

LAB ASSIGNMENT 3

AIM: To study AWS S3 service and create a bucket for hosting static web application.

LO1: To understand the fundamentals of Cloud Computing and be fully proficient with Cloud based DevOps solution deployment options to meet your business requirements.

THEORY:

1. Create a S3 bucket.

The screenshot displays the AWS S3 Management Console in a web browser. The top navigation bar shows the 'Services' menu and a search bar. The main content area is titled 'Storage' and 'Amazon S3', with the tagline 'Store and retrieve any amount of data from anywhere'. A 'Create a bucket' button is prominently displayed. Below this, there is a 'How it works' section with a video player showing an 'Introduction to Amazon S3' video. To the right, there are sections for 'Pricing' and 'Resources'. The bottom part of the screenshot shows the 'Create bucket' configuration page. The 'General configuration' section includes a 'Bucket name' field with the value 'prasad-websitd', an 'AWS Region' dropdown set to 'Europe (Stockholm) eu-north-1', and a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. The 'Object Ownership' section shows 'ACLs disabled (recommended)' selected. The bottom of the screen shows the Windows taskbar with the date and time as 02:00 on 15-10-2023.

S3 bucket

s3.console.aws.amazon.com/s3/bucket/create?region=eu-north-1

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.

Warning 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.

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

2. Upload the files of web application.

The image displays three sequential screenshots of the AWS S3 Management Console, illustrating the upload process of a file set to a bucket named 'prasad-website' in the 'eu-north-1' region.

Top Screenshot: Upload Page

The 'Upload' page shows instructions for uploading files and folders. The 'Files and folders' section is empty, indicating no files have been selected for upload.

Middle Screenshot: Files Selected

The 'Files and folders' section now displays 24 files and folders, totaling 89.5 KB. The files are listed in a table with columns for Name, Folder, Type, and Size.

