A Report

❖ Introduction

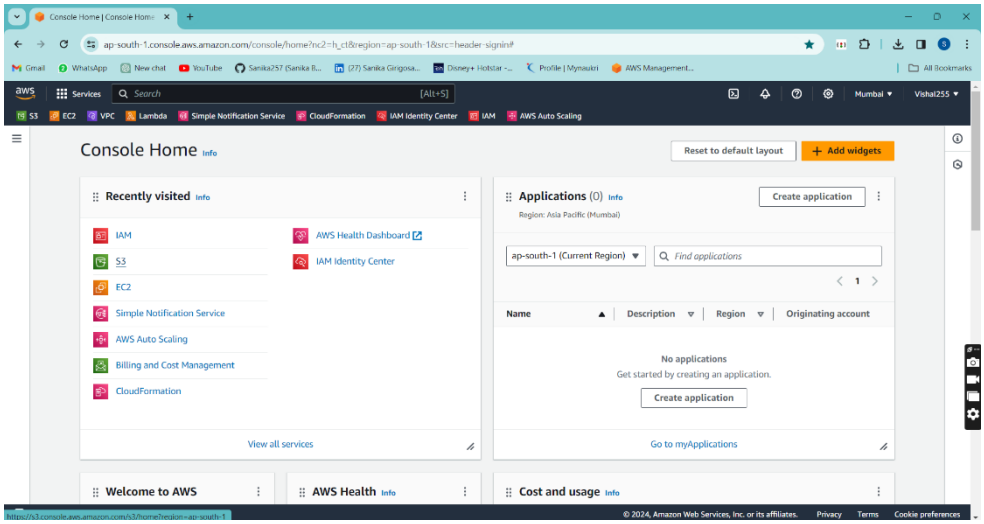
Amazon S3, a scalable object storage service, provides a cost-effective solution for hosting static content, such as HTML, CSS, and image files. Initiated the project by creating a new Amazon S3 bucket, and by configured the necessary settings to enable website hosting for the bucket. Used a Simple HTML CSS Code to craft the simple portfolio website. S3 bucket to serve as a web hosting platform, Uploaded the developed portfolio website files. Files to the S3 Bucket. And After completion of the task Create a GitHub repository named "Techplement." Upload a dedicated folder within the repository named "week1-tasks."

