**Assignment No: 5**

**Name**: Tanishq Thuse **Roll No**: 52 **PRN**: 12310237 **Div**: CS (AI) - B

**Title:** To create login into AWS and use S3 Bucket Service for storage. To work on different Cloud Storage Services.

**Description**

An object storage service called Amazon Simple Storage Service (Amazon S3) provides performance, security, scalability, and data availability that are among the best in the business. Any quantity of data may be stored and protected using Amazon S3 by users of all sizes and sectors for a variety of use cases, including data lakes, websites, mobile apps, backup and restoration, archives, and enterprise apps, Internet of Things gadgets, and big data analytics. Amazon S3 offers control functionalities, therefore that access to your data may be optimized, arranged, and configured to suit your unique business needs, organizational as well as legal criteria.

# **Key Features of AWS S3**

AWS S3 provides a strong set of features that make it a versatile and essential tool for businesses and individuals alike. Here are some of the key features in detail:

## **Scalability**

AWS S3 can handle massive amounts of data and traffic. It allows users to store an unlimited amount of data,with individual objects ranging from 0 bytes to 5 TB. The service automatically scales storage resources to meet demand, ensuring that applications run smoothly without the need for manual intervention.

## **High Durability and Availability**

One of the most compelling features of AWS S3 is its high durability and availability. It guarantees 99.99% durability, meaning that data is extremely safe and unlikely to be lost. It also promises 99.99% availability, ensuring that data is accessible when needed. This is achieved through redundant storage across multiple facilities and devices.

## **Security**

AWS S3 provides comprehensive security features to protect data:

* **Encryption:**It offers both server-side encryption (SSE) and client-side encryption for data security. Server-side encryption includes options like S3-managed keys (SSE-S3), AWS Key Management Service keys (SSE-KMS), and customer-provided keys (SSE-C).
* **Access Control:** Users can manage access to S3 resources using Identity and Access Management (IAM) policies, Access Control Lists (ACLs), and bucket policies. These tools help in finely tuning who can access what data.

## **Data Transfer and Acceleration**

AWS S3 supports data transfer at high speeds, making it ideal for moving large volumes of data. Features like S3 Transfer Acceleration enable faster uploads and downloads of content by leveraging Amazon CloudFront’s globally distributed edge locations.

## **Data Transfer and Acceleration**

AWS S3 supports data transfer at high speeds, making it ideal for moving large volumes of data. Features like S3 Transfer Acceleration enable faster uploads and downloads of content by leveraging Amazon CloudFront’s globally distributed edge locations.

Amazon S3 (Simple Storage Service) is a scalable cloud storage service that allows users to store and retrieve any amount of data at any time. Here are its key concepts in brief:

**How Amazon S3 works**

Amazon S3 is an object storage service that stores data as objects within buckets. An object is a file and any metadata that describes the file. A bucket is a container for objects. To store your data in Amazon S3, you first create a bucket and specify a bucket name and AWS Region. Then, you upload your data to that bucket as objects in Amazon S3. Each object has a key (or key name), which is the unique identifier for the object within the bucket. S3 provides features that you can configure to support your specific use case. For example, you can use S3 Versioning to keep multiple versions of an object in the same bucket, which allows you to restore objects that are accidentally deleted or overwritten. Analytics and insights API Version 2006-03-01 5 Amazon Simple Storage Service User Guide Buckets and the objects in them are private and can be accessed only if you explicitly grant access permissions. You can use bucket policies, AWS Identity and Access Management (IAM) policies, access control lists (ACLs), and S3 Access Points to manage access.

**Key Aspects of S3**

**Buckets:**  Containers for storing objects. Each bucket has a unique name within the S3 namespace and is used to organize and manage data.

**Objects:** The fundamental entities stored in S3, consisting of data (files), metadata, and a unique identifier (key). Each object is stored within a bucket.

**Keys:** Unique identifiers for objects within a bucket. They are used to retrieve and manage objects.

**Regions:** Geographic locations where S3 buckets are created. Data is stored redundantly within a region to ensure durability and availability.

**Storage Classes:** Different types of storage options (e.g., Standard, Intelligent-Tiering, Glacier) that offer varying levels of access frequency, durability, and cost.

**Permissions:** Access controls and policies that determine who can view, upload, or manage objects and buckets. These include bucket policies, access control lists (ACLs), and Identity and Access Management (IAM) policies.

**Versioning:** A feature that keeps multiple versions of an object, allowing for recovery from accidental deletions or overwrites.

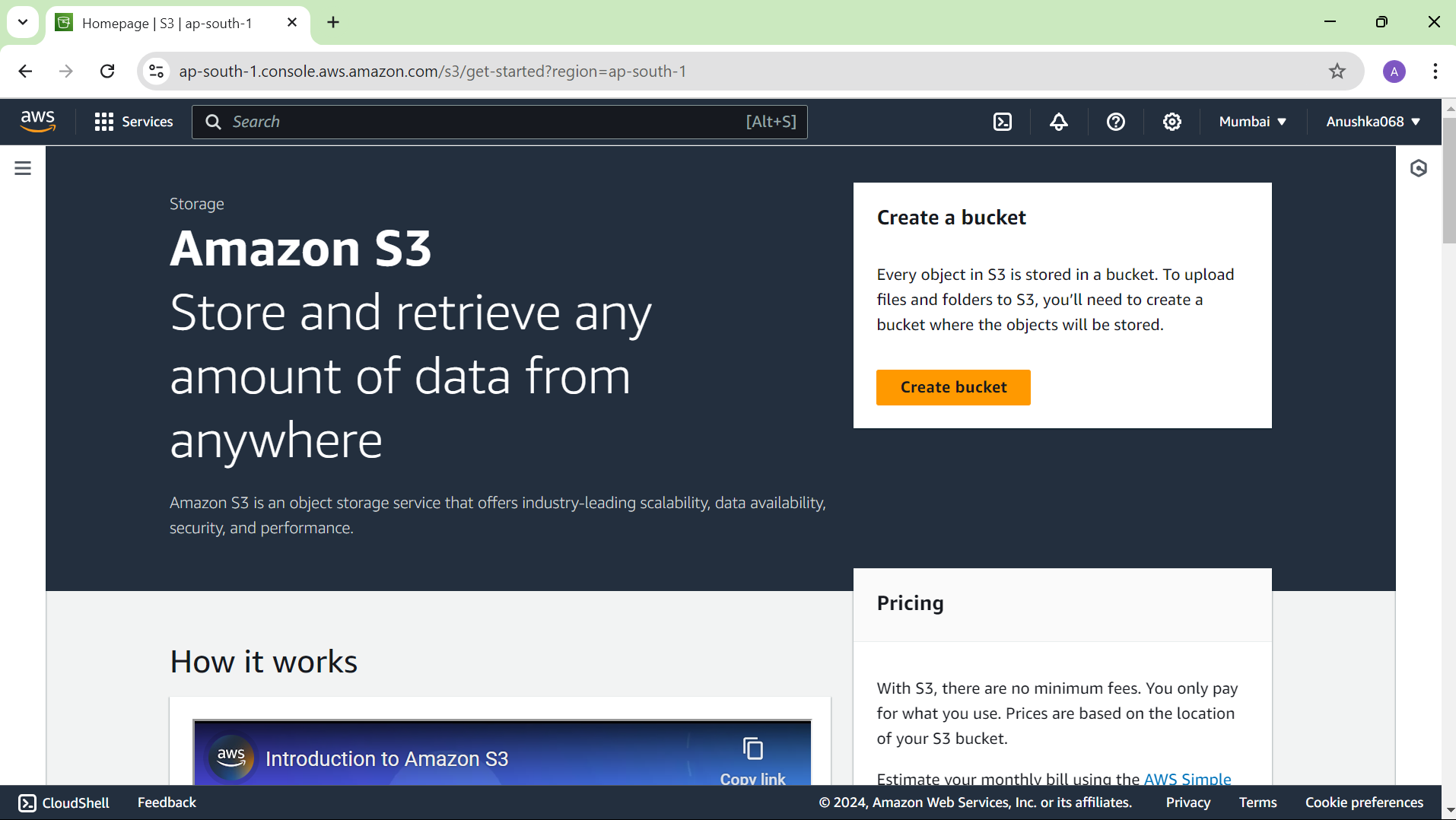
**Lifecycle Policies:** Rules that automate the transition of objects between storage classes or the deletion of objects after a certain period.

These concepts form the foundation of how Amazon S3 provides scalable, secure, and flexible storage solutions in the cloud.

