazon S3 creates a unique version ID and allocates it to the object

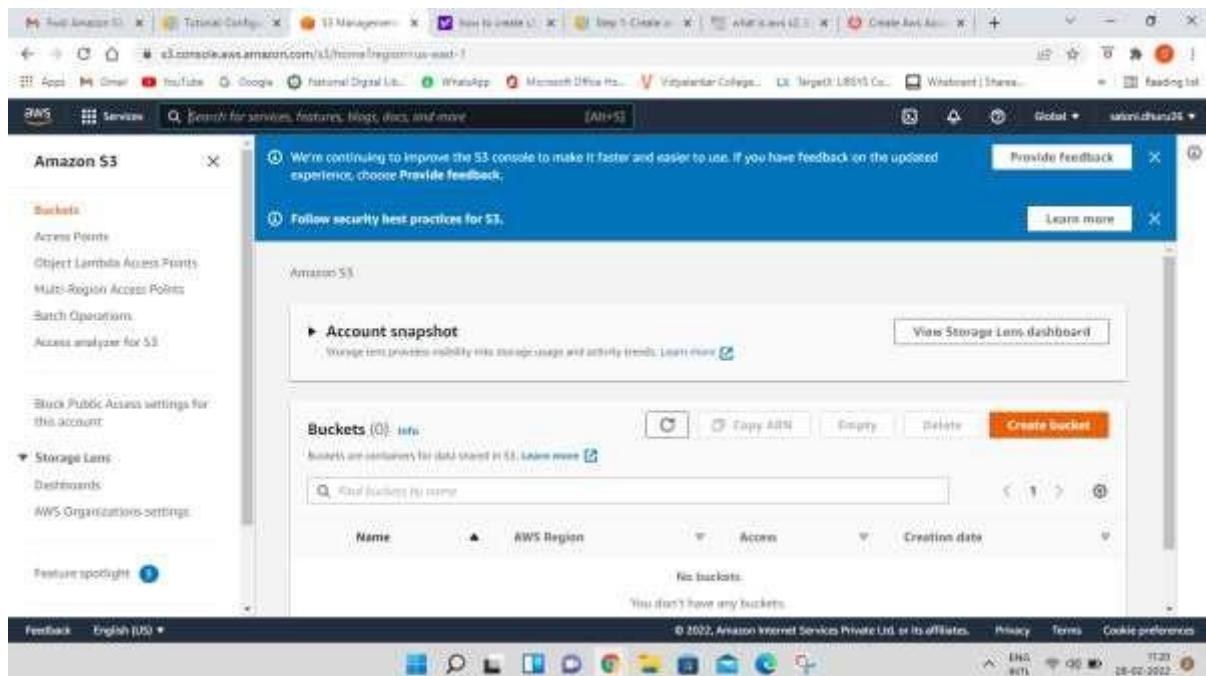
For Example:



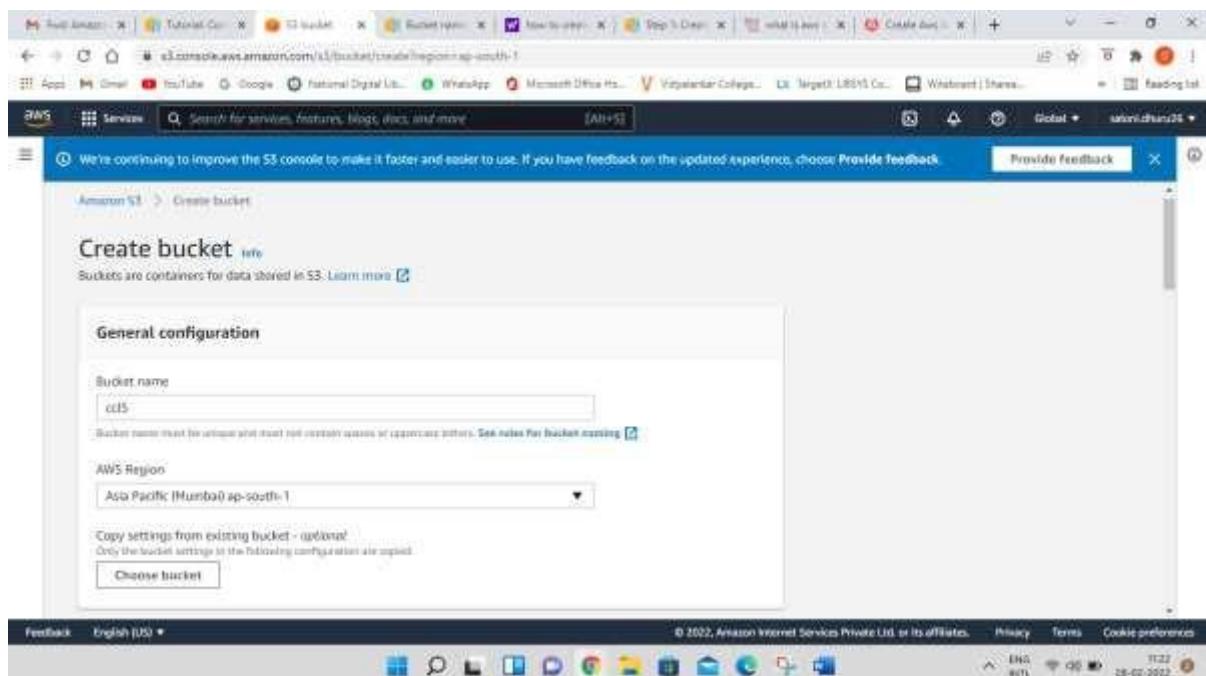
Object: folder/Penguins.jpg → Key(name)  
 Bucket: simplilearn → Version ID  
 Link Address: <https://s3.amazonaws.com/simplilearn/folder/Penguins.jpg>

## Steps to Implement Storage as a Service using Own Cloud/ AWS, Glaciers

### Step-1: click on create bucket



### Step-2: Give Bucket name & select region for storage



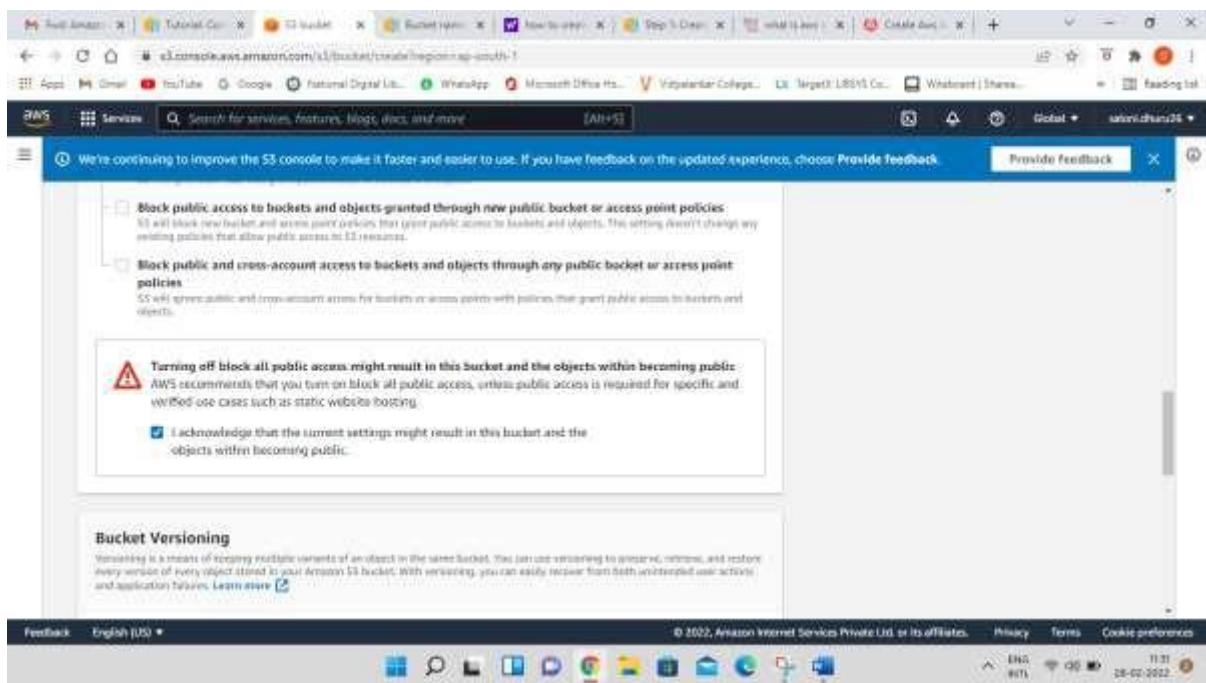
### Step-3: Keep object ownership setting as ACLs Disabled as by-default

The screenshot shows the 'Object Ownership' section of the AWS S3 Bucket Properties page. It includes two options: 'ACLs disabled (recommended)' and 'ACLs enabled'. The 'Object Ownership' dropdown below is set to 'Bucket owner enforced'. A note at the bottom states: 'Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or ad. In order to ensure that public access to this bucket and its contents is blocked, turn on Block all public access. These settings apply only to this bucket and its objects present. 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.' A checkbox for 'Block all public access' is checked.