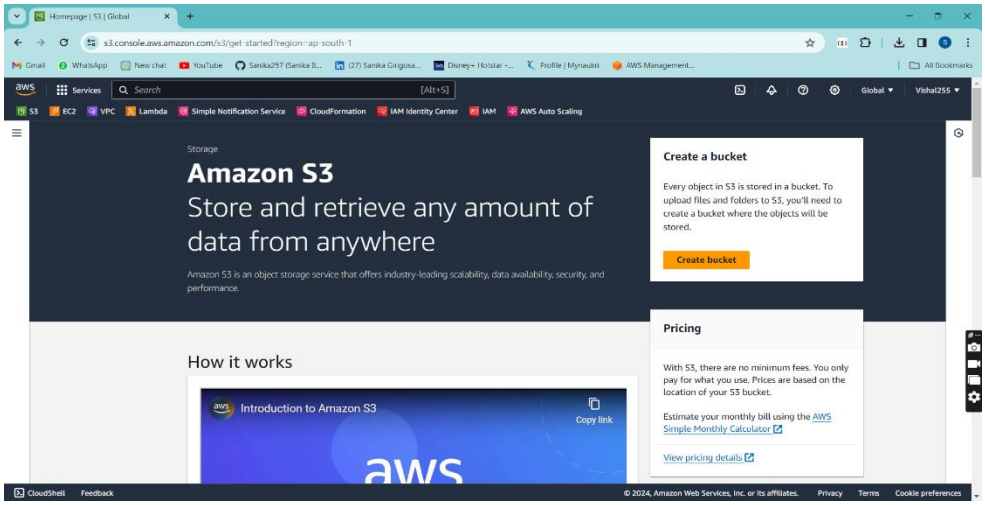
❖ Workflow of the task

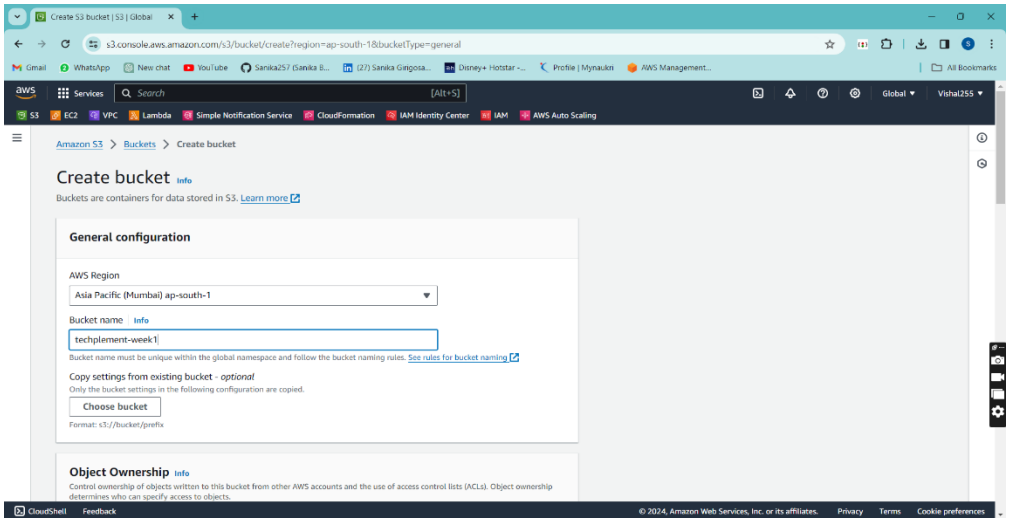
1.Login to the AWS Console

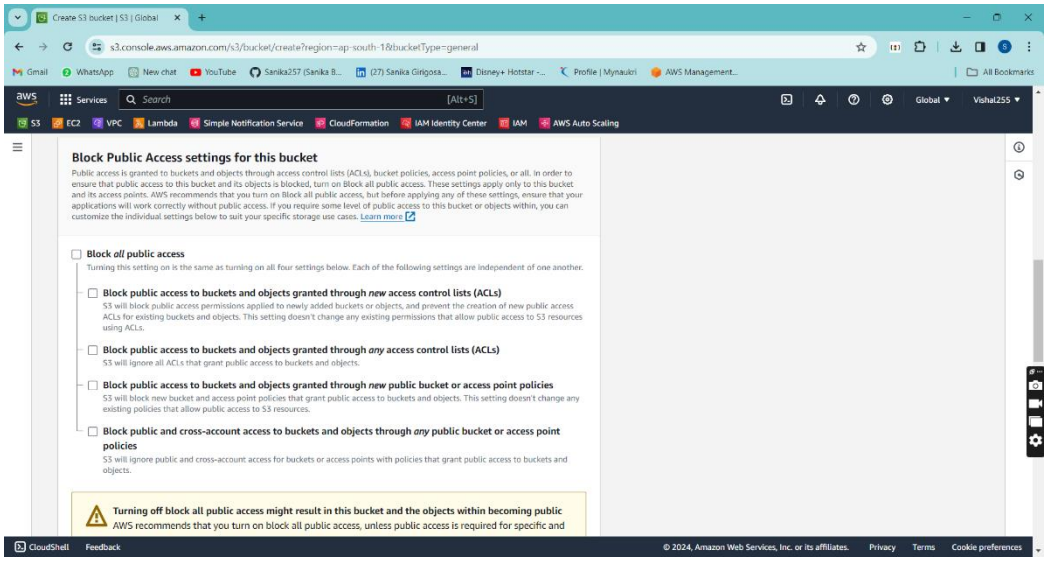