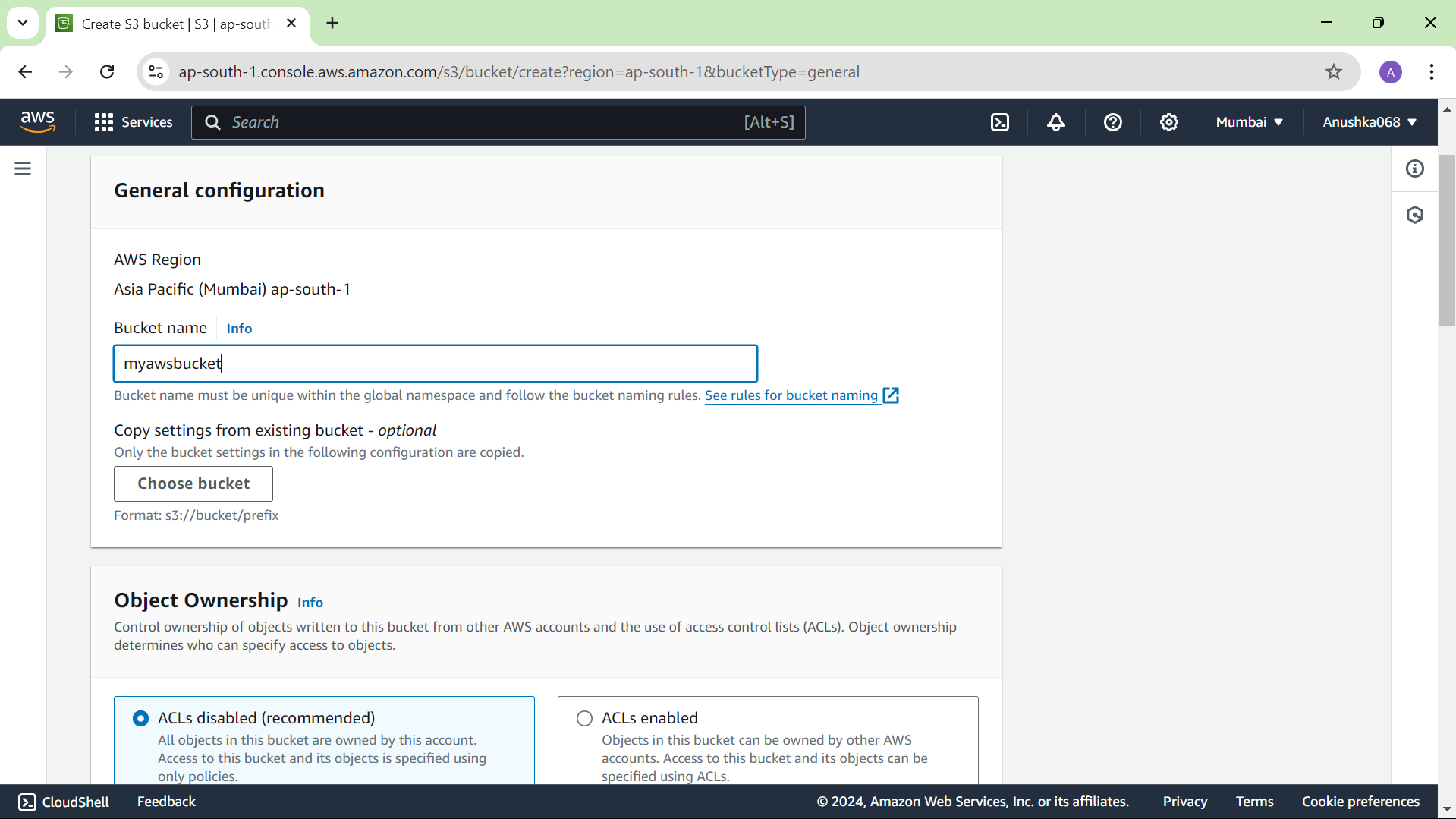


**Step 1: Create your first S3 bucket**

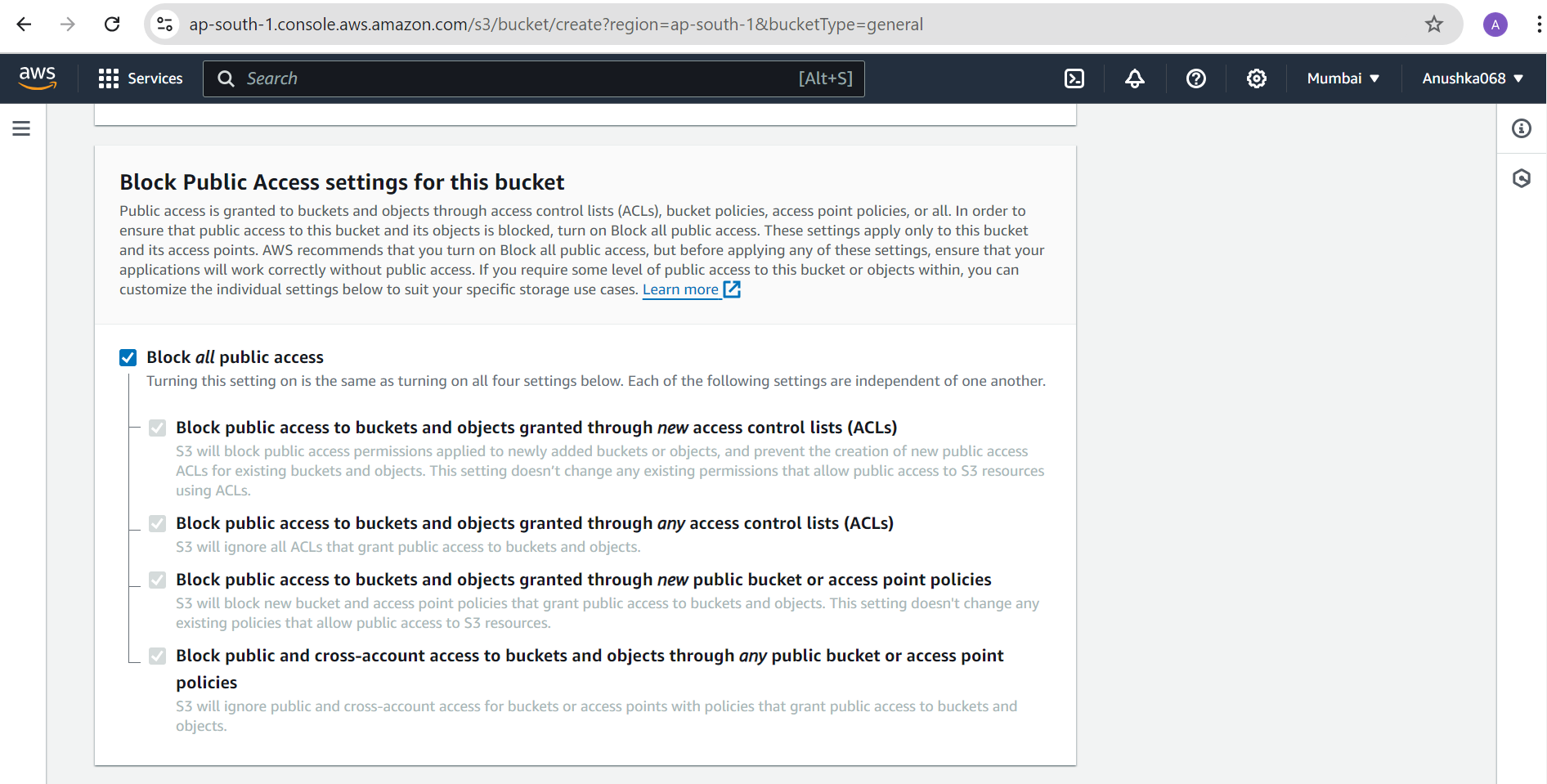
After you sign up for AWS, you're ready to create a bucket in Amazon S3 using the AWS Management Console. Every object in Amazon S3 is stored in a bucket. Before you can store data in Amazon S3, you must create a bucket.