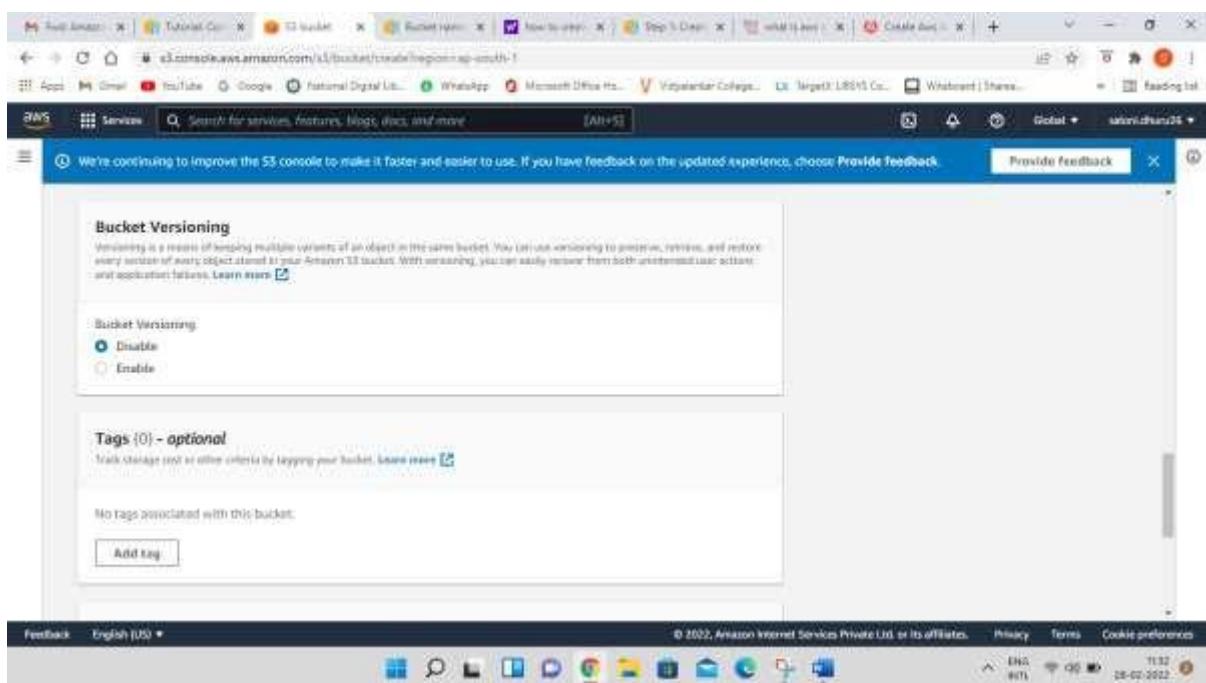
#### Step-4: Disable block all public access checkbox

The screenshot shows the 'Block Public Access settings for this bucket' section of the AWS S3 Bucket Properties page. It lists four checkboxes: 'Block all public access', '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)', and 'Block public access to buckets and objects granted through new public bucket or access point policies'. The 'Block all public access' checkbox is unchecked. A note at the bottom states: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' A note also states: 'This 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 using ACLs.'

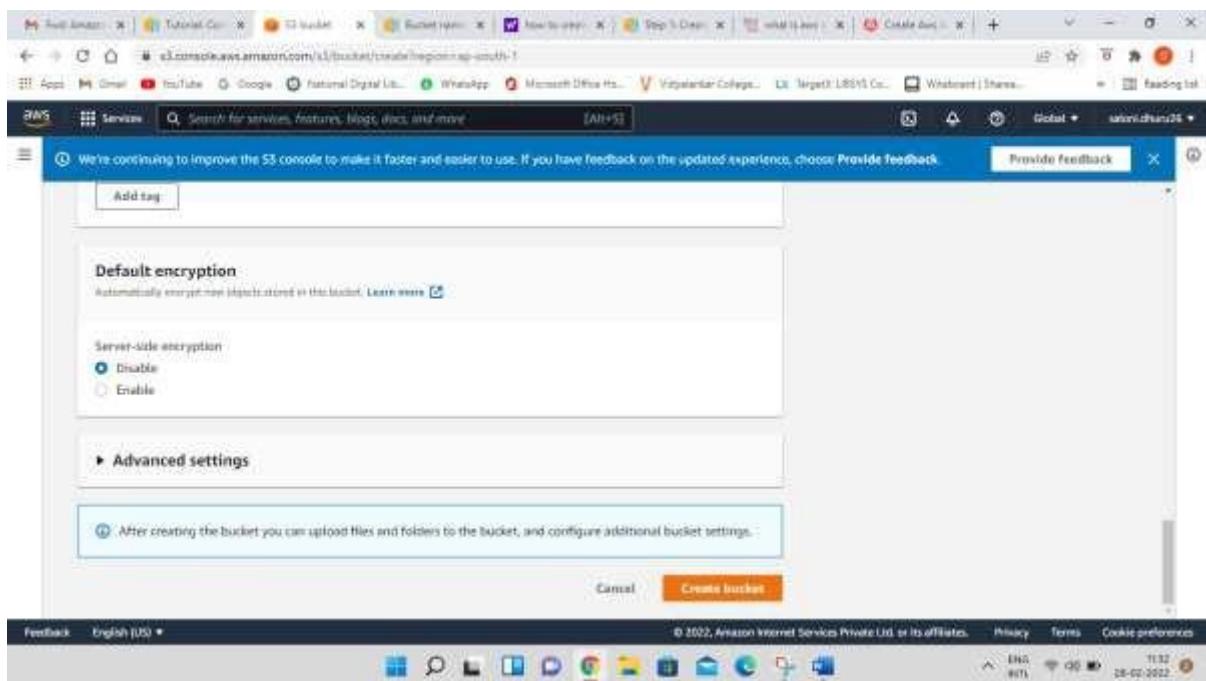
#### Step-5: Select the checkbox for Turning off block all public access might result in this bucket and the objects within becoming public



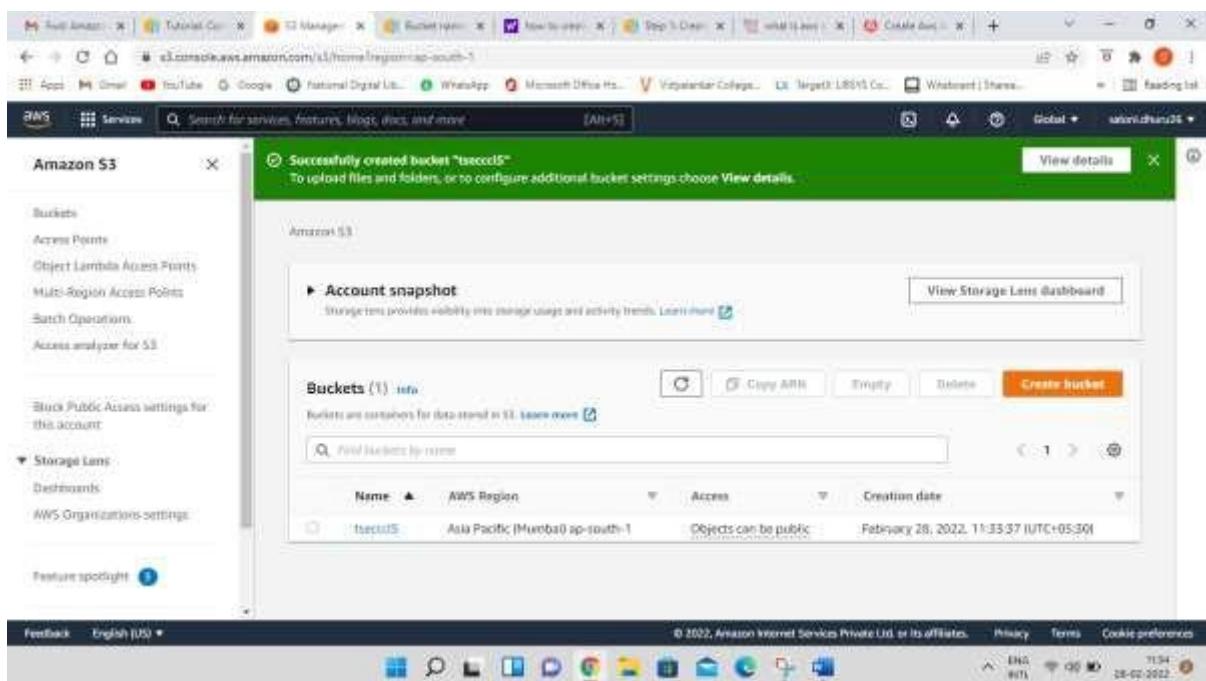
Step-6: Keep bucket versioning as disabled and add tags if required.



