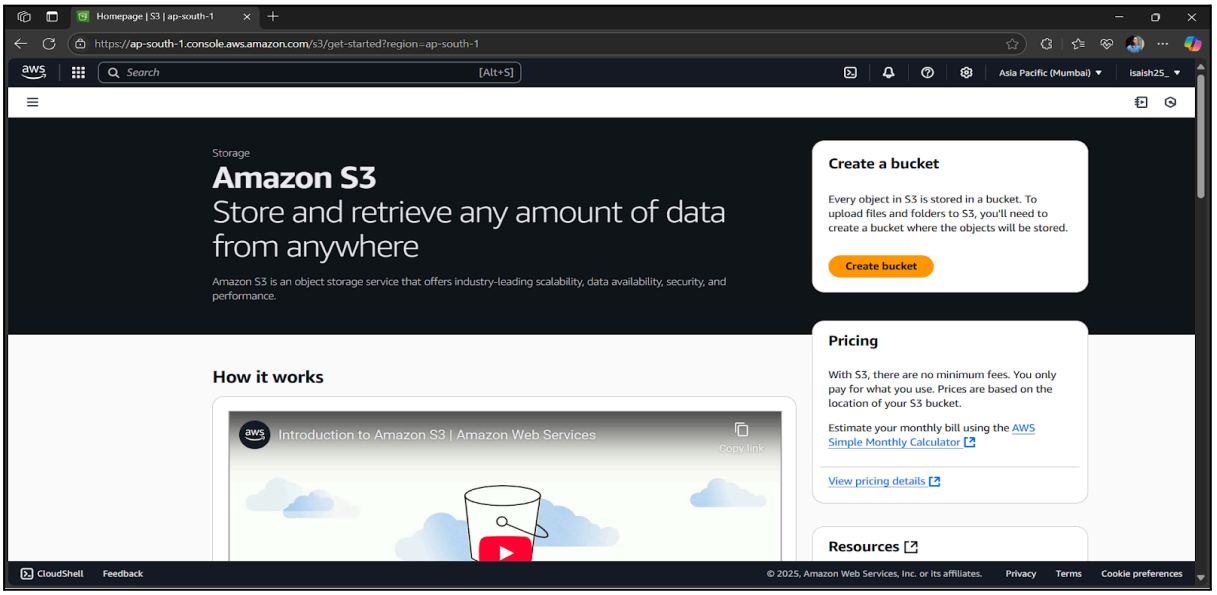
Week-3 Securing Cloud Storage

Name- Saish Dhiwar
PRN- 2124UCSM2011
Email- saish.dhiwar_24ucs@sanjivani.edu.in

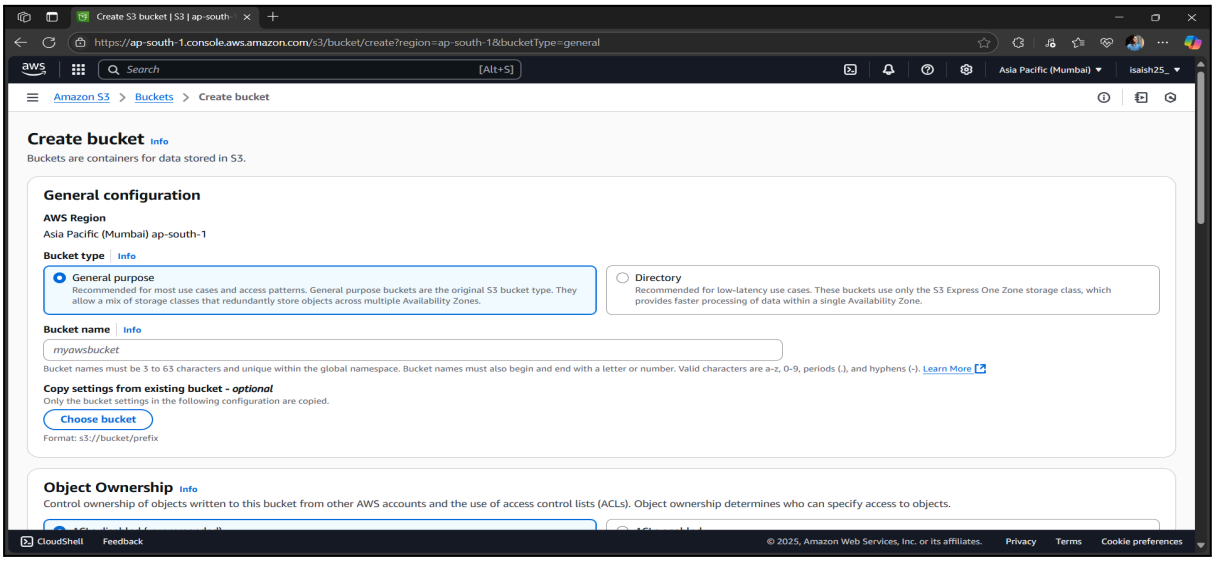
Task- 1) Set up an S3 bucket.
2) Apply access control policies.
3) Document security configurations.