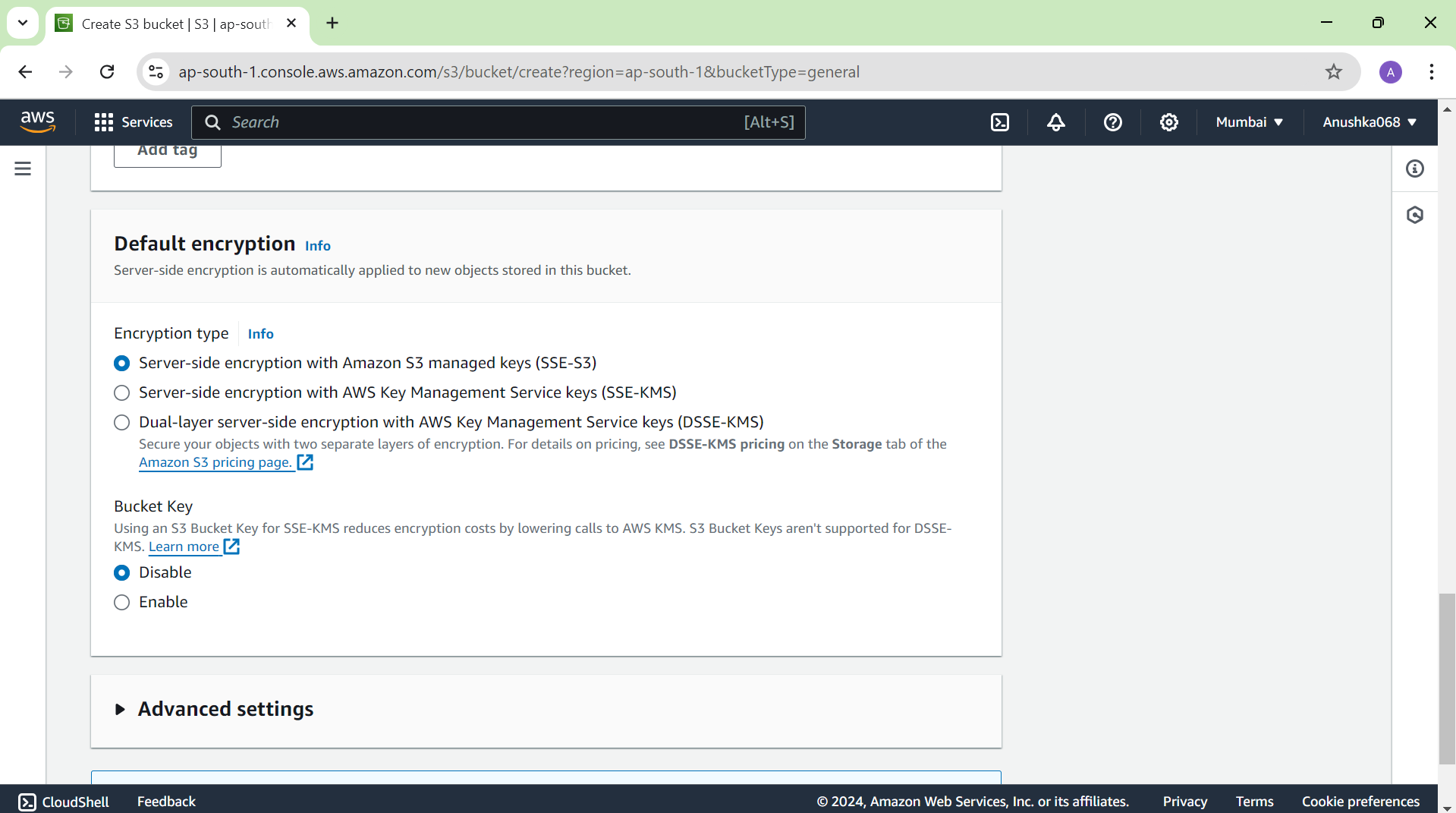
**Step 02:** On the search bar type **“S3”** and click enter on it. It opens a window for creating a bucket. Give a unique bucket name and make **“object ownership as enabled”.**



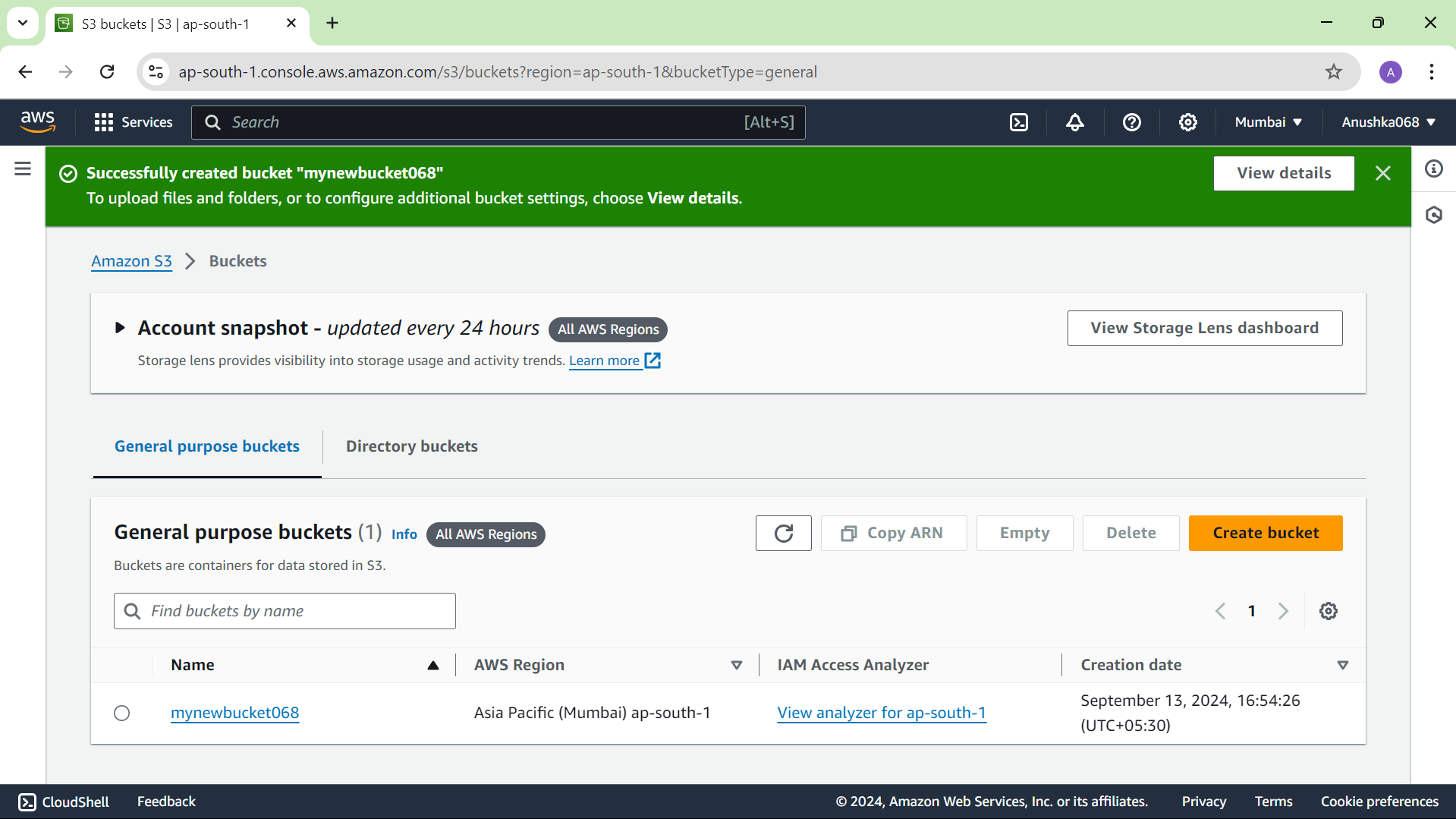
Tick on **“Block all public access”**



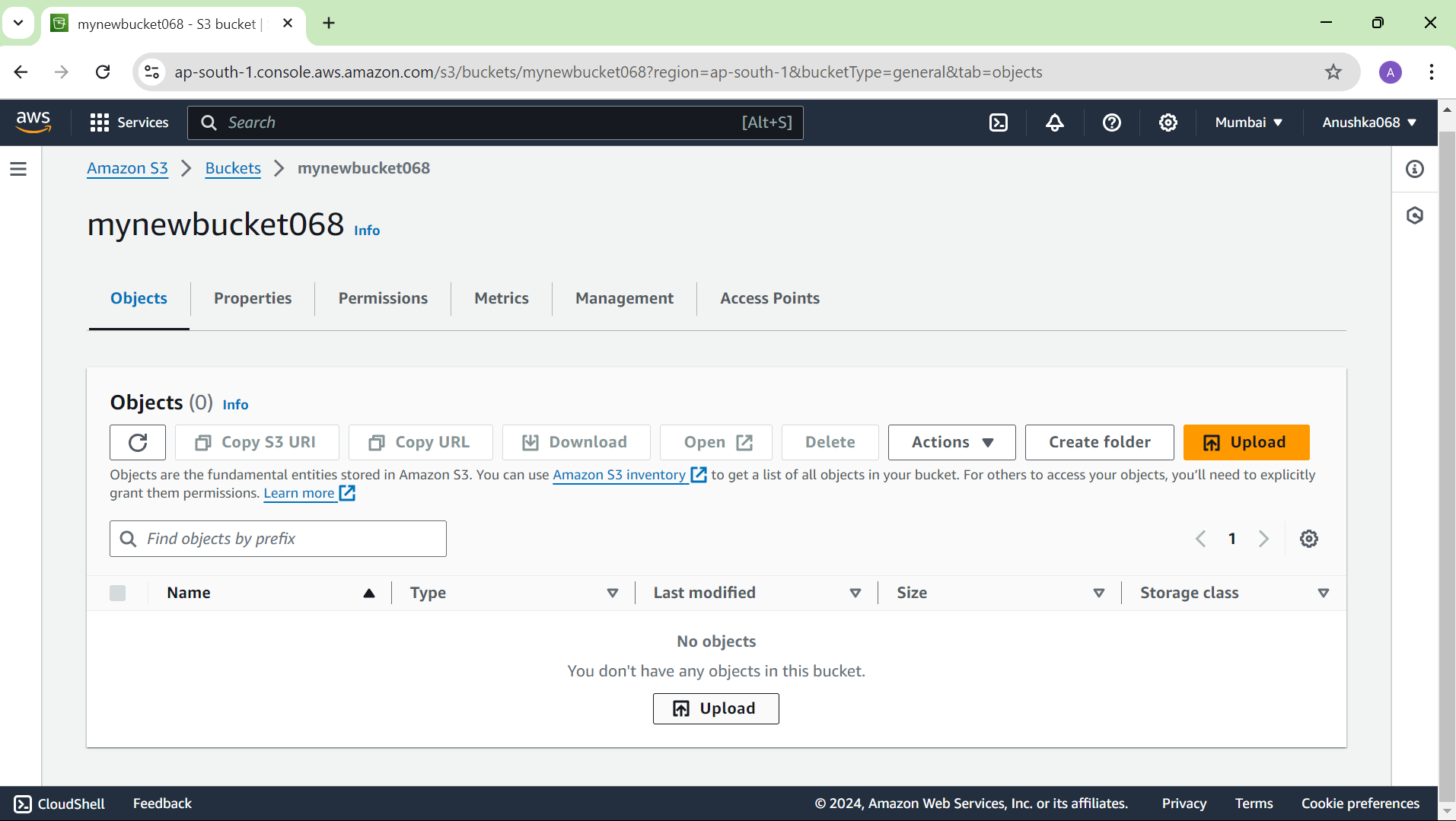
After checking all the things, click on the “create bucket” button for creating a bucket.