Step-7: Keep default encryption disabled and click on create bucket button



You can now see the successful creation of your bucket



Step-8: now click on the bucket that you have created

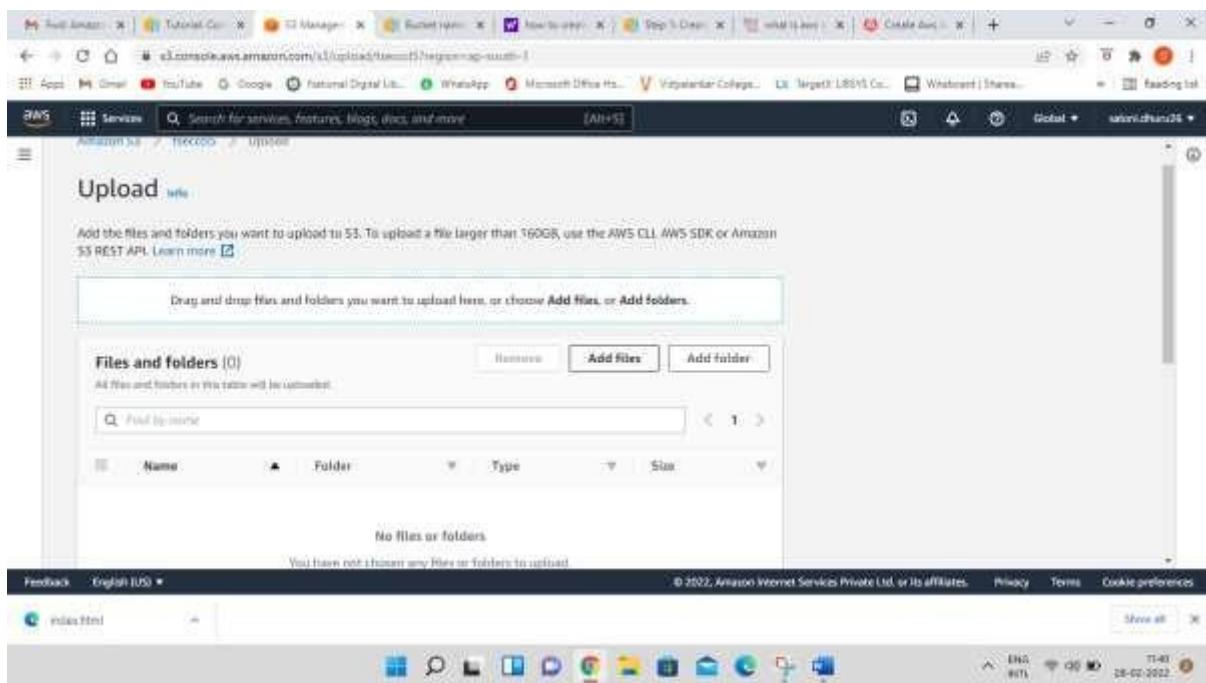
The screenshot shows the AWS S3 console with the 'Buckets' list. A red circle highlights the 'Django' bucket entry in the list.

Name	AWS Region	Access	Creation date
Django	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 28, 2022, 11:33:37 (UTC+05:30)

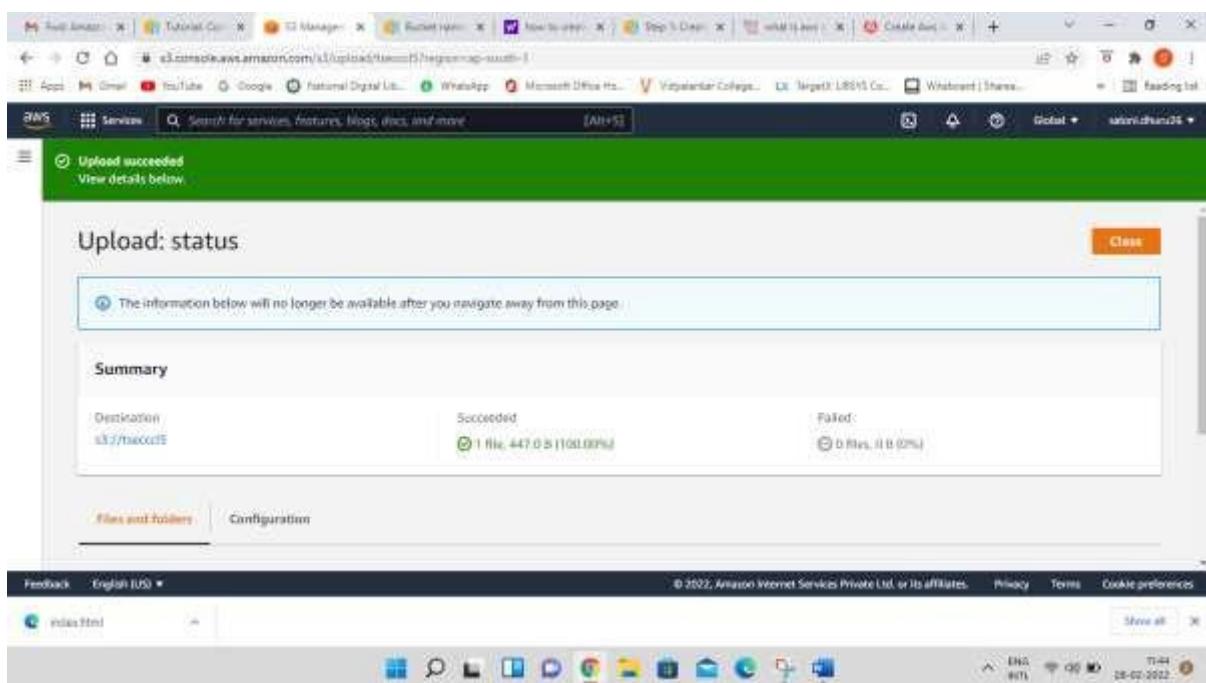
Step-9: You can either create a folder here or upload an existing file in the bucket

The screenshot shows the AWS S3 console with the 'Objects' tab selected. A red circle highlights the 'Upload' button.

Step-10: now click on upload button and click on add files button browse your local machine and select which file you need to upload on S3 next click on upload button at bottom right end



Now you can check the upload status screen



Now click on close button

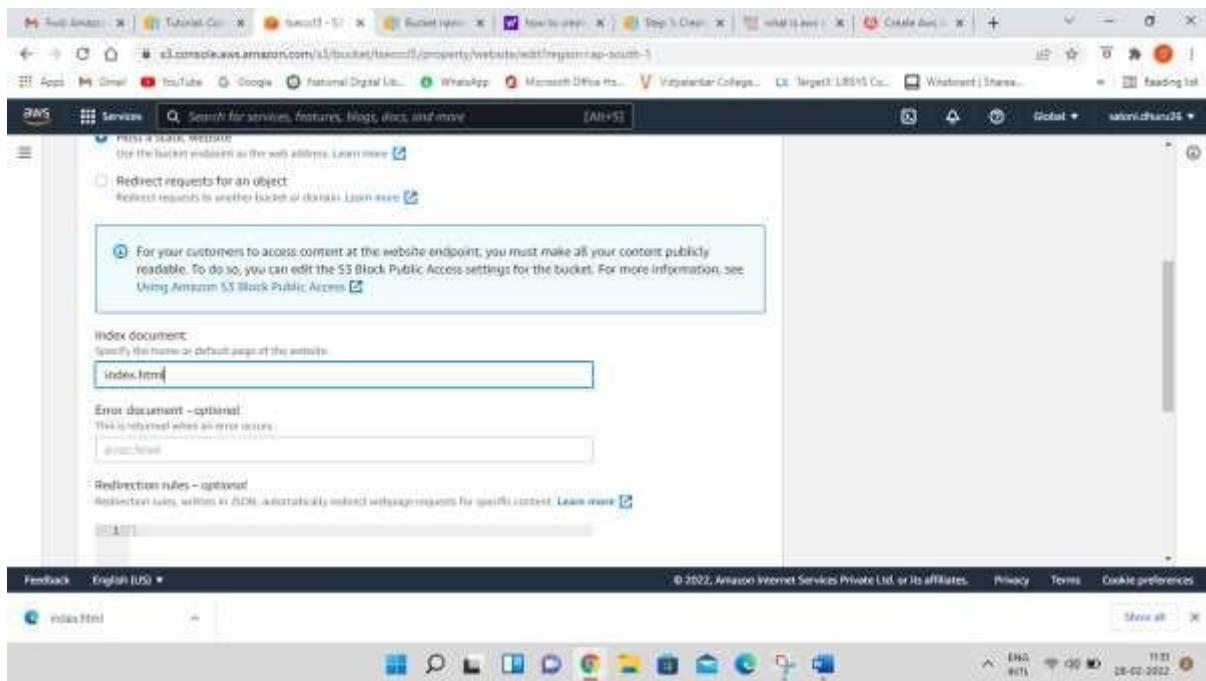
The screen will appear as below

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with various tabs and links. Below it, the main content area has a header 'Amazon S3 > tsecccl5'. Underneath is a sub-header 'tsecccl5.info'. A horizontal menu bar with tabs 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points' follows. The main content area is titled 'Objects (1)'. It contains a table with one row for 'index.html'. The table columns are 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. The 'Name' column shows 'index.html', 'Type' shows 'html', 'Last modified' shows 'February 28, 2022, 11:48:51 (UTC+05:30)', 'Size' shows '447.0 B', and 'Storage class' shows 'Standard'. Below the table is a toolbar with buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A search bar labeled 'Find objects by prefix' is also present. At the bottom of the page, there's a footer with links for 'Feedback', 'English (US)', and copyright information.