Task 1- Steps to Set Up an S3 Bucket-

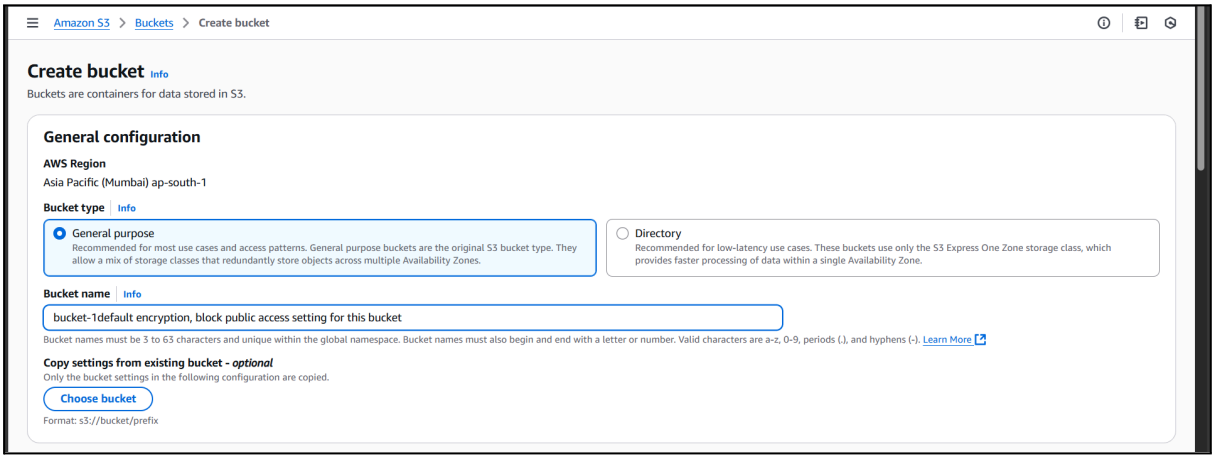
1) Logged in to the AWS Console.
2) Search S3 and then click.



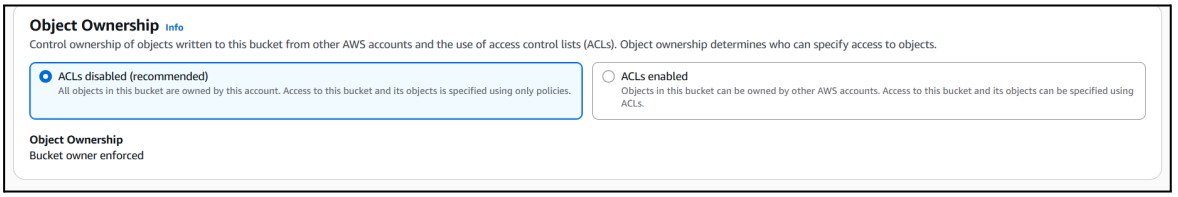
3) Then click Create bucket Options.