2.Then go the S3 Bucket

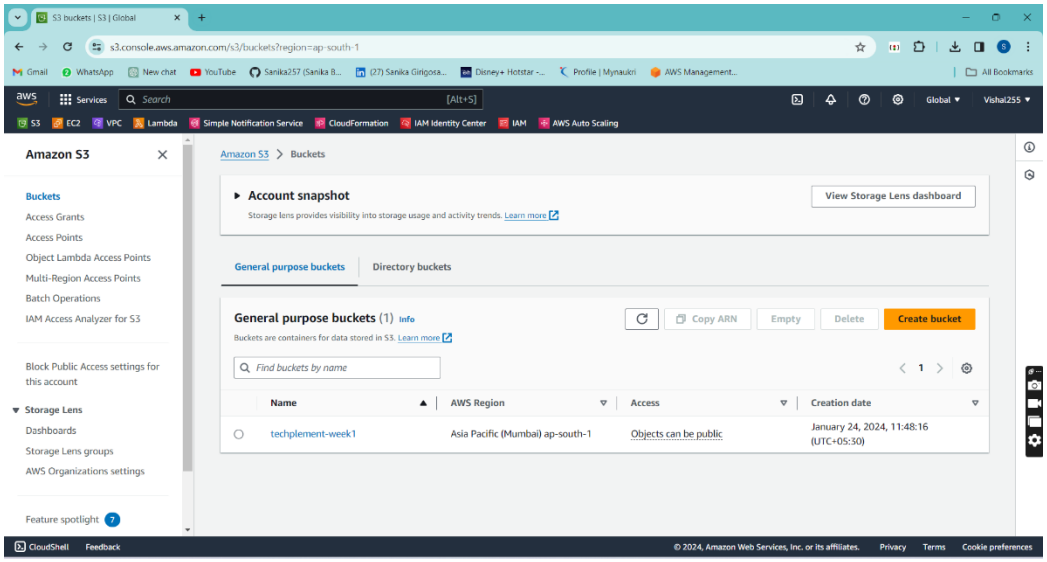
3.Then Create Bucket with name “techplement-week1” and then Configure the bucket and uncheck the block public access.