Step-11: Select properties and scroll down to **Static website hosting** option which is disabled now click on Edit option on right side

This screenshot shows the 'Properties' page for the 'tsecccl5' bucket in the AWS S3 console. At the top, there's a message: 'Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact Customer Support.' Below this, there are two main sections: 'Requester pays' and 'Static website hosting'. The 'Requester pays' section is set to 'Disabled' and has an 'Edit' button. The 'Static website hosting' section is also set to 'Disabled' and has an 'Edit' button. At the bottom of the page, there's a footer with links for 'Feedback', 'English (US)', and copyright information.

Step-12: Enable the radio button and specify the file name in **Index document** which you have added in S3



## Edit static website hosting Info

### Static website hosting

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

#### Static website hosting

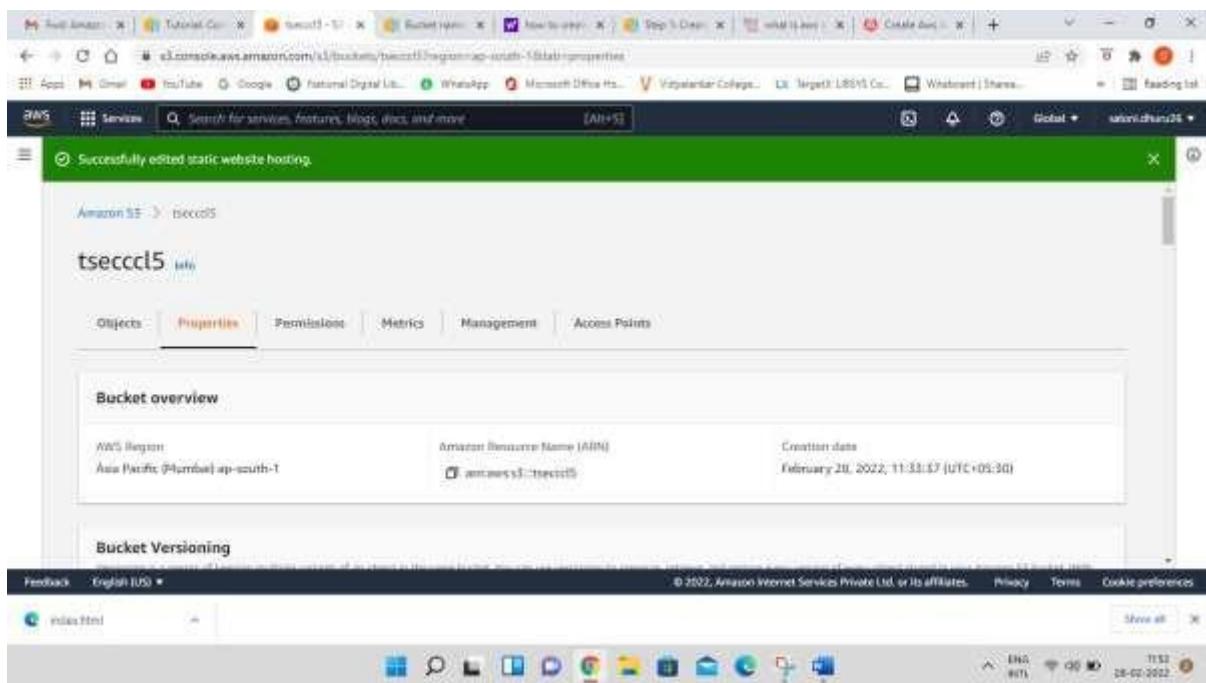
- Disable  
 Enable

#### Hosting type

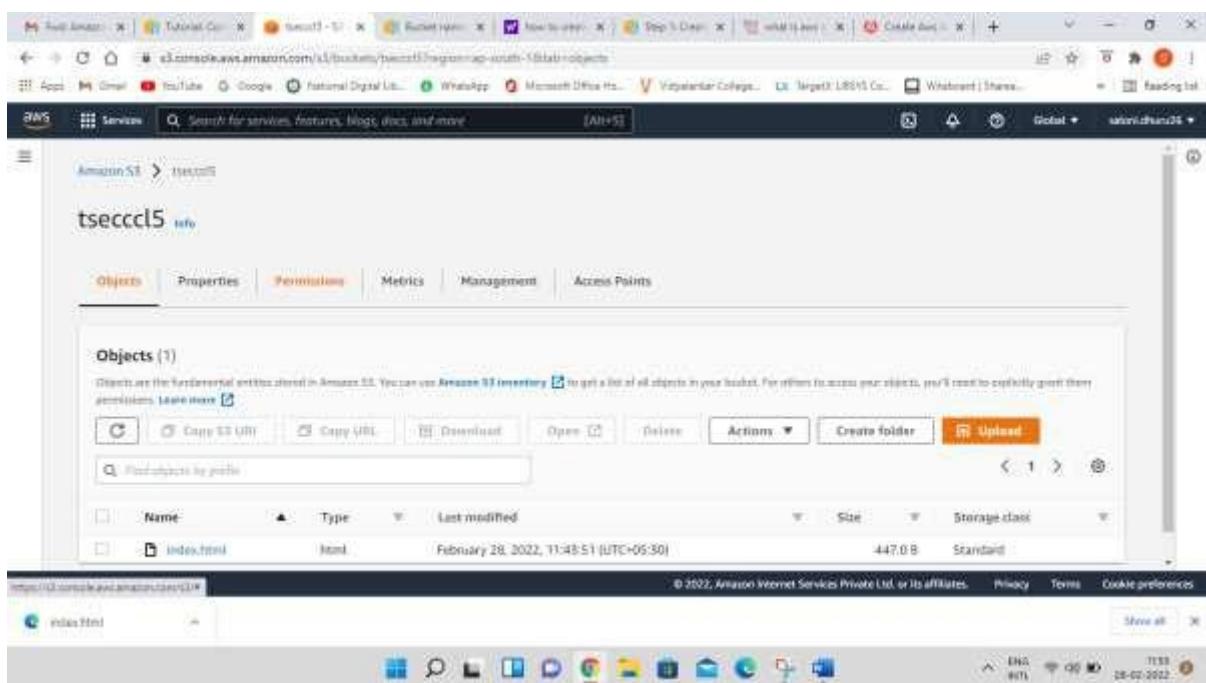
- Host a static website  
Use the bucket endpoint as the web address. [Learn more](#)  
 Redirect requests for an object  
Redirect requests to another bucket or domain. [Learn more](#)