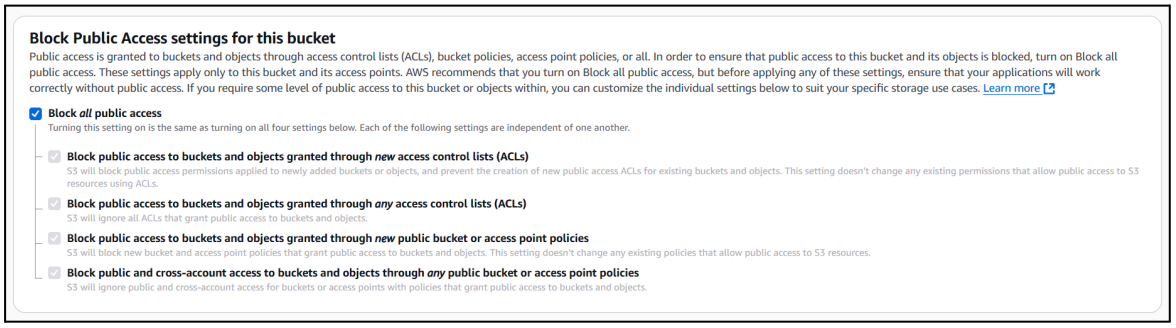
4) Enter the Bucket name and select the Bucket type.



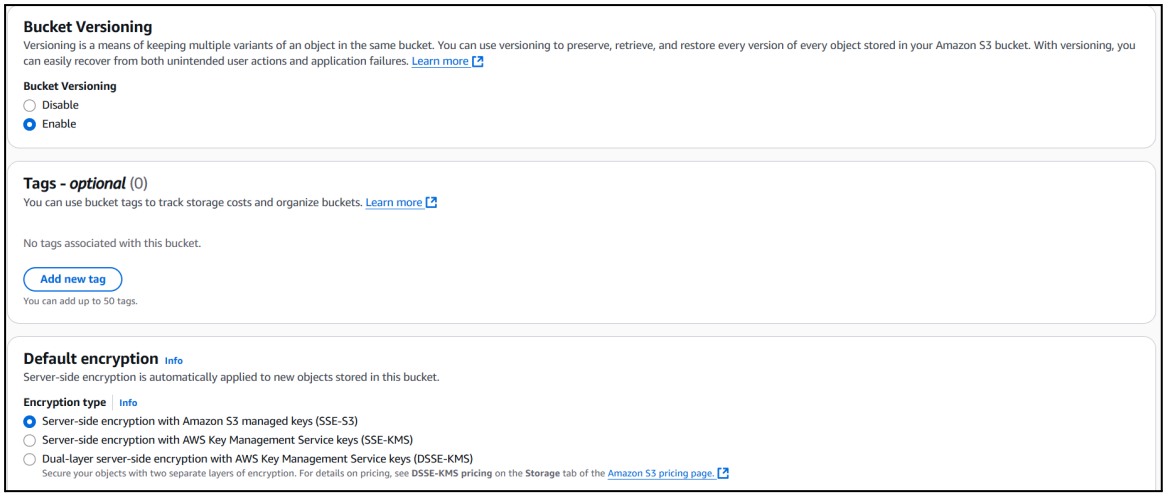
5) Select the Object Ownership.



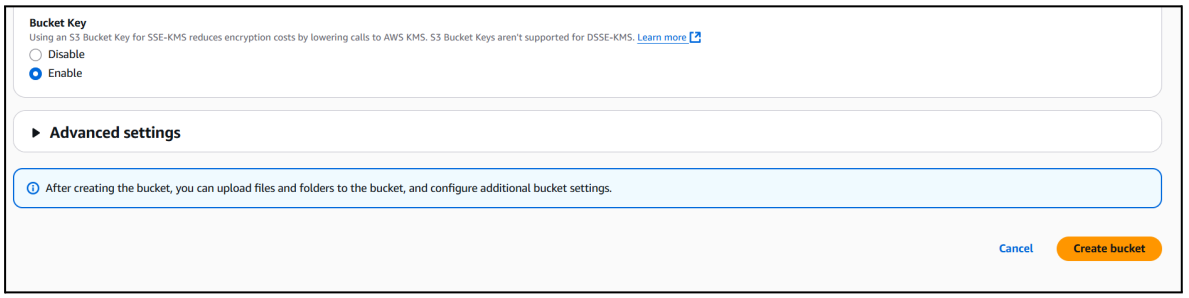
6) Block Public access setting for this bucket.