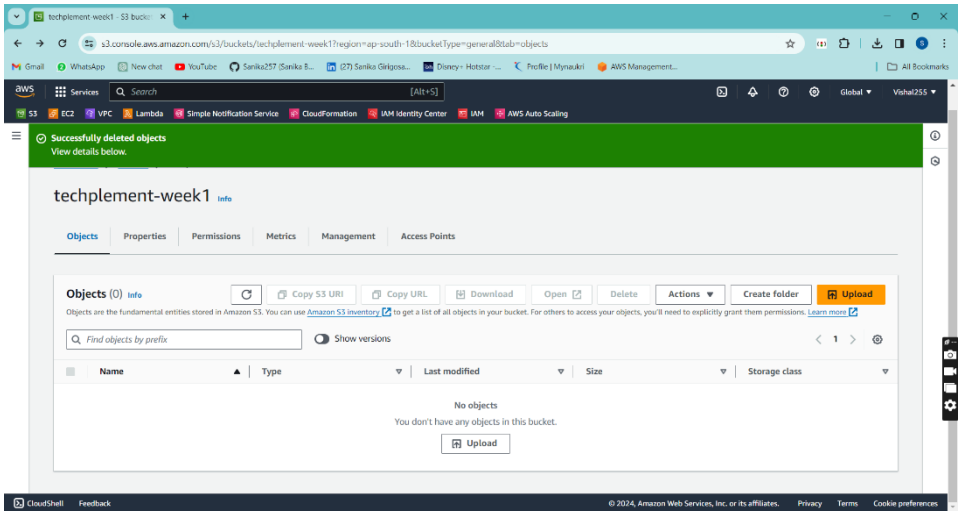


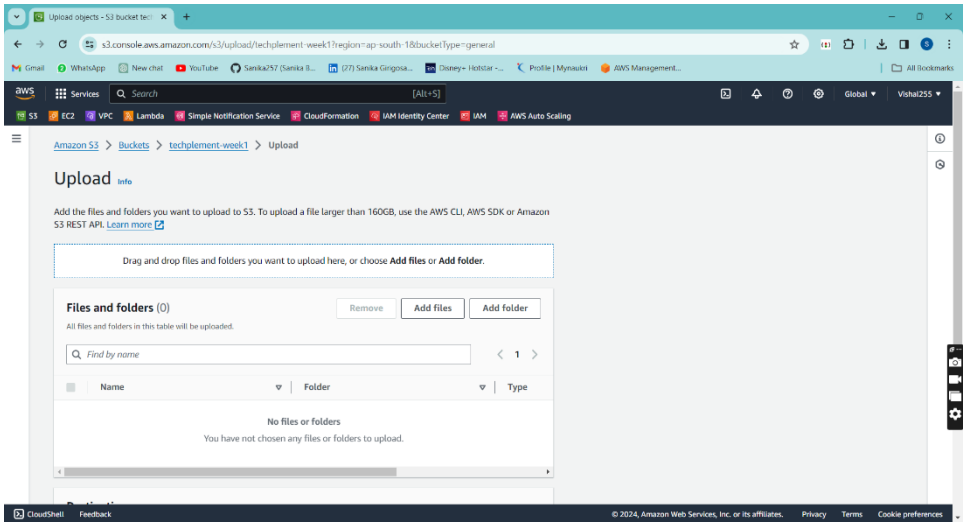

Create S3 bucket | S3 | Global
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3. Learn more
General configuration
AWS Region
Asia Pacific (Mumbai) ap-south-1
Bucket name Info
techplement-week1
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.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

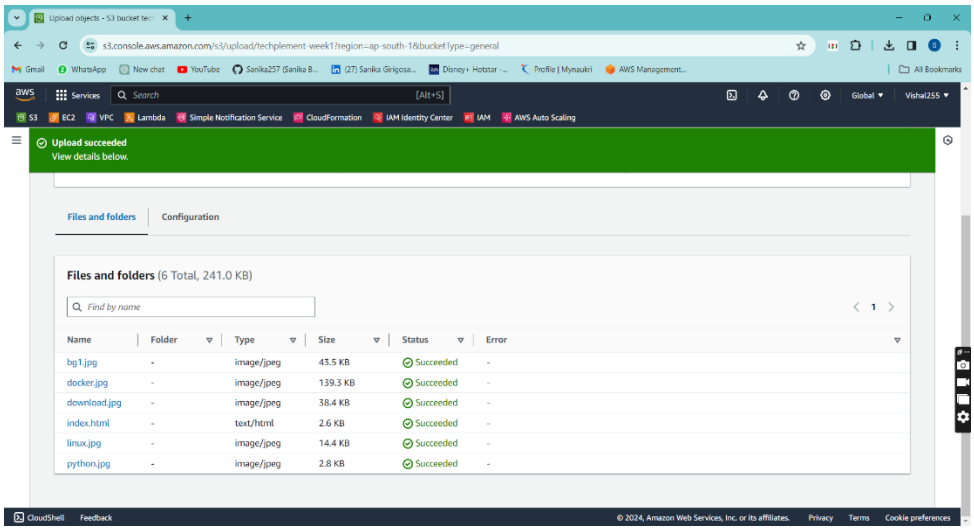

Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


S3 buckets | S3 | Global
s3.console.aws.amazon.com/s3/buckets?region=ap-south-1
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
techplement-week1
Asia Pacific (Mumbai) ap-south-1
Objects can be public
January 24, 2024, 11:48:16 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