Scroll down and save the changes at bottom right

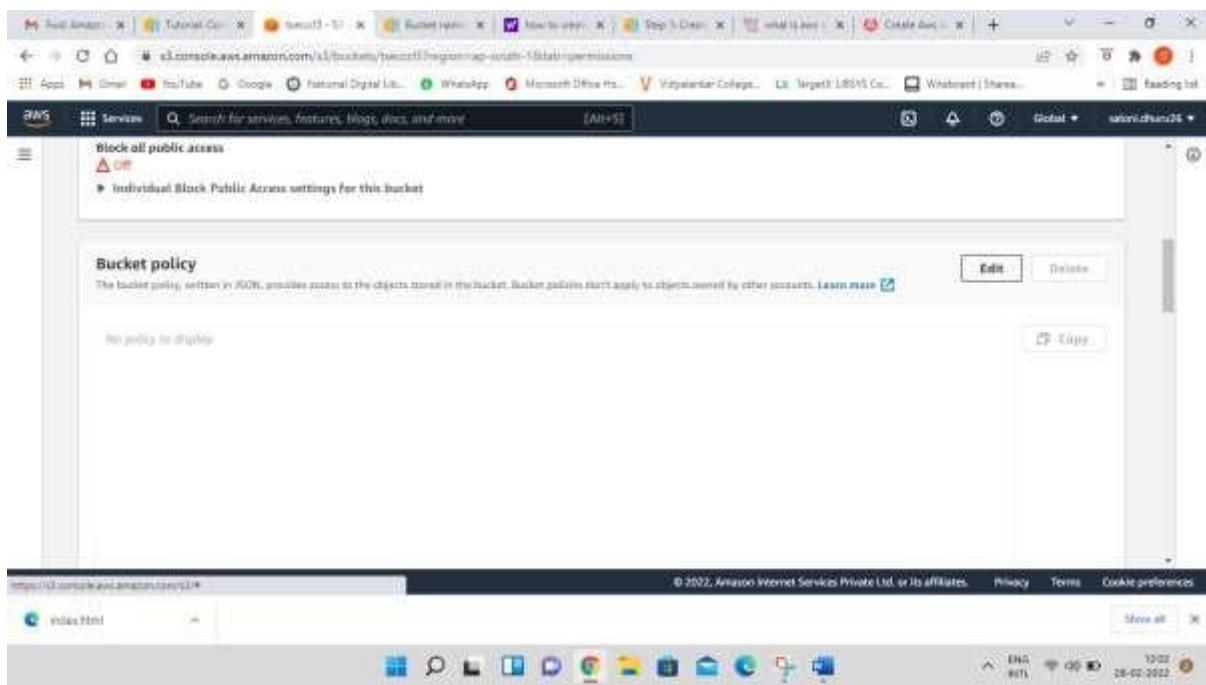
Following screen will appear



### Step-13: Click on Permissions Tab



### Step-14: In bucket policy click on Edit option

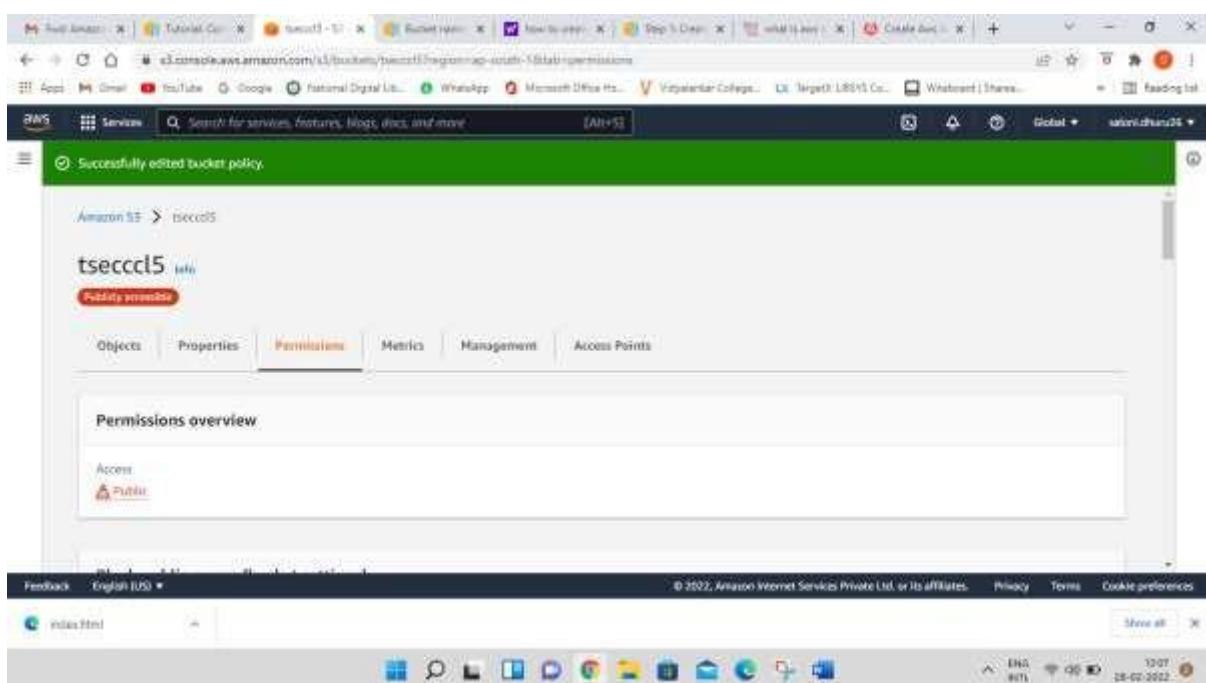
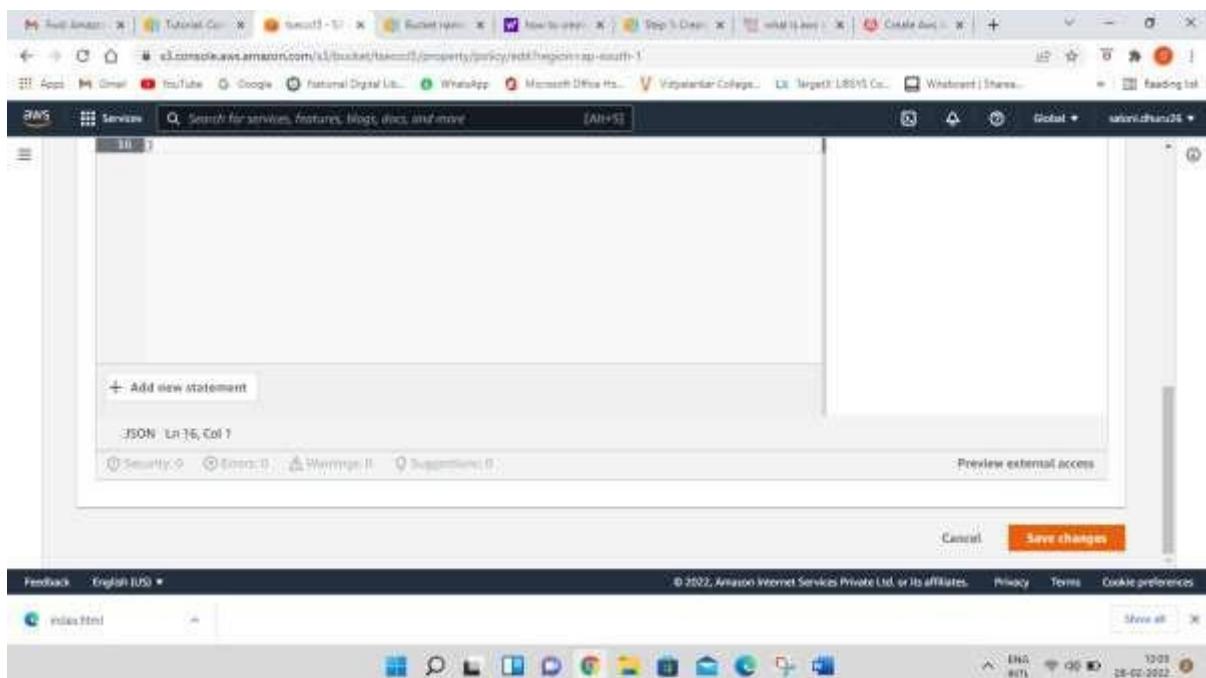


Step 15- after clicking on edit button paste the following code in bucket policy

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

Note-Make sure that you add your bucket name in the code above

Scroll down and click on Save Changes button



Step-16: open your html file and click on Object URL

The screenshot shows the AWS S3 console with the object 'index.html' selected. The 'Properties' tab is active. Key details shown include:

- Owner:** f91863fb664067b4878c512d4dc5096f303b6#0096d9e12bee7ed2fce085fa5e
- Region:** Asia Pacific (Mumbai) ap-south-1
- Last modified:** February 28, 2022, 11:43:51 (UTC+05:30)
- Size:** 447.0 B
- Type:** index.html

The object URL is displayed as <https://tsecccl5.s3.ap-south-1.amazonaws.com/index.html>.