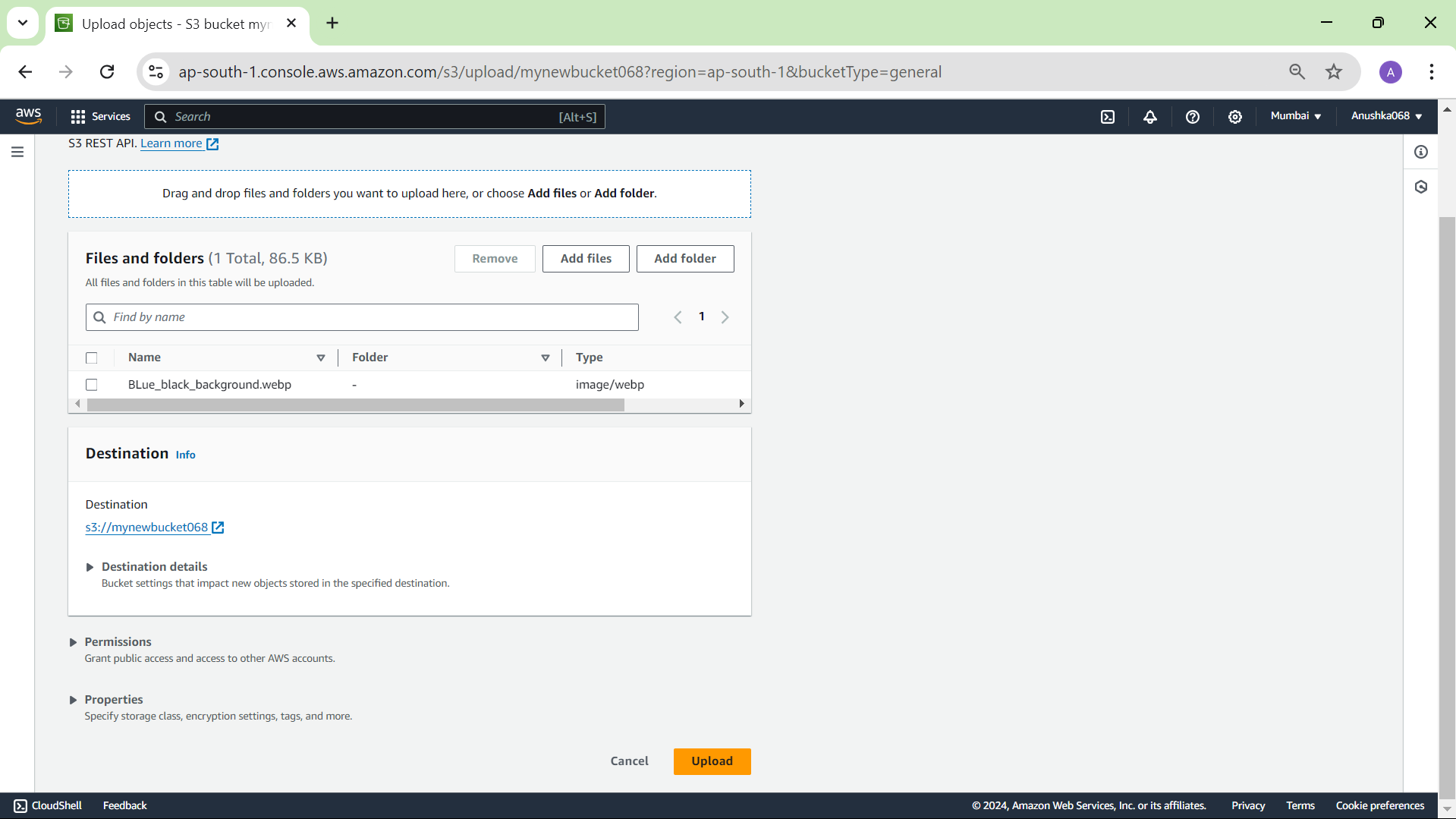
**Step 03:** You have successfully created a bucket with name **“mynewbucket068”** and click on “view details” for more information.



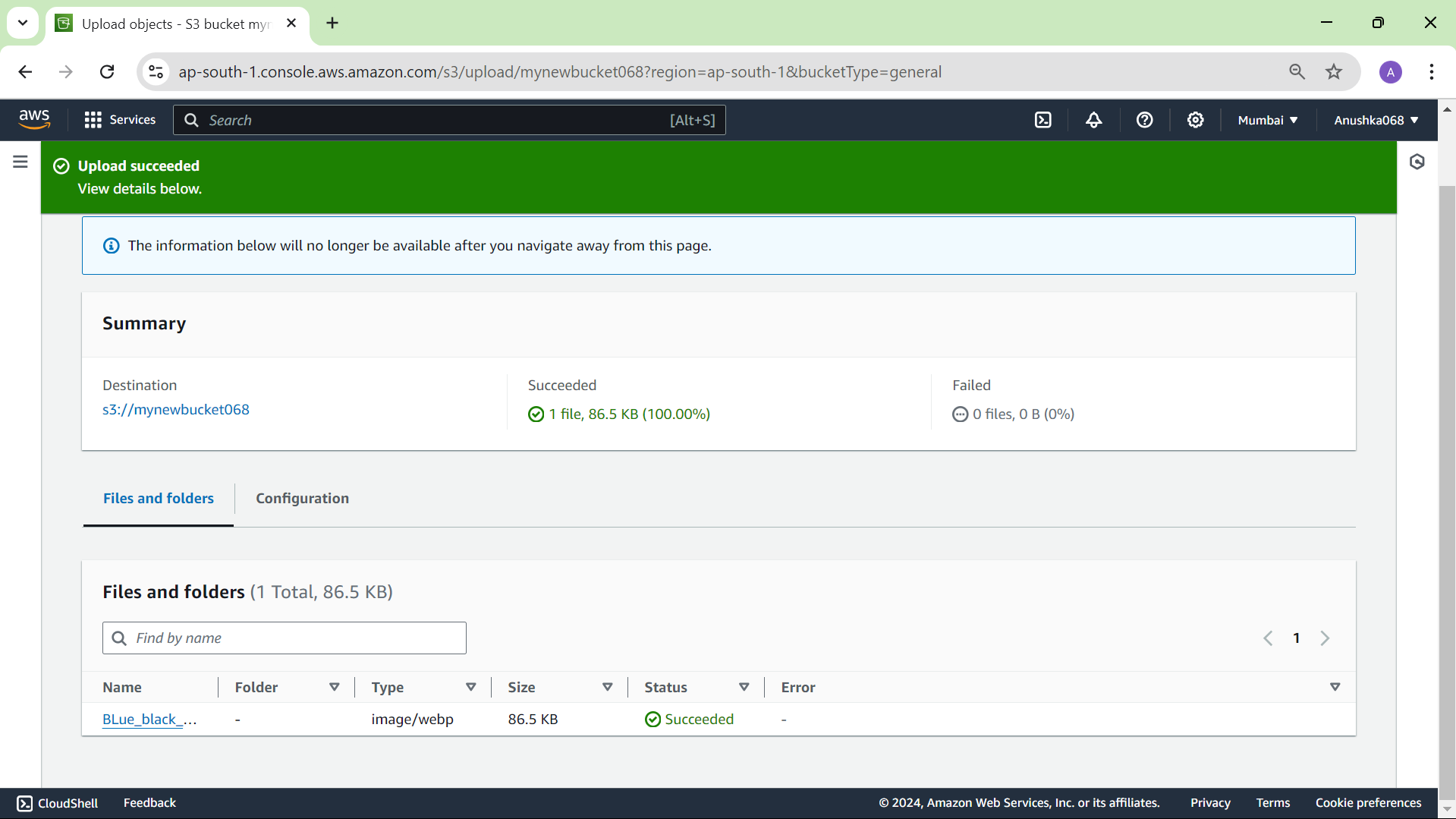
**Step 04:** After going inside the new bucket, you can add and store any file or folder you want. For adding a file or folder click on the **‘upload’** button.