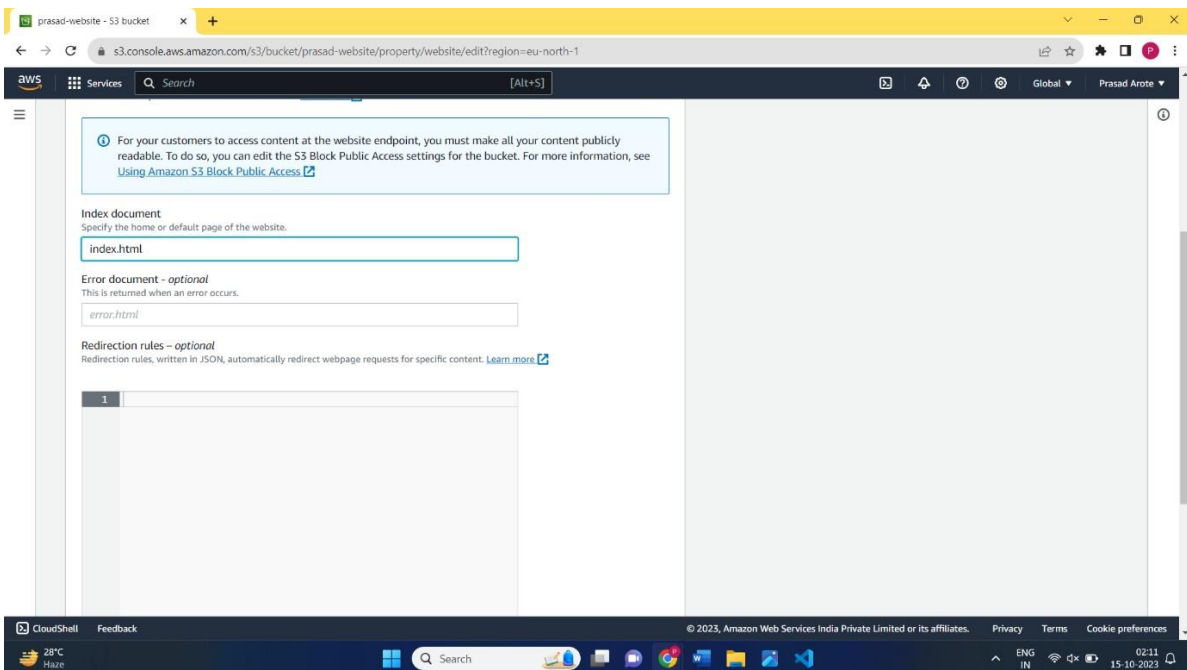
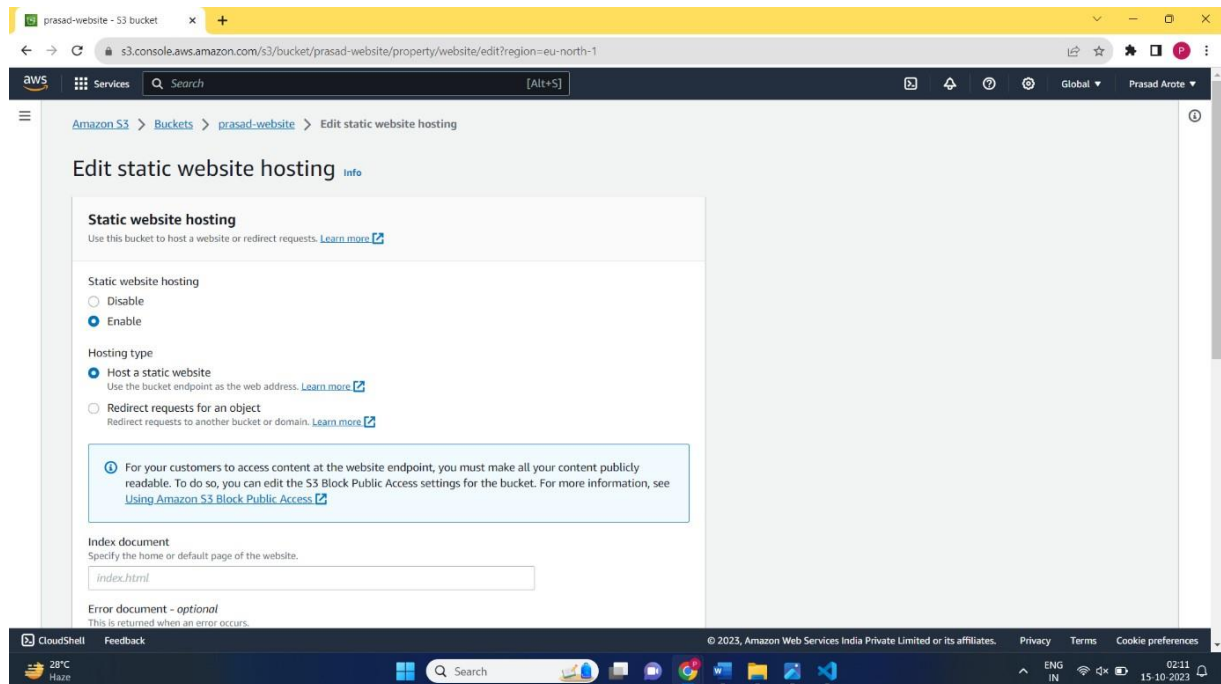
Name	Folder	Type	Size
Bun 1.svg	-	image/svg+xml	865.0 B
Bun 1@2x.png	-	image/png	8.6 KB
Cheese.svg	-	image/svg+xml	619.0 B
Cheese@2x.png	-	image/png	1.4 KB
Lettuce.svg	-	image/svg+xml	629.0 B
Lettuce@2x.png	-	image/png	2.4 KB
Onion.svg	-	image/svg+xml	831.0 B
Onion@2x.png	-	image/png	2.8 KB
Patty.svg	-	image/svg+xml	639.0 B
Patty@2x.png	-	image/png	3.9 KB