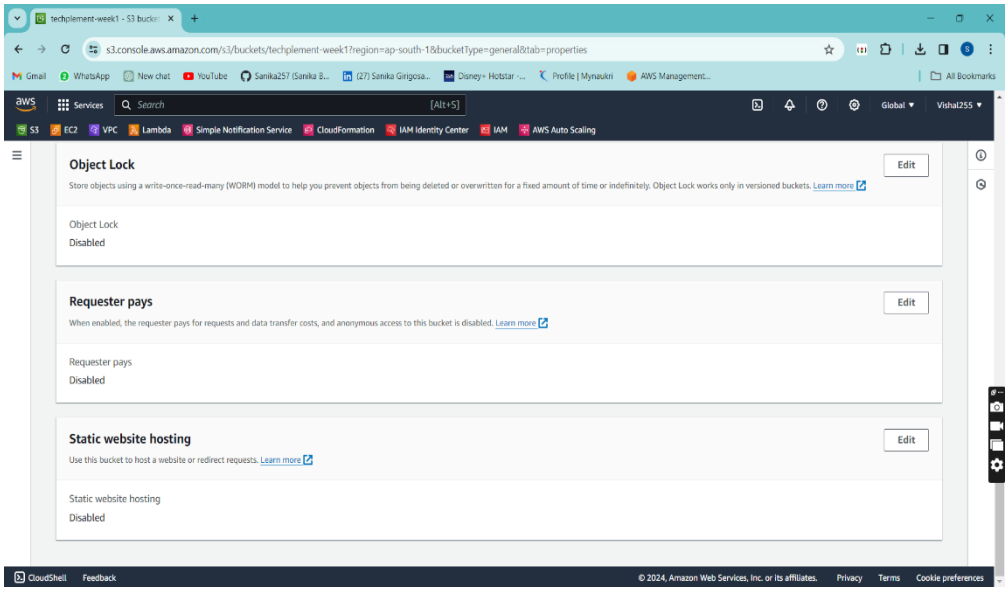
4.Click on bucket then upload the required files in the bucket.