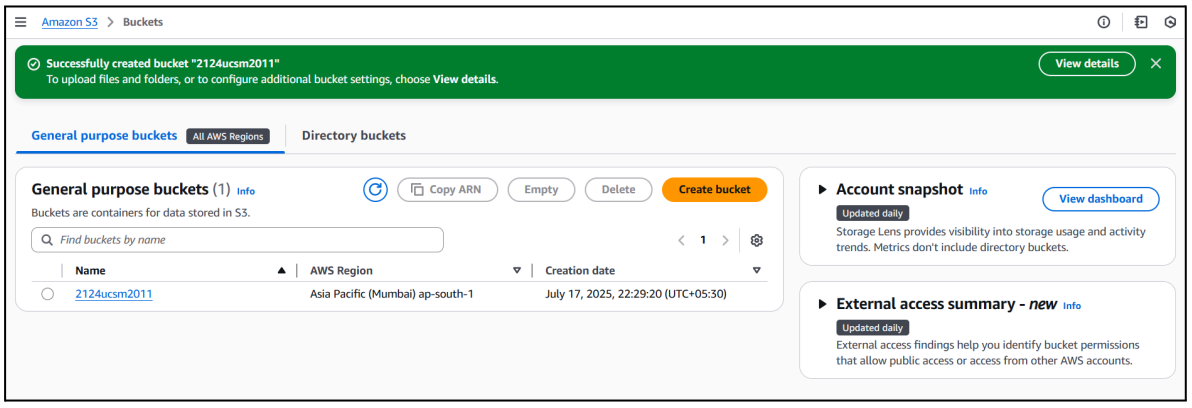
7) Select Bucket versioning Enable, and then select Default encryption server-side encryption with Amazon S3 managed key(SSE-S3).



8) Select Bucket key Enable, and then click the create bucket button.

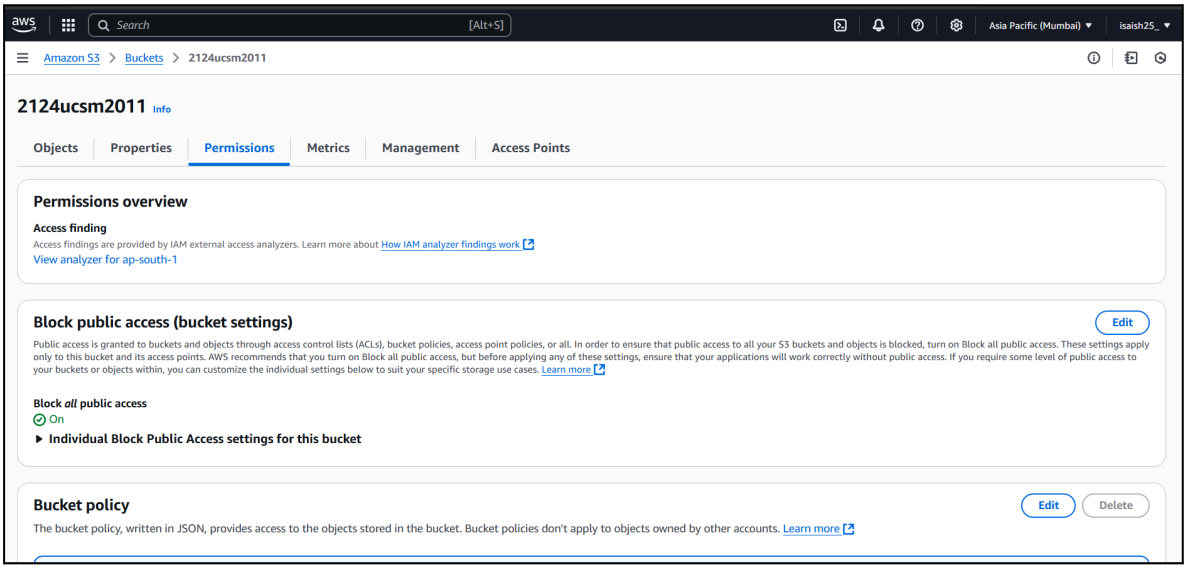


9) Bucket Successfully Created.