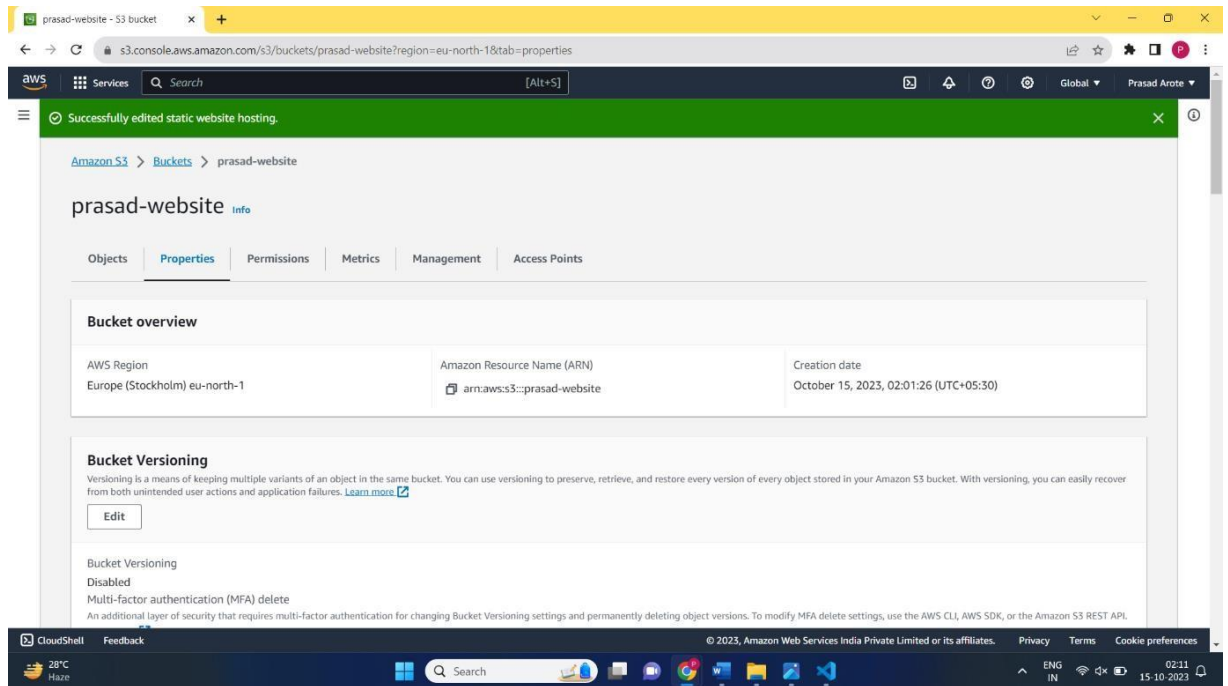
Bottom Screenshot: Upload Succeeded

The 'Upload: status' page shows the upload was successful. The 'Summary' section indicates that 24 files (89.5 KB) were successfully uploaded (100.00%) and 0 files (0 B) failed (0%).

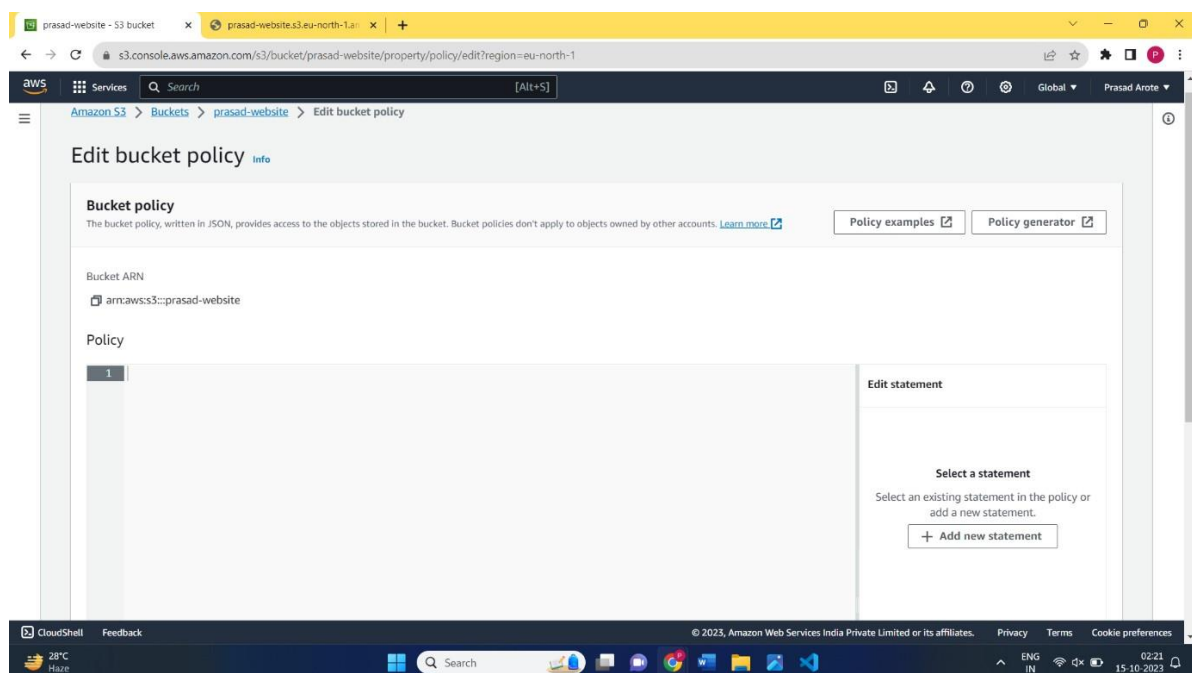
The 'Files and folders' section shows the same list of 24 files and folders, confirming the successful upload.