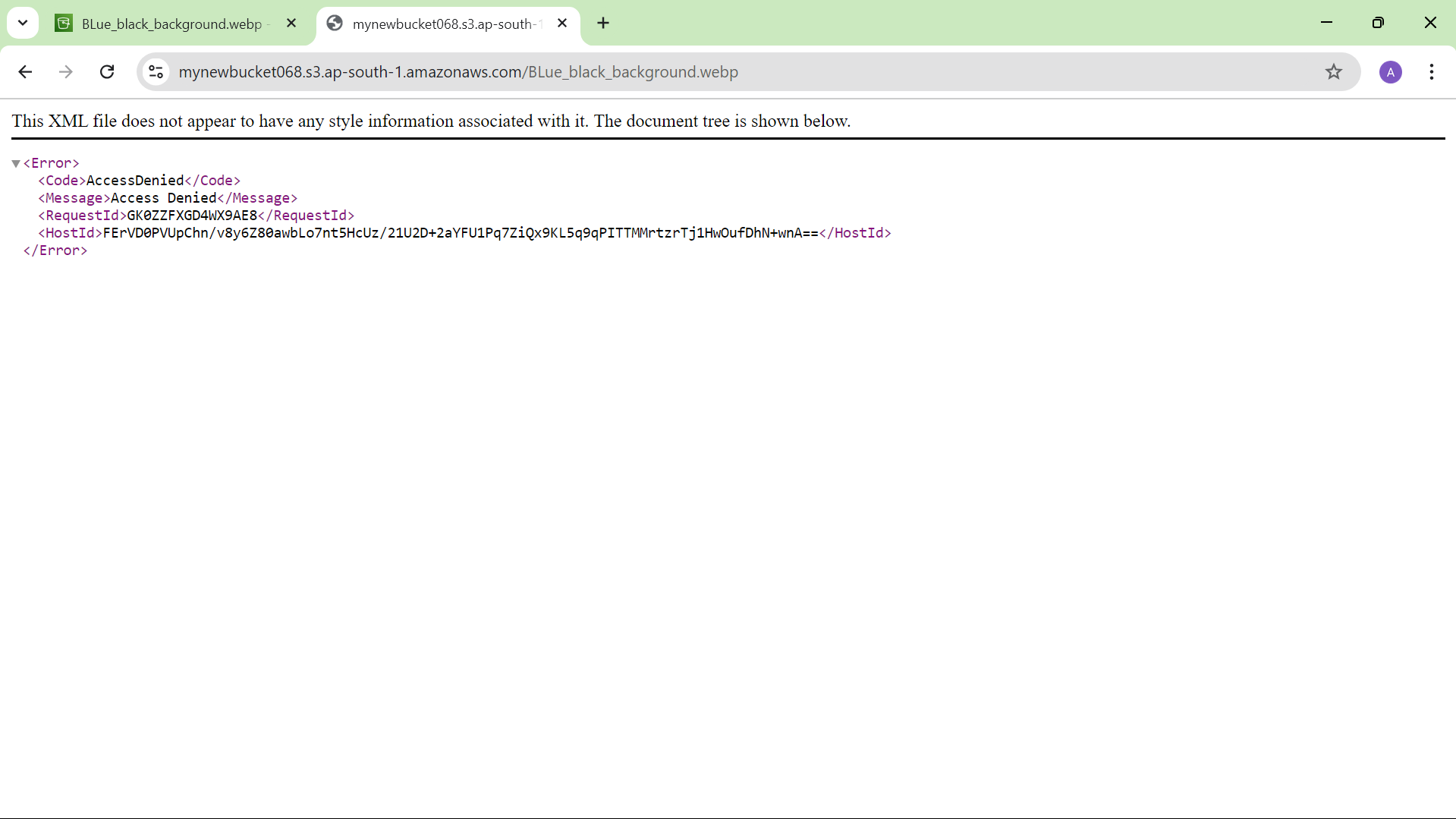
After selecting the file, click on the ‘upload’ button given at the end.



You have successfully uploaded a file (here, an image) in the newly created bucket **mynewbucket068**

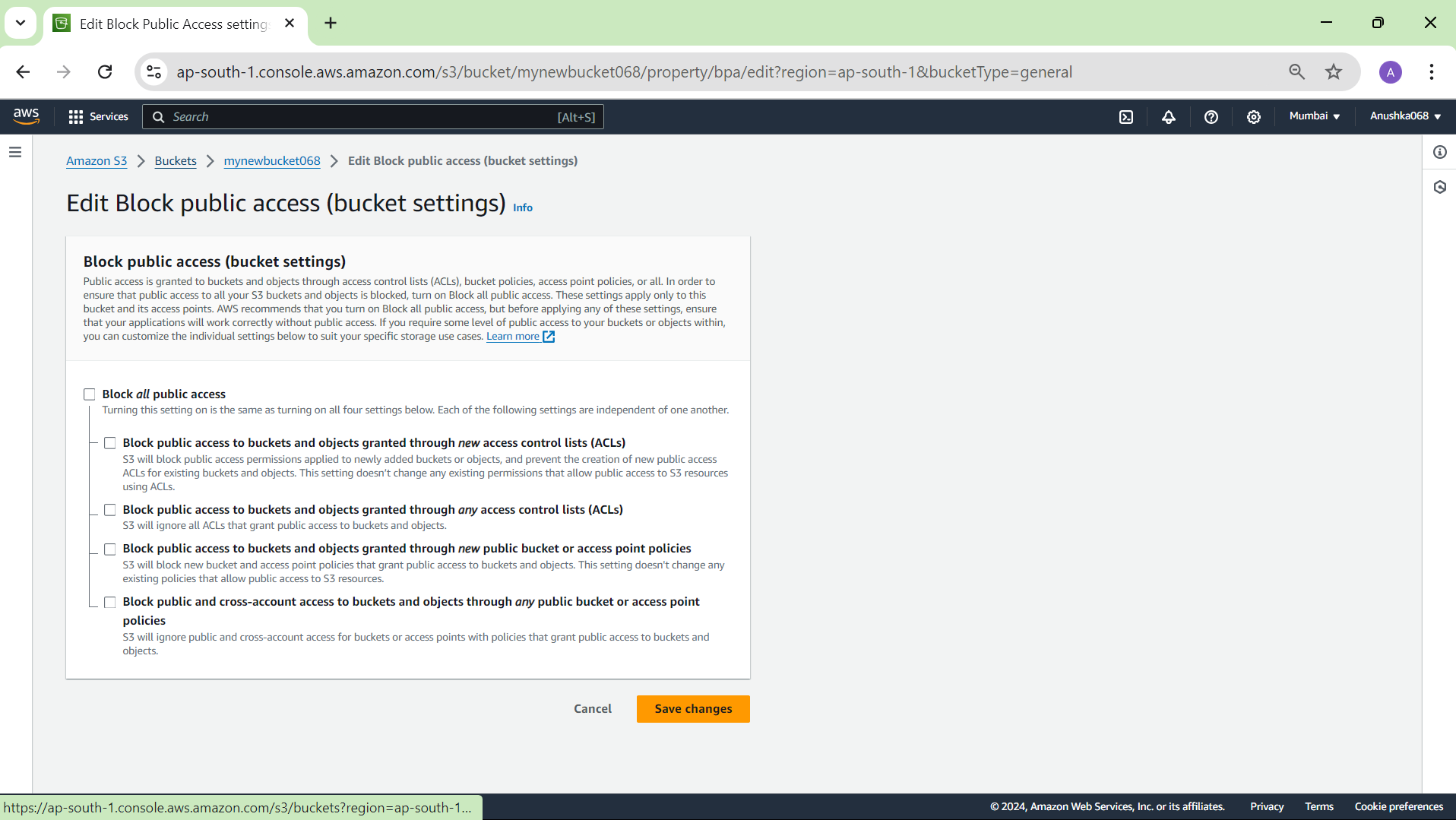


**Step 05:** Now you want to view that file, so for that go to the objects in the bucket and there would be an URL, copy it and paste it in the new tab. Initially, you would see an error given below.