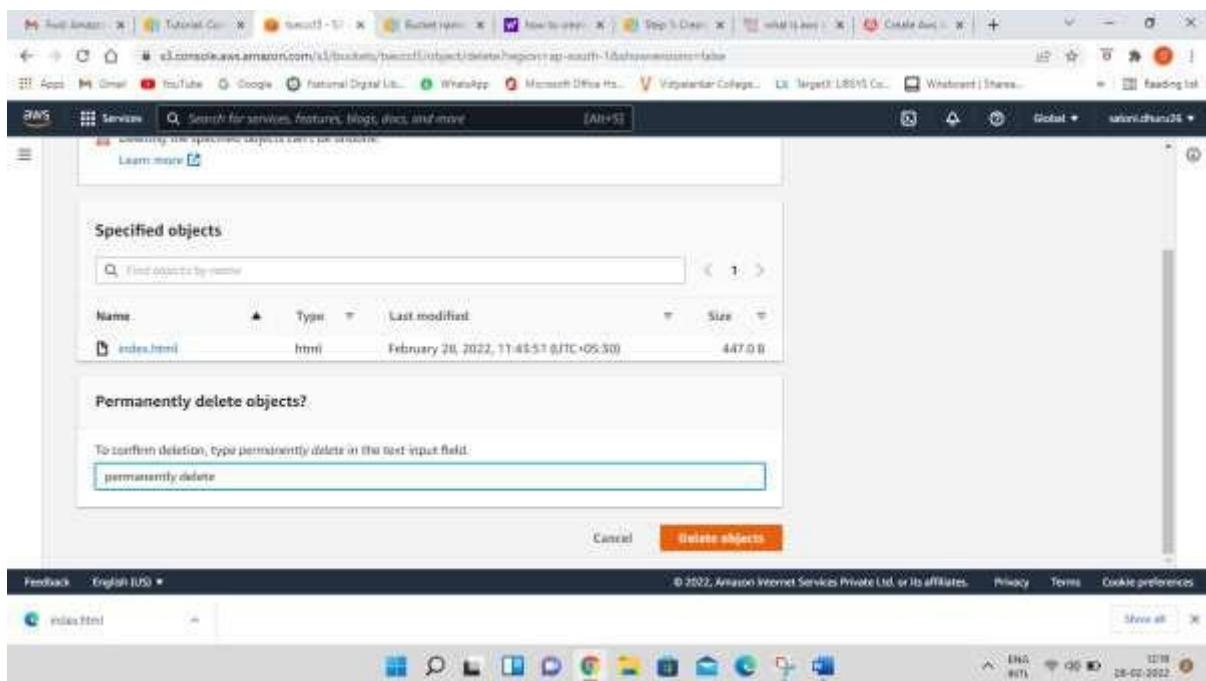
Step-17: Now for delete files click on checkbox of your file and then click on **Delete** Button

The screenshot shows the AWS S3 console with the 'Objects' list. Two files are selected for deletion:

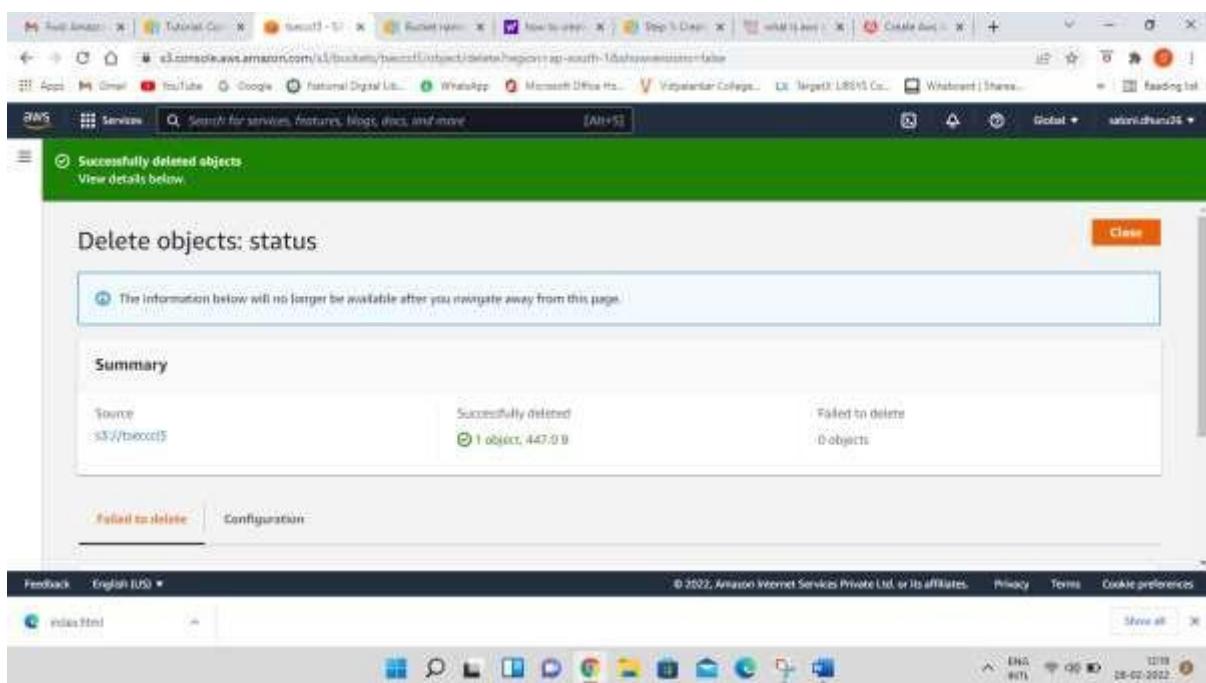
- Exp-1 Study of HIST Model of Cloud Computing.pptx
- index.html

The 'Delete' button is highlighted in orange at the top of the list.

Write permanently delete and click on delete object button



Now click on close button



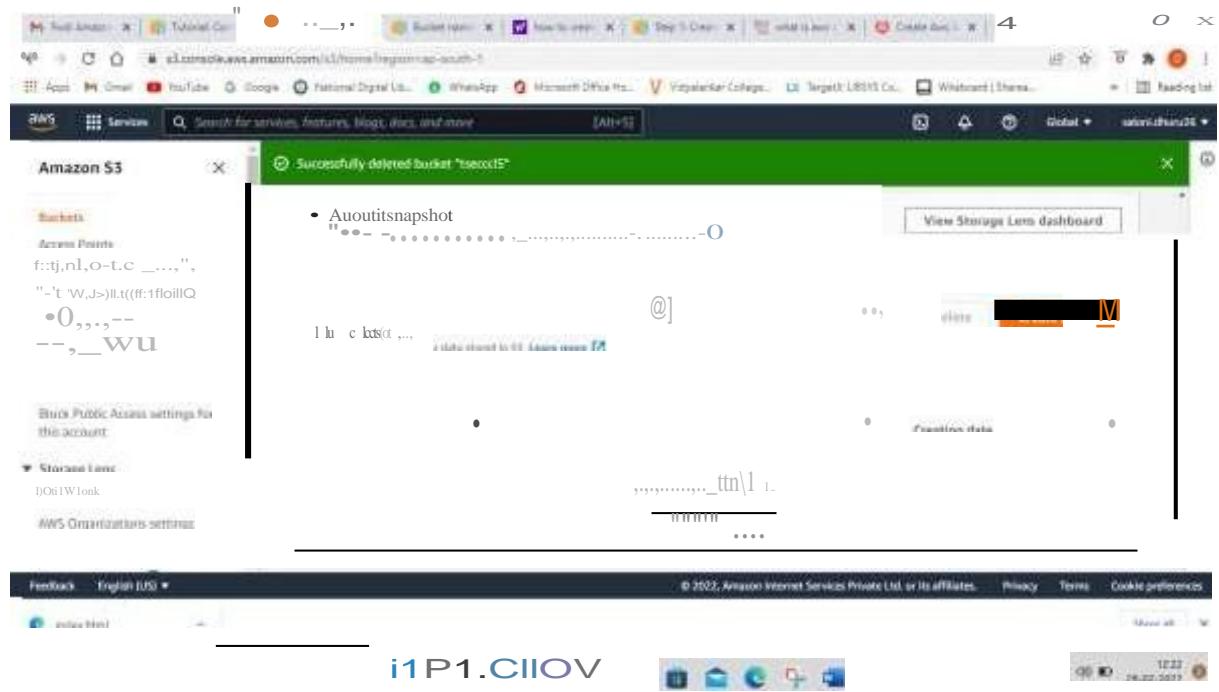
Step-18: now come to Amazon S3 tab and select your bucket and then click on delete button

The screenshot shows the AWS S3 console. On the left, there's a sidebar with options like Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and Access analyzer for S3. Under Storage Lens, it shows Dashboards and AWS Organizations settings. The main area is titled 'Amazon S3' and has a sub-header 'Read the S3 resources page for documentation and technical content.' It features an 'Account snapshot' section with a link to 'View Storage Lens dashboard'. Below that is a table titled 'Buckets (1) info'. The table has columns for Name, AWS Region, Access, and Creation date. One row is shown: 'tsecc15' (AWS Region: Asia Pacific (Mumbai) ap-south-1, Access: Public, Creation date: February 28, 2022, 11:33:37 (UTC+05:30)). At the bottom right of the table is a red 'Delete' button.

Write down your bucket name in delete bucket tab and click on delete button at bottom right

The screenshot shows the 'Delete bucket' confirmation dialog. It includes a warning message: '⚠ Deleting a bucket cannot be undone.' followed by three bullet points: 'Bucket names are unique. If you delete a bucket, another AWS user can use the name.', 'This bucket is configured to host a static website. We recommend that you clean up the Route 53 hosted zone settings that are related to the bucket.', and a 'Learn more' link. Below this is a section titled 'Delete bucket "tsecc15"?'. It contains a note 'To confirm deletion, enter the name of the bucket in the text input field.' with a text input field containing 'tsecc15'. At the bottom right of the dialog is a large red 'Delete' button.