3. Enable Static website hosting





5. Change the Bucket Policy




AWS

prasad-website.s3.eu-north-1.amazonaws.com

+

logen.h



AW5 Policy Generator

Step 1 : Select Policy *type

Step 2: Add Statement(s)

Enter a description of a single permission.

Allow

Deny

Service

Amazon S3

Use a comma to separate multiple values.

Use multiple statements to add permissions for more than one service.

Amazon Resource Name (ARN)

Add Statement

Add Conditions (optional)

Add Statement

Generate Policy

Start Over

An amazon.com company

The image shows a screenshot of a Windows desktop with two browser windows open. The top window is the AWS Policy Generator tool, and the bottom window is the AWS console.

AWS Policy Generator Window:

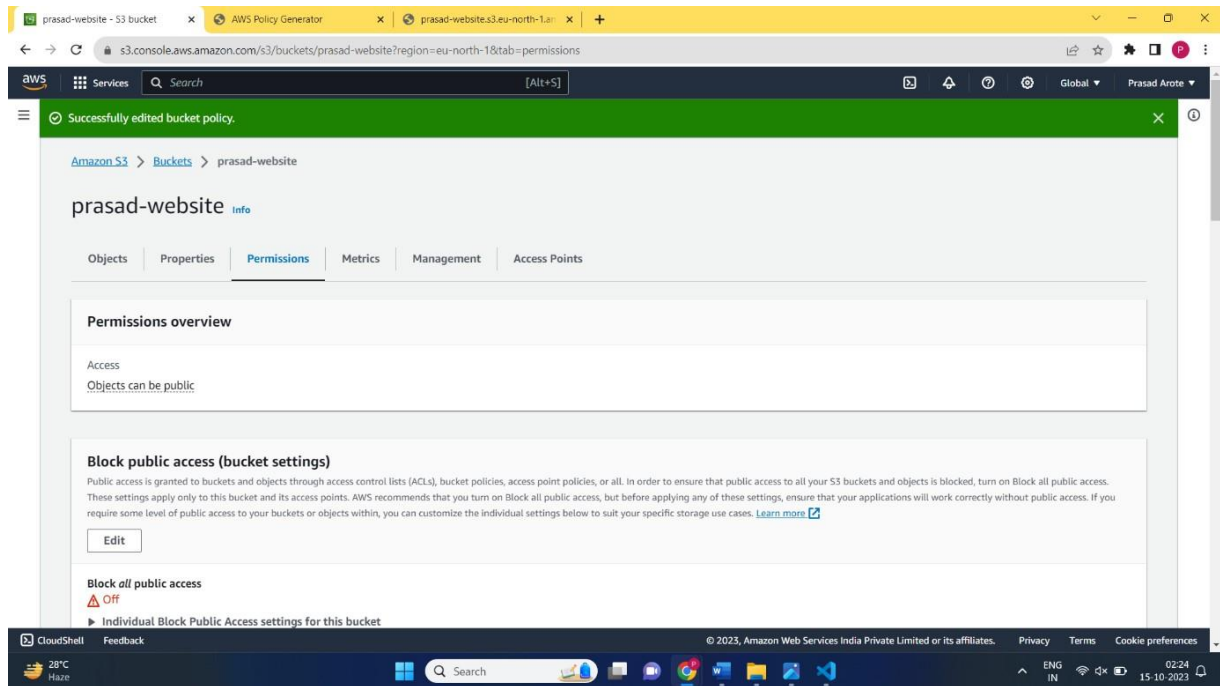
- URL: `awspolicygen.s3.amazonaws.com/policygen.html`
- Service: Amazon S3
- Actions: Select Actions --
- A modal window titled "Policy JSON Document" is open, displaying the following JSON:

```
{
  "Id": "Policy1697316791653",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1697316788348",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::prasad-website",
      "Principal": "*"
    }
  ]
}
```