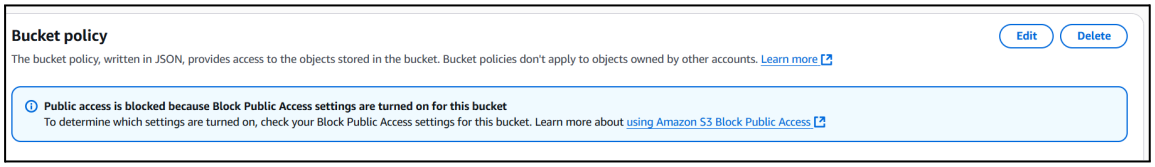


Task 2- Steps to Apply Access Control Policies-

1) Open S3 > Bucket > 2124ucsm2011 > Permission.



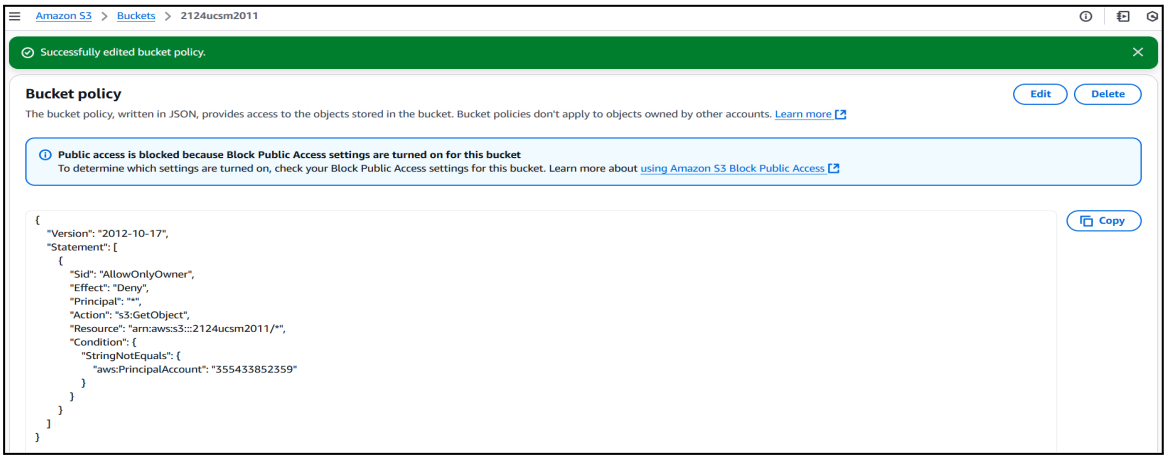
2) Scroll down and Click Edit.