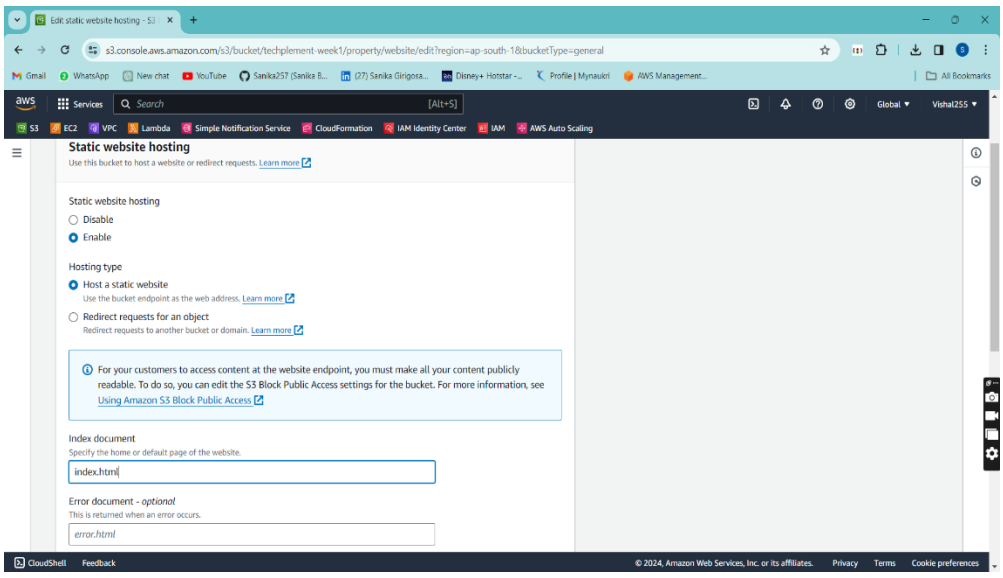


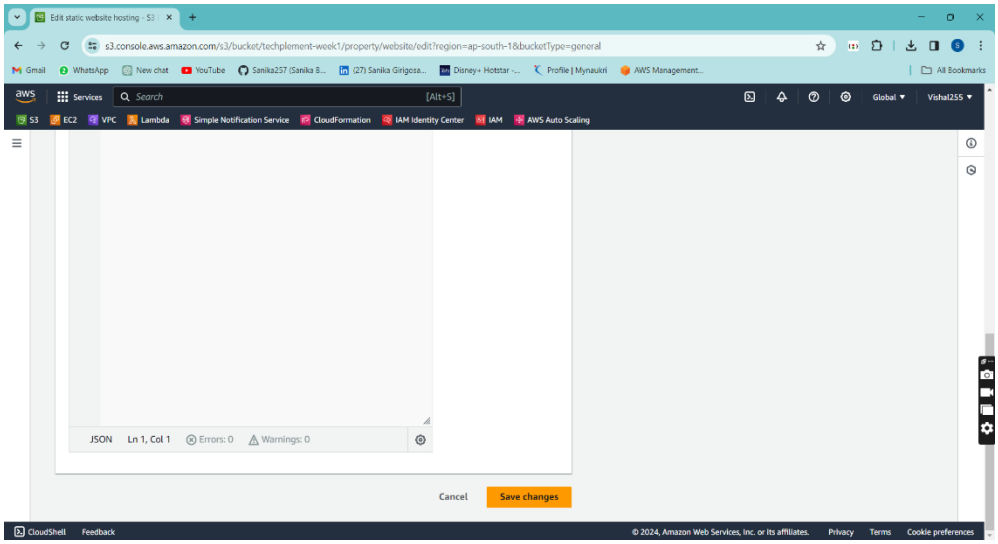




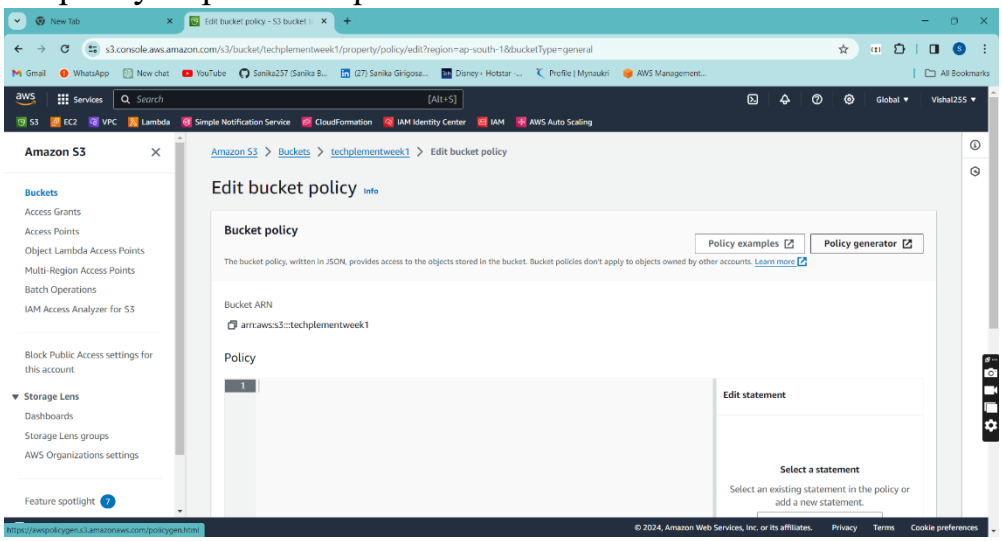
5.Then go the properties and enable the static web hosting with name of website **index.html** and click on save changes.