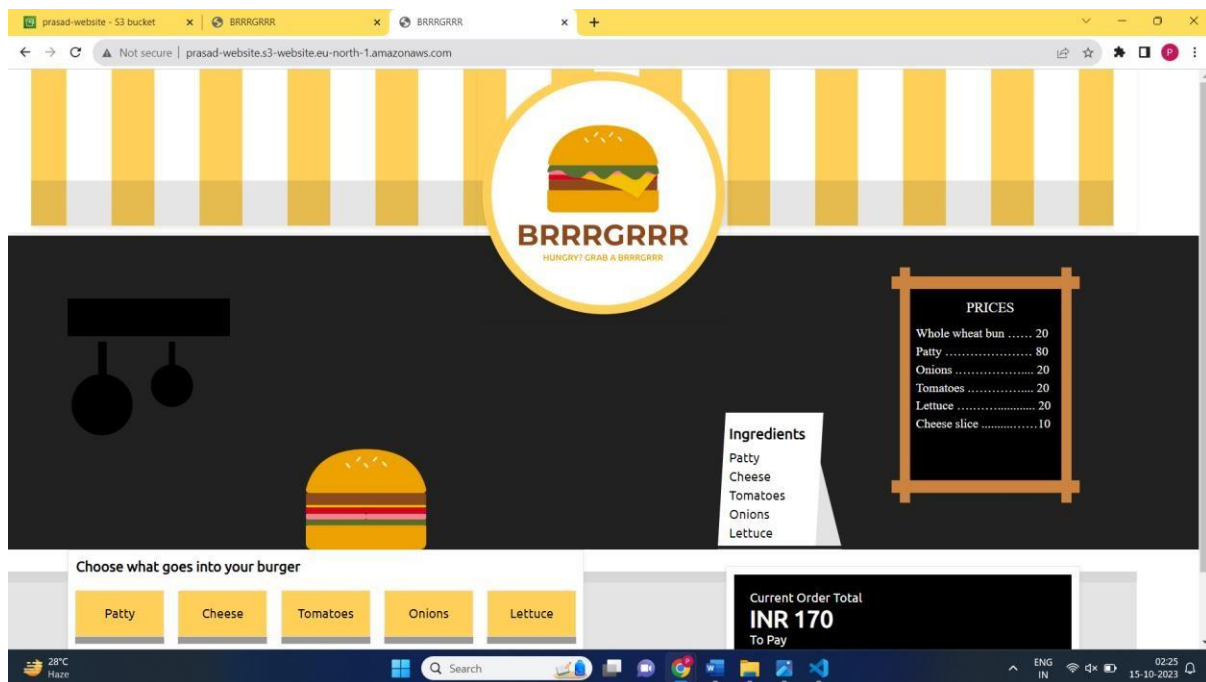
AWS Console Window:

- URL: `s3.console.aws.amazon.com/s3/bucket/prasad-website/property/policy/edit?region=eu-north-1`
- Page Title: Policy
- The policy document is displayed in a text area, matching the JSON from the generator.
- On the right, there is an "Edit statement" section with a "Select a statement" prompt and an "Add new statement" button.

The Windows taskbar at the bottom shows the date and time as 02:23 on 15-10-2023, and the system temperature as 28°C.



6. Now open the link (given in the bucket below) in browser and you can see the static website hosted.



CONCLUSION:

Here we studied to host a static website on S3 bucket.