You can see that the bucket is deleted



## PART B

### (PART B: TO BE COMPLETED BY STUDENTS)

**(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the ERP or emailed to the concerned lab in charge faculties at the end of the practical in case there is no ERP access available)**

Roll No.B48	Name: Aryan Unhale
Class :TE COMPS B	Batch :B3
Date of Experiment:27/2/25	Date of Submission:4/4/25
Grade :	

#### B.1 Question of Curiosity:

**Q.1: Create Bucket using AWS S3 service (Add stepwise screenshots of the same)**

Step-1: click on create bucket

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with options like 'General purpose buckets', 'Storage Lens', and 'AWS Marketplace'. The main area displays a table for 'General purpose buckets'. The table has columns for 'Name', 'AWS Region', 'IAM Access Analyzer', and 'Creation date'. One row is selected, showing the name 'elasticbeanstalk-ap-south-1-699475959073', the region 'Asia Pacific (Mumbai) ap-south-1', and the creation date 'February 26, 2025, 22:35:44 (UTC+05:30)'. At the top right of the table, there are buttons for 'Create bucket' (highlighted in orange), 'Copy ARN', 'Empty', and 'Delete'. Above the table, a message says 'Account snapshot - updated every 24 hours'.

Step-2: Give Bucket name & select region for storage

The screenshot shows the 'Create bucket' wizard. The first step, 'General configuration', is displayed. It includes a section for 'AWS Region' (set to 'Asia Pacific (Mumbai) ap-south-1') and 'Bucket type' (radio button selected for 'General purpose', with a note about it being suitable for most use cases). Below these are fields for 'Bucket name' (containing 'intazaeep5') and 'Format' (set to 's3://bucket/prefix'). There are also sections for 'Copy settings from existing bucket - optional' and a 'Choose bucket' button.

## Step-3: Keep object ownership setting as ACLs Disabled as by-default

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.

**Object Ownership**  
Bucket owner enforced

## Step-4: Disable block all public access checkbox

Step-5: Select the checkbox for Turning off block all public access might result in this bucket and the objects within becoming public

Step-6: Keep bucket versioning as disabled and add tags if required.

**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.

**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](#)

**Disable**

**Enable**

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

No tags associated with this bucket.

[Add tag](#)

## Step-7: Keep default encryption disabled and click on create bucket button

**Default encryption [Info](#)**  
Server-side encryption is automatically applied to new objects stored in this bucket.

**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-8: You can now see the successful creation of your bucket

Step-9: now click on the bucket that you have created

The screenshot shows the AWS S3 Buckets page. A green banner at the top indicates the successful creation of the bucket 'intazaexp5'. Below this, there's an 'Account snapshot' section and a table for 'General purpose buckets'. The table lists two buckets: 'elasticbeanstalk-ap-south-1-699475959073' and 'intazaexp5'. The 'intazaexp5' row shows its creation date as March 2, 2025, at 23:51:09 UTC+05:30.

## Q2: Add Objects to Bucket created (Add stepwise screenshots of the same)

Step-10: You can either create a folder here or upload an existing file in the bucket

The screenshot shows the 'Upload objects - S3 bucket intazaexp5' page. The 'Upload' tab is active. It features a large input field for dragging and dropping files. Below it, there's a table for 'Files and folders' which is currently empty. The 'Destination' section shows the URL 's3://intazaexp5/'. The 'Permissions' and 'Properties' sections are also present at the bottom.

Step-10: now click on upload button and click on add files button browse your local machine and select which file you need to upload on S3 next click on upload button at bottom right end

The screenshot shows the AWS S3 'Upload objects' interface. In the 'Files and folders' section, a single file named 'Name.html' is listed with a size of 907.0 B. Below the table are sections for 'Destination' (set to 's3://intazaexp5') and 'Permissions'. At the bottom right are 'Cancel' and 'Upload' buttons.

Step-11: Now you can check the upload status screen, Now click on close button.

The screenshot shows the 'Upload: status' page. It displays a summary table with one row: 'Succeeded' (1 file, 907.0 B (100.00%)) and 'Failed' (0 files, 0 B (0%)). Below this is a 'Files and folders' table showing the uploaded file 'Name.html' with a status of 'Succeeded'.

Step-12: Select properties and scroll down to Static website hosting option which is disabled now click on Edit option on right side

The screenshot shows the 'Properties' tab for the 'intazaexp5' bucket. Under the 'Bucket overview' section, there is a note about 'Bucket Versioning' stating it is disabled. The 'Edit' button next to this note is highlighted.

The screenshot shows the AWS S3 Bucket Properties page for the bucket 'intazaexp'. The top navigation bar includes the AWS logo, a search bar, and a 'Transfer acceleration' button. The main content area is divided into several sections:

- Transfer acceleration**: A section with a sub-link to learn more about accelerated endpoints.
- Object Lock**: A section with a sub-link to learn more about the WORM model. It shows 'Object Lock' is disabled.
- Requester pays**: A section with a sub-link to learn more about requester pays. It shows 'Requester pays' is disabled.
- Static website hosting**: A section with a sub-link to learn more about hosting websites. It shows 'S3 static website hosting' is disabled. A callout box highlights the recommendation to use AWS Amplify Hosting for static website hosting.

Step-13: Specify the file name in Index document which you have added in S3

S AWS Search [Alt+S] Asia Pacific (Mumbai) Imtaza

Amazon S3 > Buckets > intazaexp5 > 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.

**Error document - optional**  
This is returned when an error occurs.

**Redirection rules - optional**  
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

Condition	Redirection rule
1	

Step-14: Scroll down and save the changes at bottom right, Following screen will appear

intazaexp5 - S3 bucket | S3 | ap-south-1.console.aws.amazon.com/s3/buckets/intazaexp5?region=ap-south-1&bucketType=general&tab=properties

Gmail YouTube Maps Terra ERP Classroom

Search [Alt+S]

Amazon S3 > Buckets > intazaexp5

Successfully edited static website hosting.

intazaexp5 [Info](#)

Objects **Properties** Permissions Metrics Management Access Points

**Bucket overview**

AWS Region: Asia Pacific (Mumbai) ap-south-1

Amazon Resource Name (ARN): arn:aws:s3:::intazaexp5

Creation date: March 2, 2025, 23:51:09 (UTC+05:30)

**Bucket Versioning** [Edit](#)

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: Disabled

**Multi-factor authentication (MFA) delete** [Edit](#)

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Multi-factor authentication (MFA) delete: Disabled

**Tags (0)** [Edit](#)

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

Key	Value
No tags associated with this resource.	

CloudShell Feedback 29°C Smoke 025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG JN. 0002 03-03-2025

## Step-15: Click on Permissions Tab

The screenshot shows the AWS S3 console for the bucket 'intazaexp5'. The 'Permissions' tab is active. In the 'Block public access (bucket settings)' section, 'Block off public access' is set to 'Off'. Below that, under 'Bucket policy', it says 'No policy to display.' with an 'Edit' button.

## Step-16: In bucket policy click on Edit option

Step 17- after clicking on edit button paste the following code in bucket policy

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

Note-Make sure that you add your bucket name in the code above

The screenshot shows the 'Edit bucket policy' page for the 'intazaexp5' bucket. The policy document is displayed in a code editor:

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "PublicReadGetObject",
6        "Effect": "Allow",
7        "Principal": "*",
8        "Action": [
9          "s3:GetObject"
10        ],
11        "Resource": [
12          "arn:aws:s3:::intazaexp5/*"
13        ]
14      }
15    ]
16  }

```

To the right, there's a panel titled 'Edit statement' with a sub-section 'Select a statement' containing a button '+ Add new statement'.

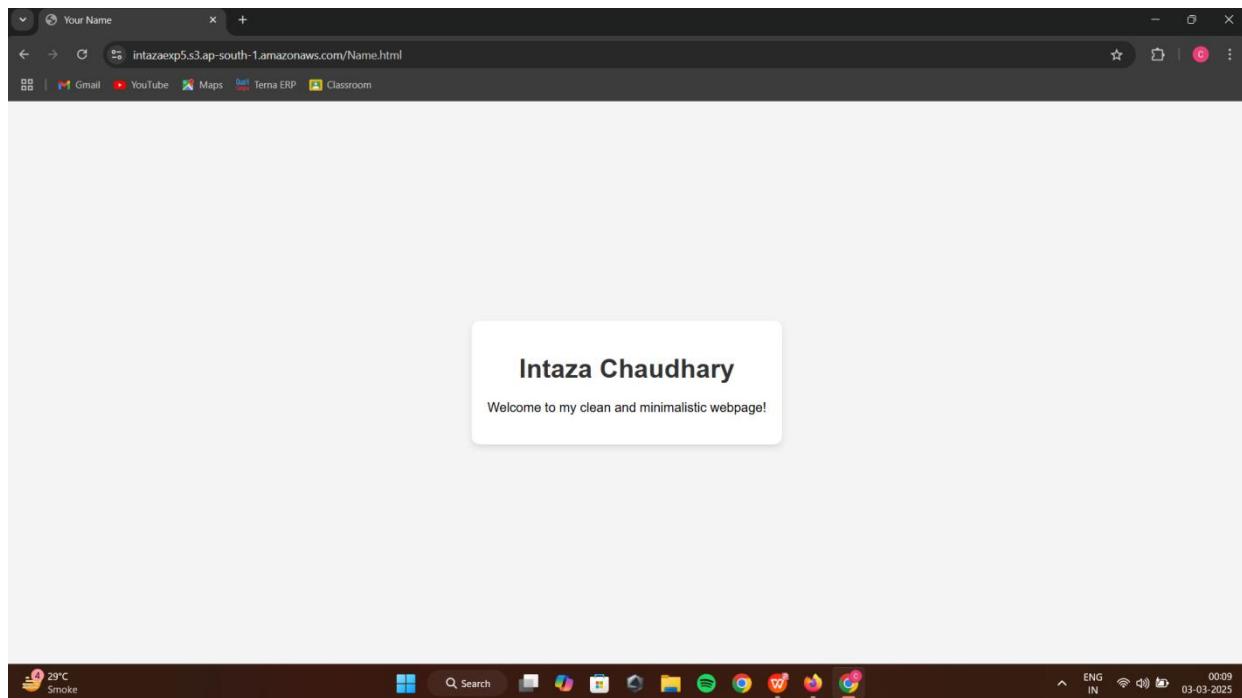
Scroll down and click on Save Changes button

The screenshot shows the 'Permissions' tab for the 'intazaexp5' bucket. A green success message box says 'Successfully edited bucket policy.' Below it, the 'Bucket policy' section shows the same JSON policy as before.

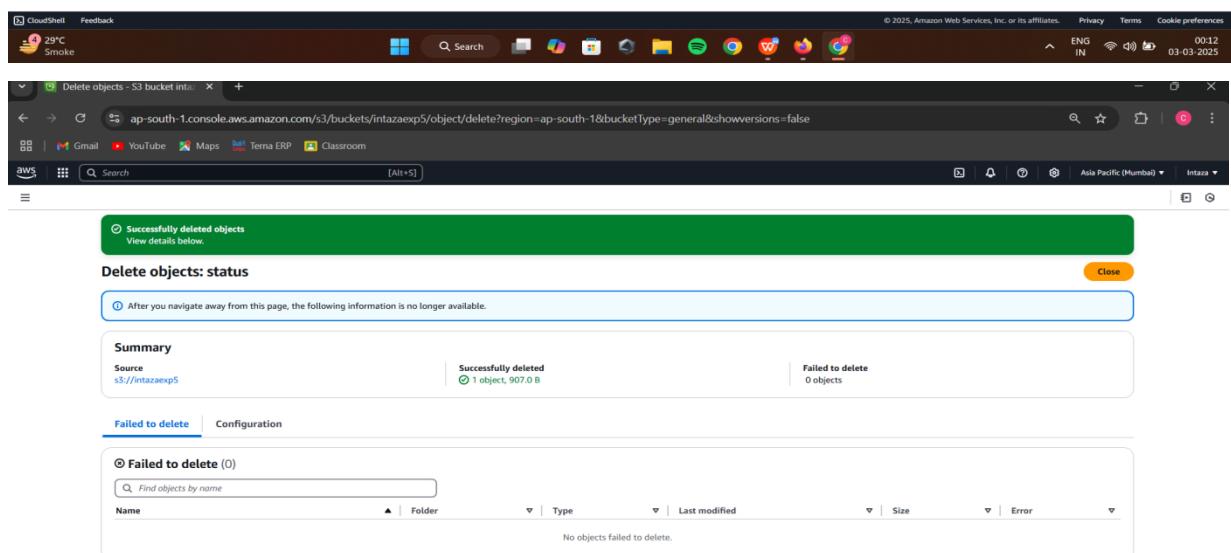
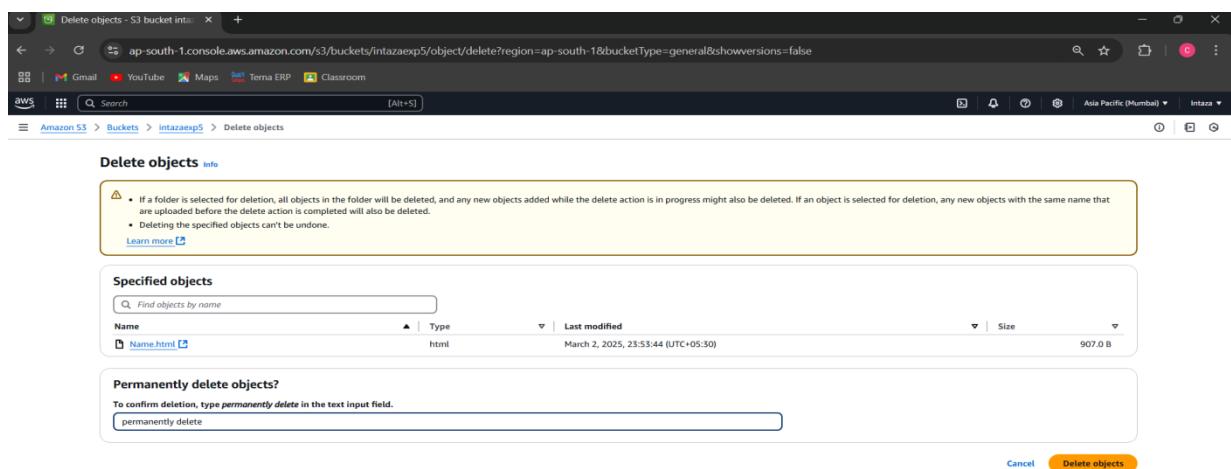
Step-18: open your html file and click on Object URL

The screenshot shows the 'Name.html' object details page. Key information includes:

- Object overview:**
  - Owner: 765c6baaa7cfdef7614f0444ebd86773e78746fdf83f7dff111dbf11b72fb5
  - AWS Region: Asia Pacific (Mumbai) ap-south-1
  - Last modified: March 2, 2025, 23:53:44 (UTC+05:30)
  - Size: 907.0 B
  - Type: html
  - Key: Name.html
- Object management overview:** The following bucket properties and object management configurations impact the behavior of this object.
- Bucket properties:** Bucket Versioning (Enabled).
- Management configurations:** Replication status (When a replication rule is applied to an object the replication status indicates the progress of the operation).



Step-19: Now for delete files click on checkbox of your file and then click on Delete Button, Write permanently delete and click on delete object button



Step-20: now come to Amazon S3 tab and select your bucket and then click on delete button, Write down your bucket name in delete bucket tab and click on delete button at bottom right

The screenshot shows the 'Delete bucket' dialog box. It includes a warning message about the不可逆性 of deleting buckets and a text input field where 'intazaexp5' is typed. Buttons for 'Cancel' and 'Delete bucket' are visible.

Step-21: You can see that the bucket is deleted

The screenshot shows the 'S3 buckets' page. A green success message indicates the bucket 'intazaexp5' was successfully deleted. The table lists one remaining bucket: 'elasticbeanstalk-ap-south-1-699475959073'. The status bar at the bottom shows the date and time as 03-03-2025 00:15.

### Q3: Compare Google drive with AWS S3

GOOGLE DRIVE	AMAZON S3
It is owned by Google LLC.	It is owned by Amazon.
It was launched in 2012.	It was launched in 2006.
It offers 15 GB free storage space.	It offers 5 GB free storage space.
It was developed by Google.	It was developed by Amazon Web Services(AWS).
The number of users using Google Drive is more.	The number of users using Amazon S3 is less.
It provides full security of data.	It also provides full security of data but comparatively less.
It has the maximum storage size of 30 TB.	It has the unlimited maximum storage size for paid users.
It does not support remote uploading.	Remote uploading is not supported here also.
Maximum file size in Google Drive is 5TB.	Here maximum file size is 5 TB.
It supports file versioning.	It also supports file versioning.

### B.2 Conclusion:

In this experiment, we successfully demonstrated the implementation of **Storage as a Service (SaaS)** using **AWS S3**. Through this, students gained practical exposure to various AWS storage solutions, including **Amazon EBS**, **Amazon EFS**, **Amazon S3 Glacier**, and **AWS Storage Gateway**, understanding their use cases and benefits.