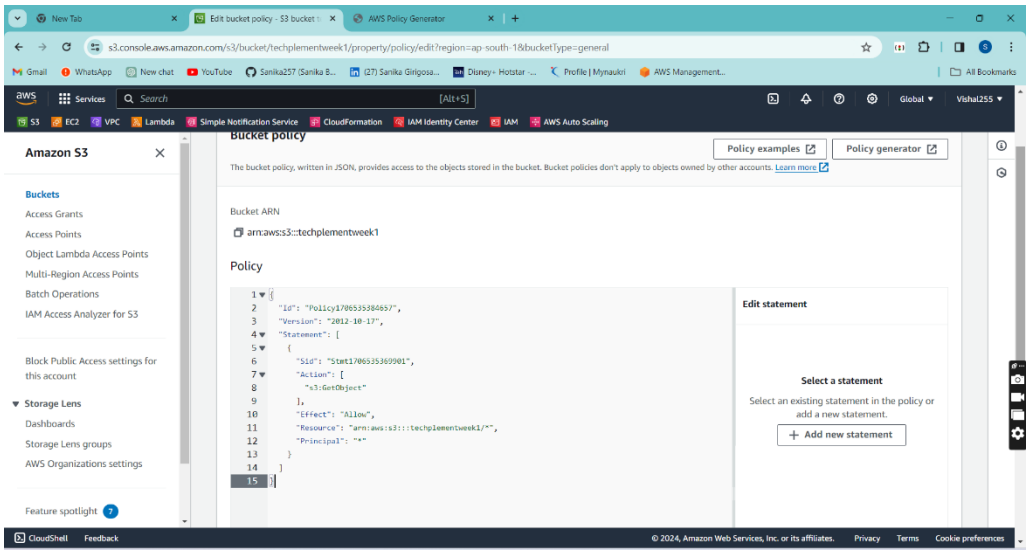




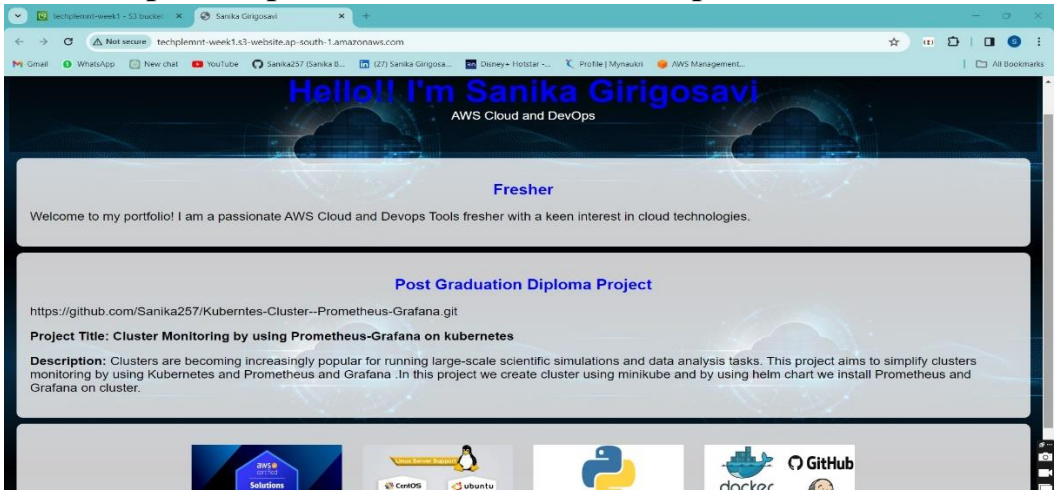


6. To host and get access to website we need to create bucket policy.
For that go the **Permissions** and click on edit of **bucket policy** and configure the policy as per the requirement.





7. Then go to Static Web hosting and click on the website. It will get the website that we want to host.
Link: http://techplemnt-week1.s3-website.ap-south-1.amazonaws.com



❖ Resources and Reference

- AWS S3 Documentation to get guidance about S3 bucket and creating policy for it.
- Amazon web Services Console used to use S3 service and host website.
- W3school and GeeksforGeeks is valuable resource for HTML and CSS , development of webpage.

❖ Conclusion

This project has been a good experience, allowing me to apply theoretical knowledge to practical scenarios. I am grateful for the opportunity and look forward to further challenges that contribute to my growth in the AWS Cloud Environment.