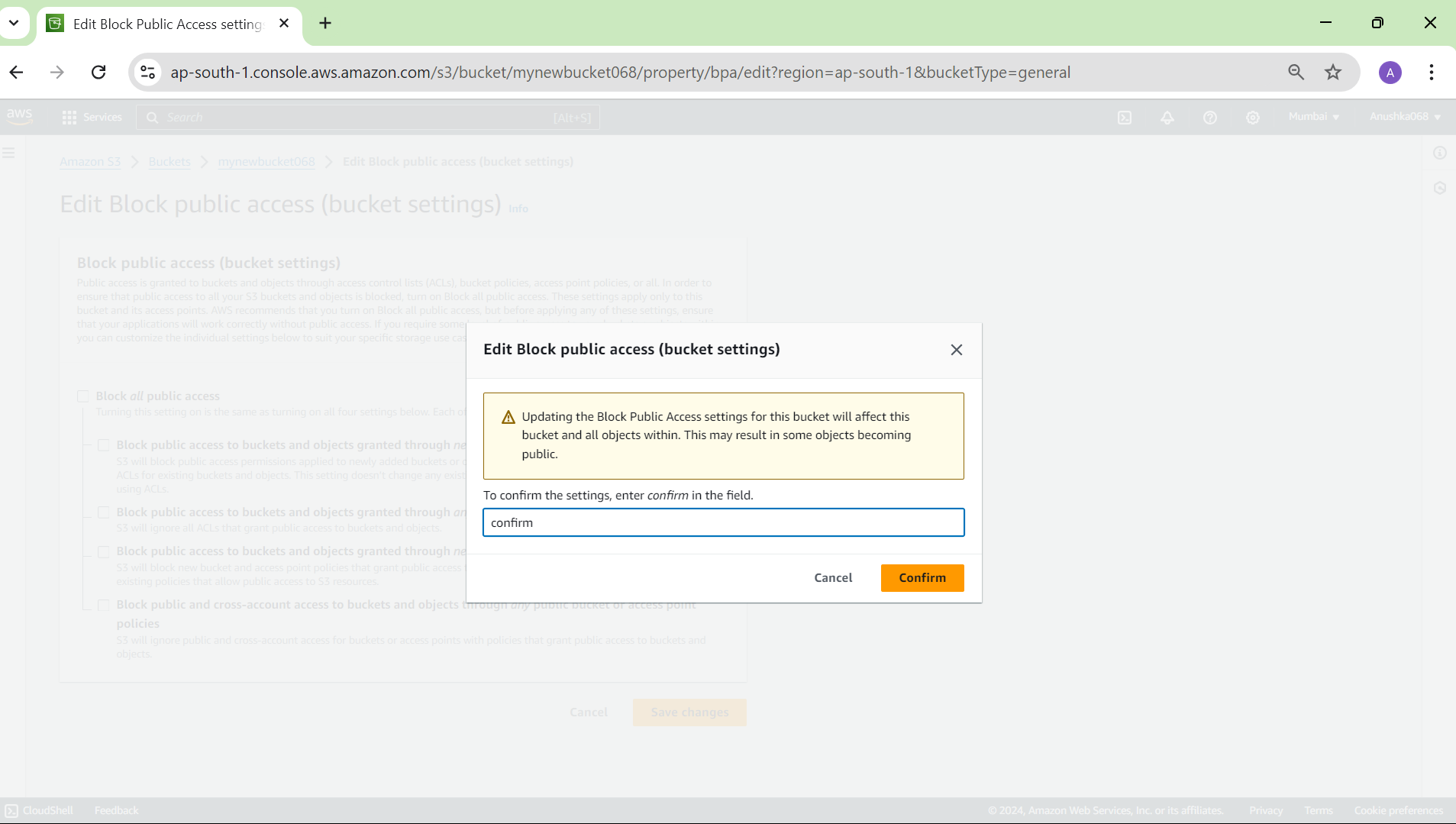


This error occurs and you are not able to see an image uploaded because while creating a bucket you had blocked the public access, so you need to edit that and give access to view it.

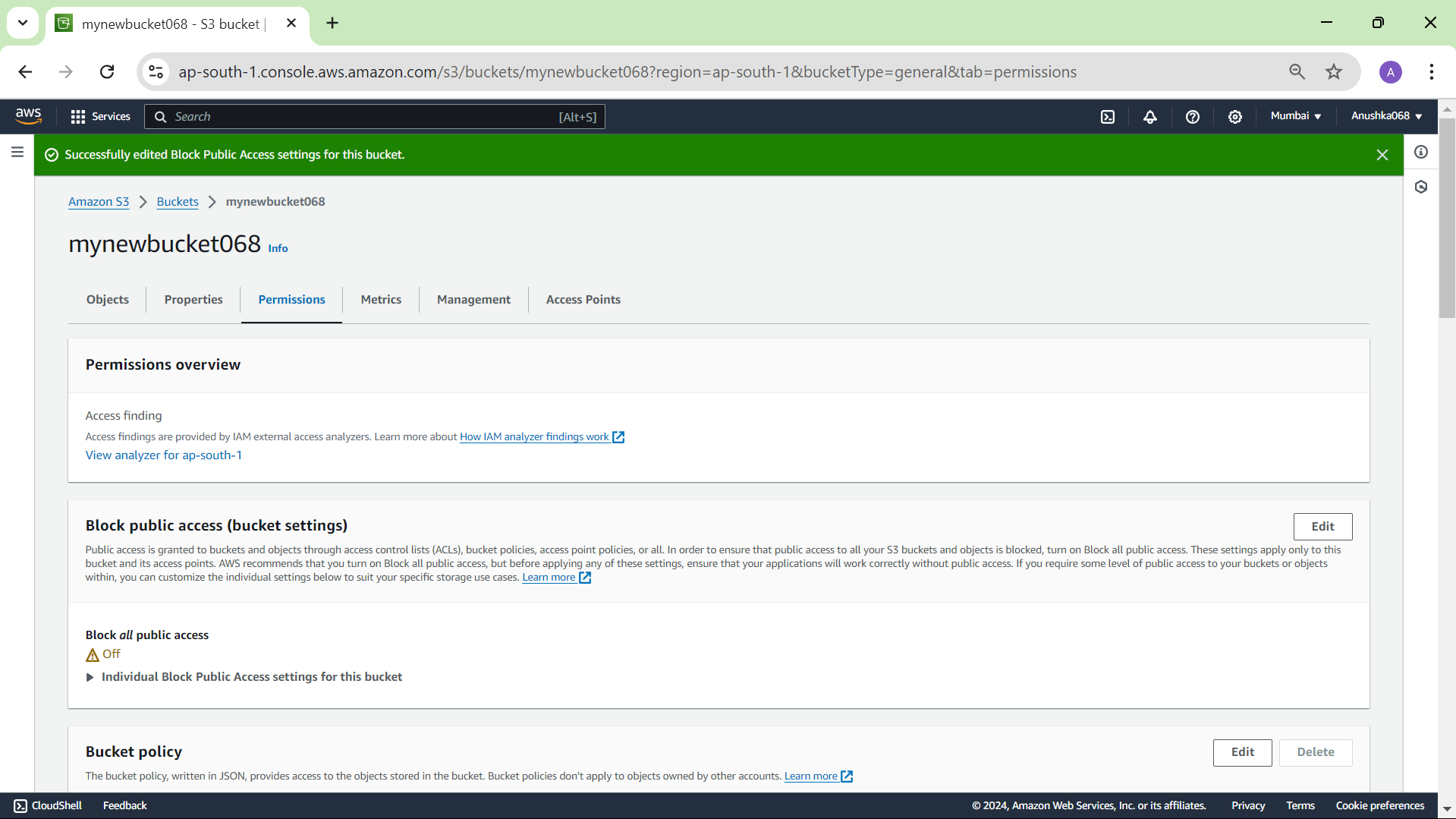
**Step 06:** For editing view access, go to **“Edit Block public access”** and untick the **‘Block all public access’** and click on **“save changes”.**



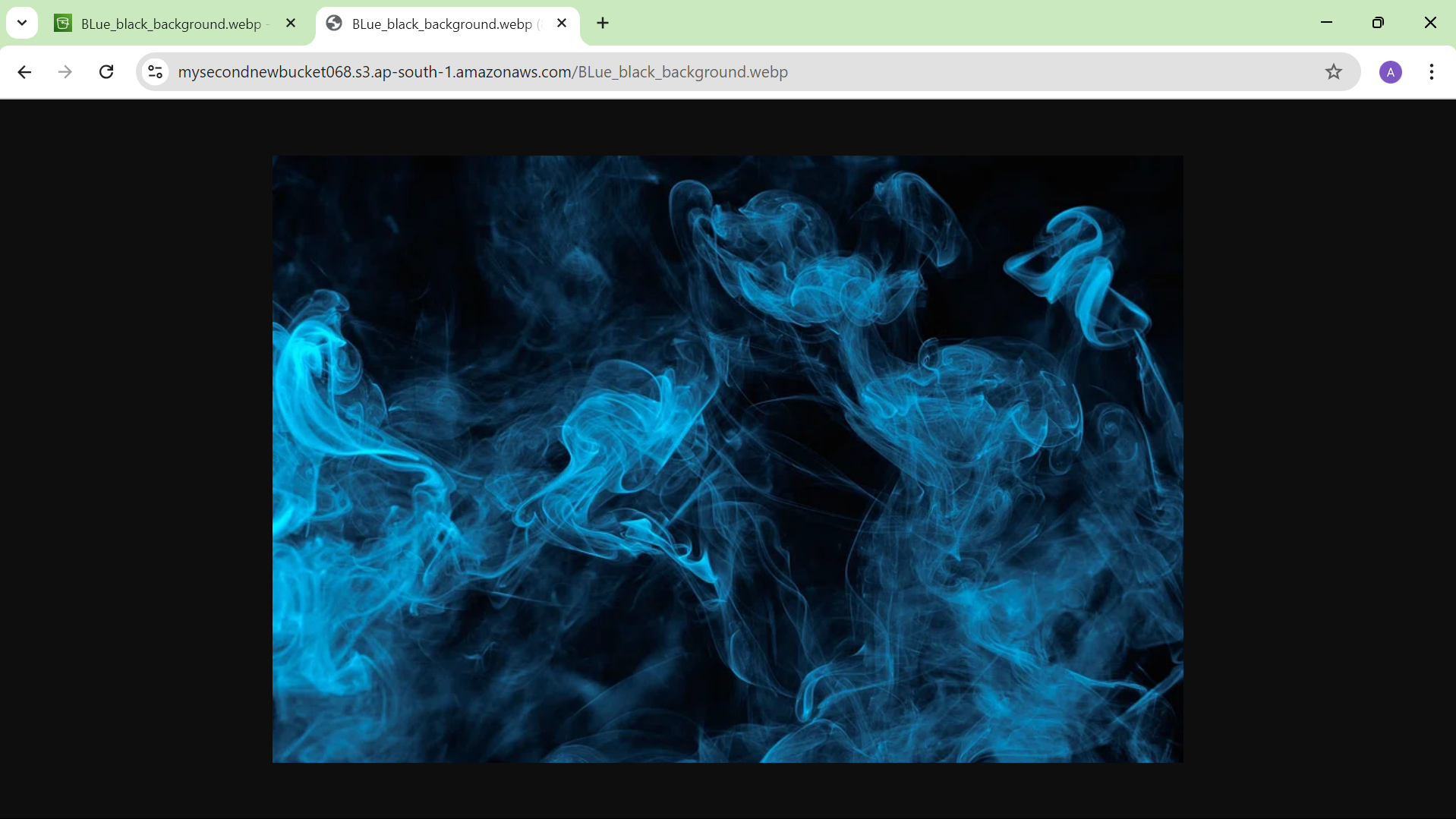
**Step 07:** After clicking on **‘save changes’**, this block will appear. Type **‘confirm’** and click on **‘confirm’** to confirm the changes you made.