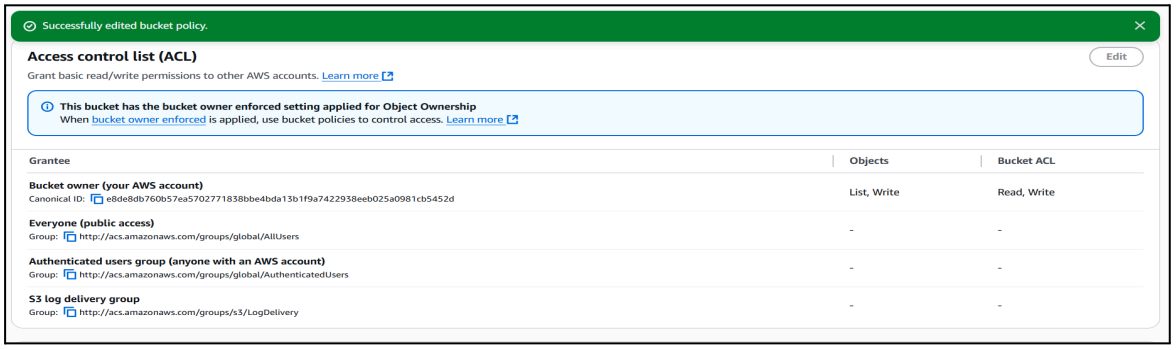


3) Then write the following code to block public access, and save the policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyOwner",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::2124ucsm2011/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "355433852359"
        }
      }
    }
  ]
}
```

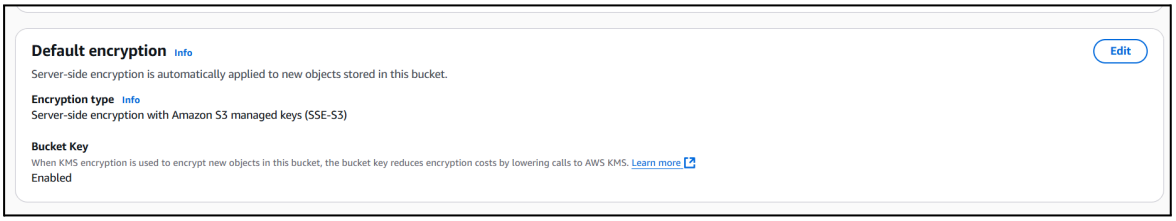
4) Save the policy → Now, only the bucket owner's account can access the objects. All other access is denied.



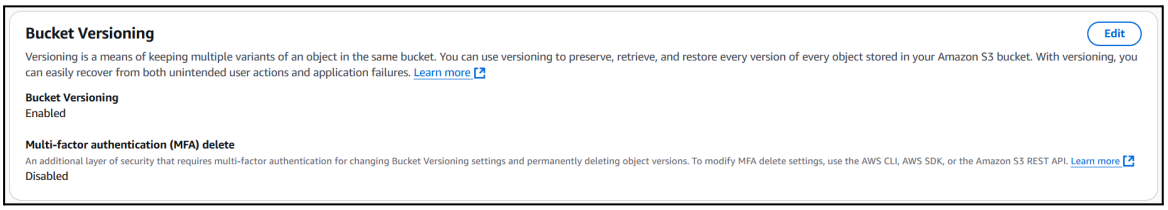


Task 3- Document security configurations.

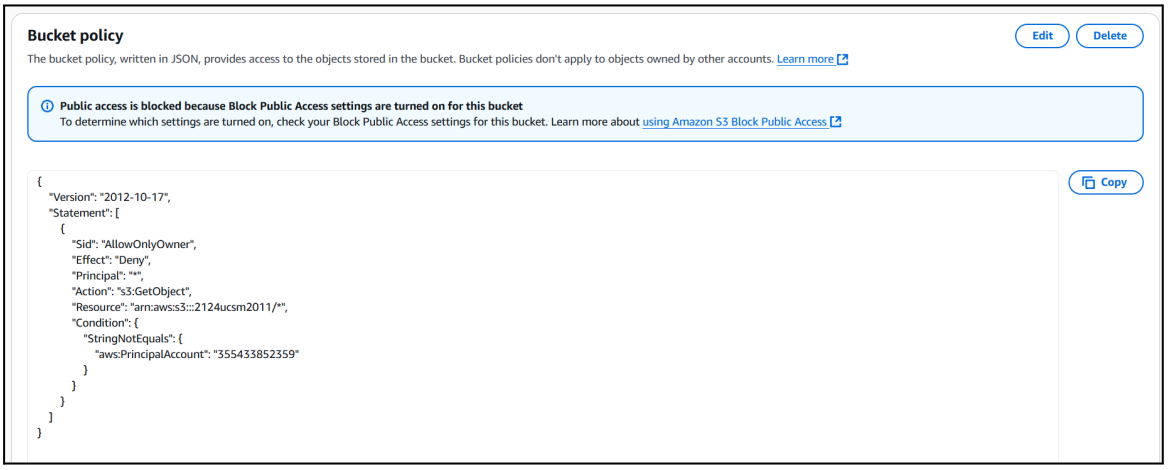
1) Default encryption with Amazon S3 managed keys (SSE-S3) is enabled to protect all objects by default.



2) Versioning is enabled to keep all versions of objects for recovery and rollback.



3) Access policy restricts object access to only the bucket owner's account.



4) Public access is blocked using AWS's Block Public Access settings for added security.