**Step 08:** Now again go to the objects of the bucket ‘mynewbucket068’ and click on the image file uploaded earlier.

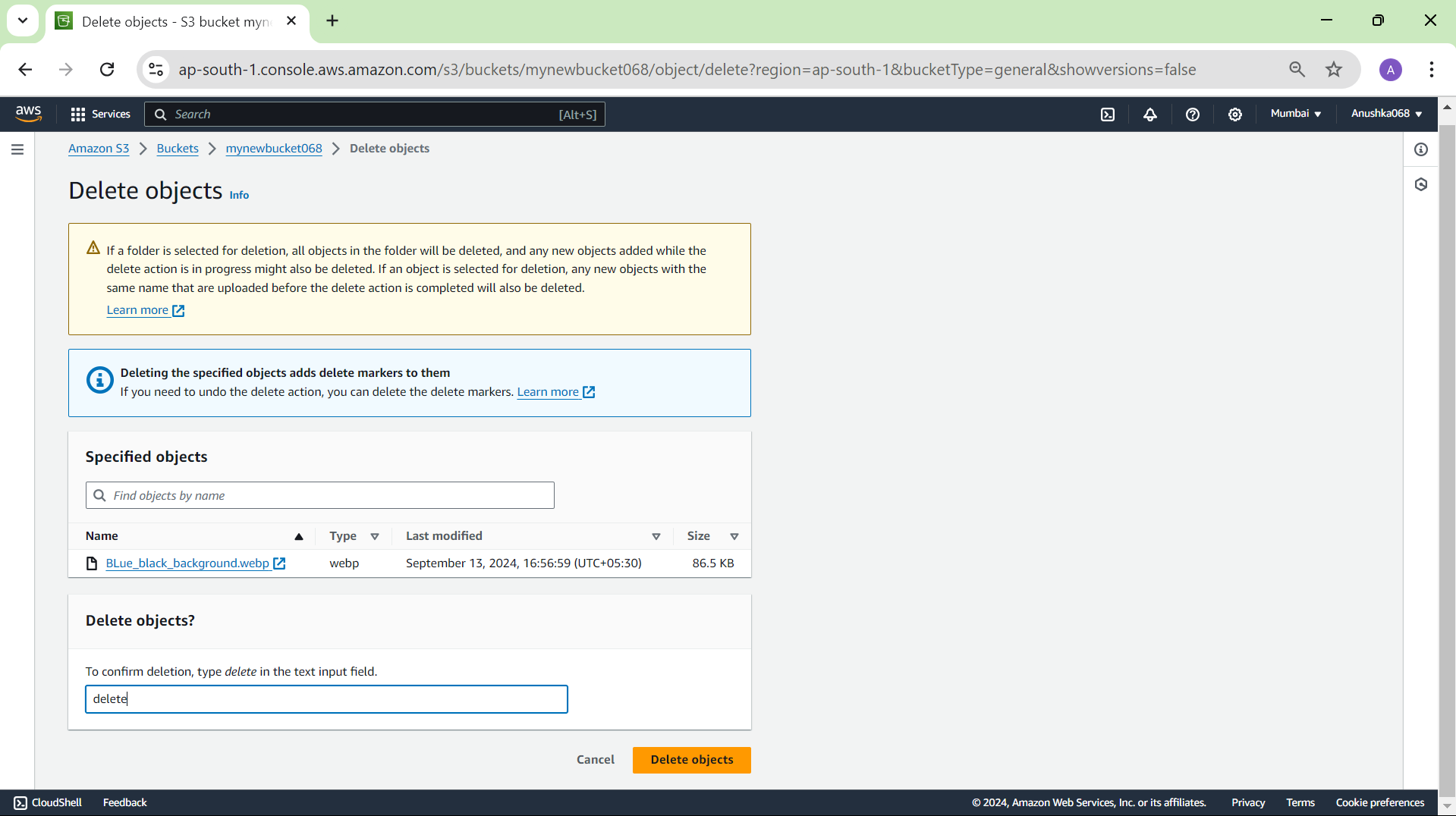


Click on the URL shown and now you should be able to see the image that you had uploaded.



**Step 09:** **Delete Object and S3 Bucket**

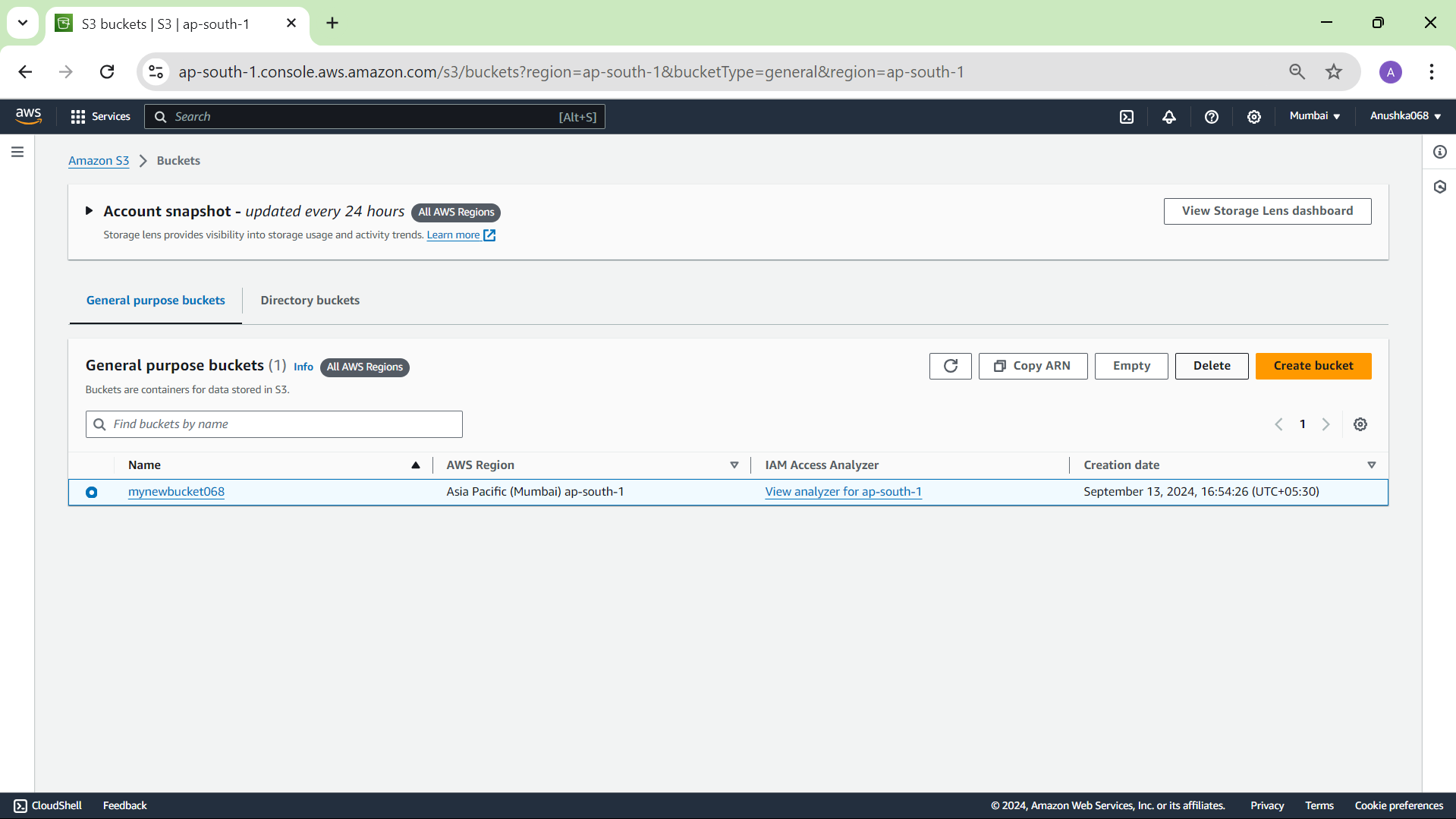
For deleting Object, you have to click on **remove**, then it will redirect to delete object console and then type **delete** and click on **‘Delete objects”** buttonto delete object.

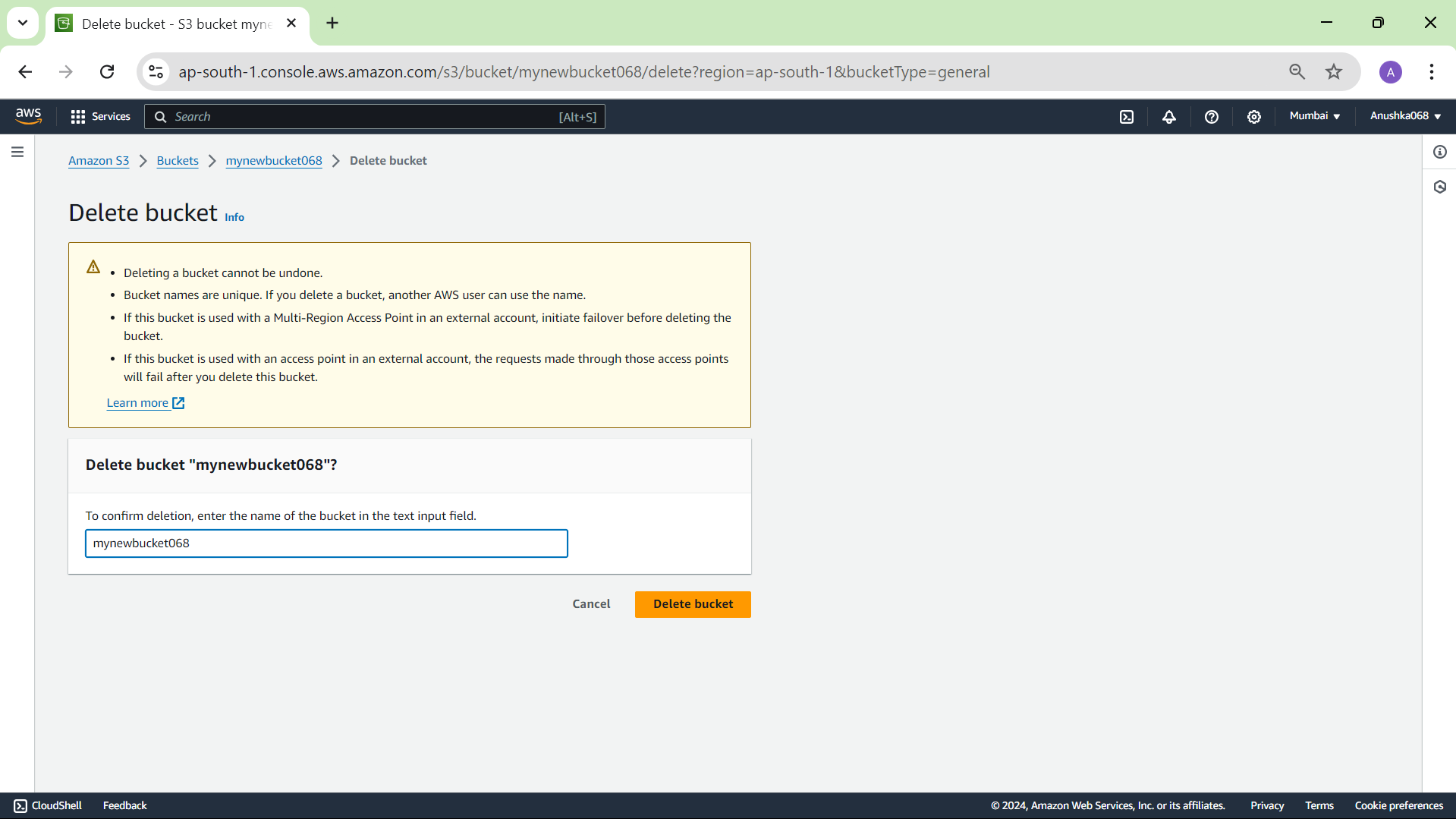


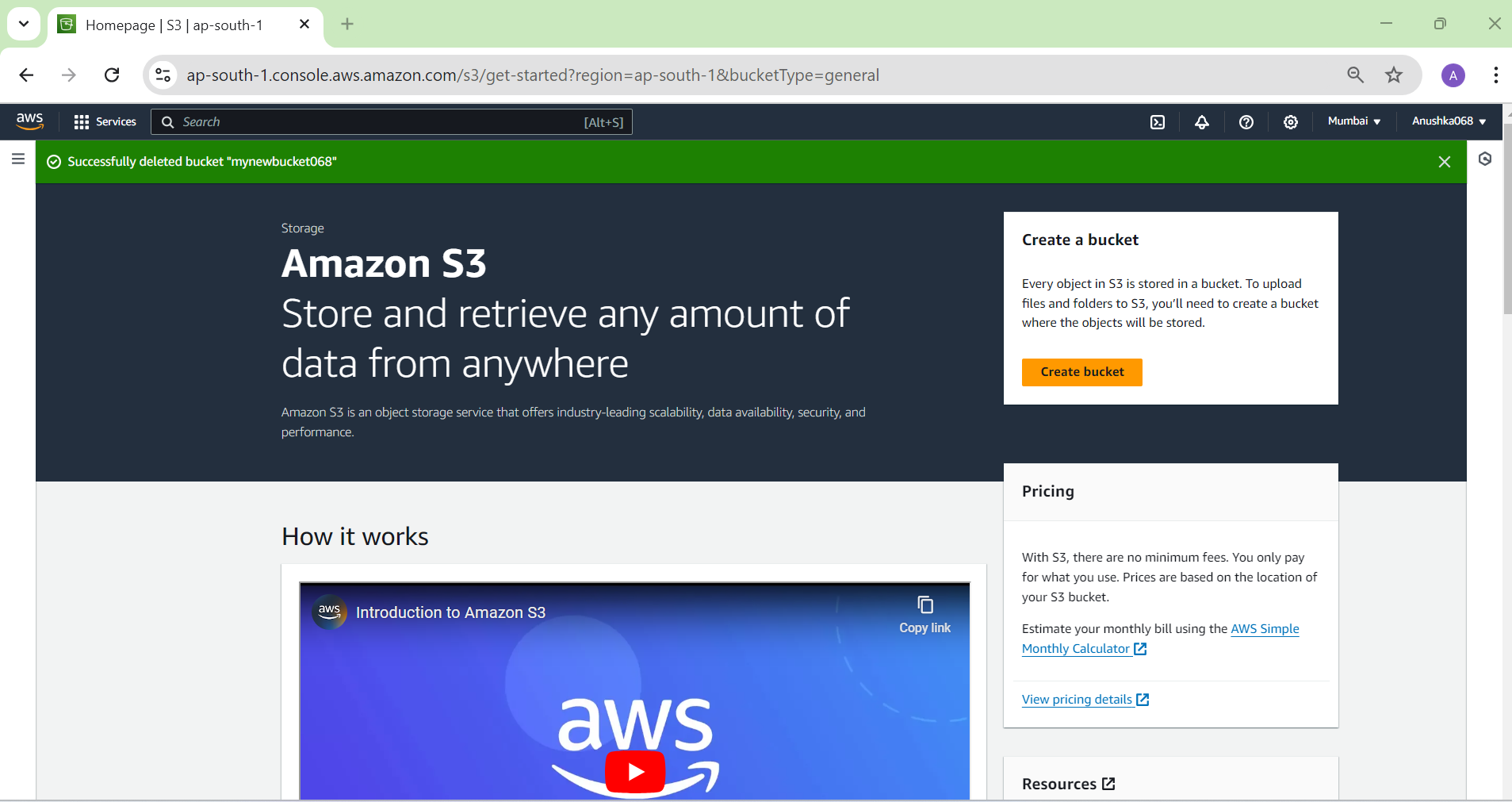
**Bucket deletion**

If you only delete object still bucket will pay charges, so you have to delete bucket also.

You have to enter the bucket name that you want to delete and then click on delete bucket button. But before deleting the bucket you need to emptied it, so click on ‘empty bucket’ and then delete that bucket again.







Insights:

In this experiment, I learned how to create an Amazon S3 bucket and upload objects (files) to it using the AWS Management Console. I created a unique bucket with settings to block public access, then uploaded a file to the bucket. To view the uploaded file publicly, I changed the bucket’s permissions by disabling the block on public access. I also learned how to delete objects and empty and delete the bucket itself to avoid charges. This exercise helped me understand key AWS S3 features like object storage, buckets, permissions, scalability, durability, and security, which are essential for managing cloud data efficiently.