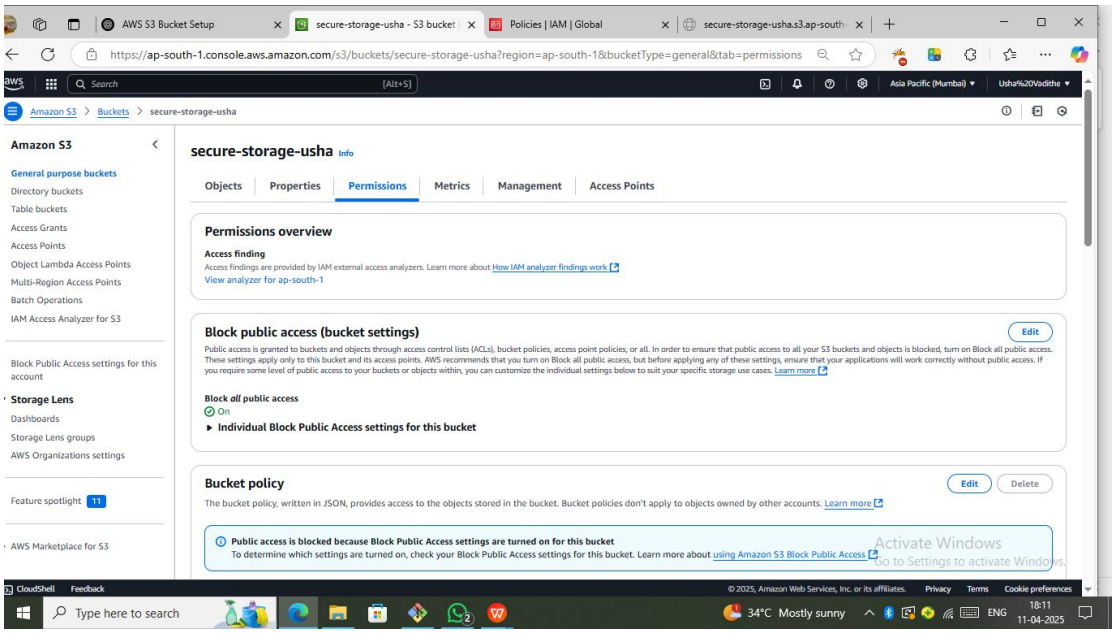
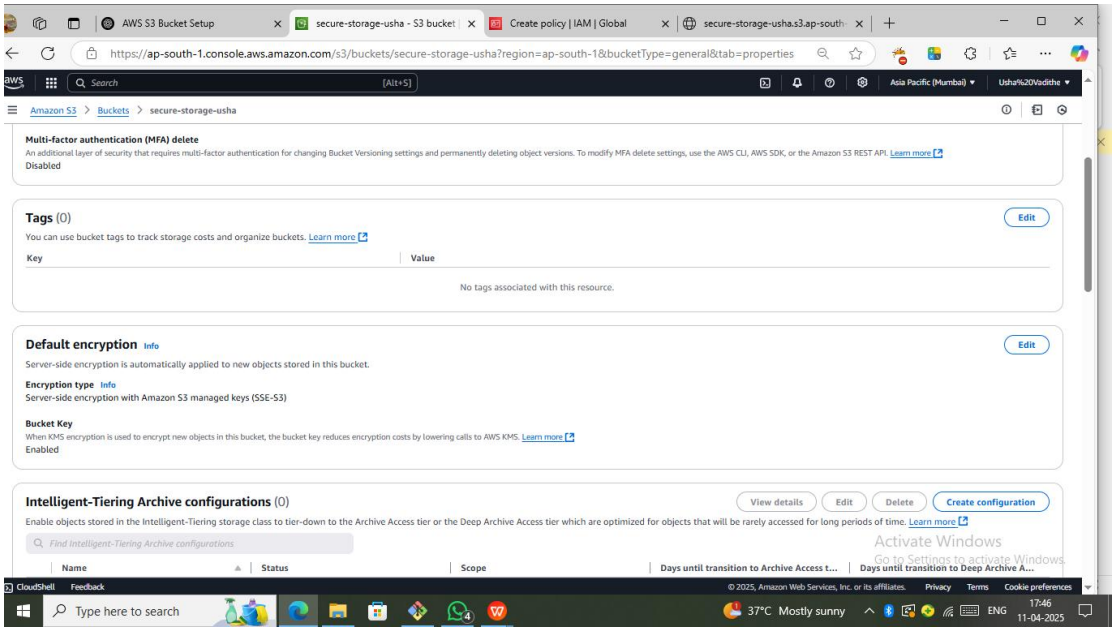
NAME:VADITHE USHA BAI
TASK: Cloud Security – IAM Policies, Secure Storage, and Data Encryption
Platform used: Amazon Web Services (AWS)

STEPS PERFORMED:

1. Created a Secure S3 Bucket
   Bucket name: secure-storage-usha
   Region: Asia Pacific (Mumbai)
   Blocked all public access to ensure data was private by default

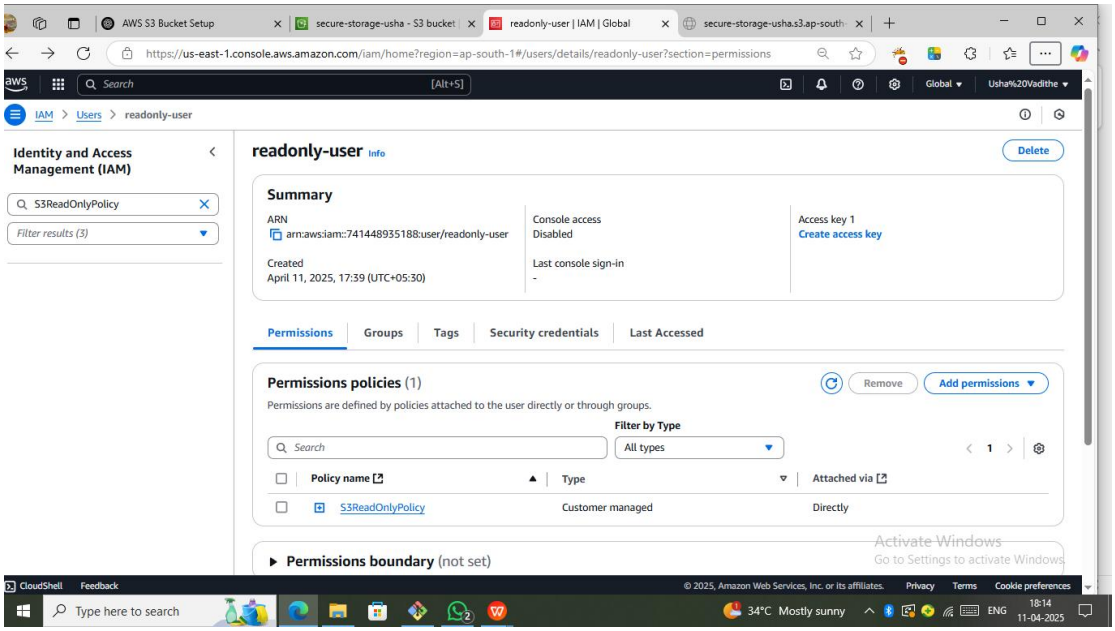


2. Enabled Encryption
   Enabled **Default Encryption** using **SSE-S3 (Amazon S3-managed keys)**
   Verified that all uploaded objects are encrypted automatically

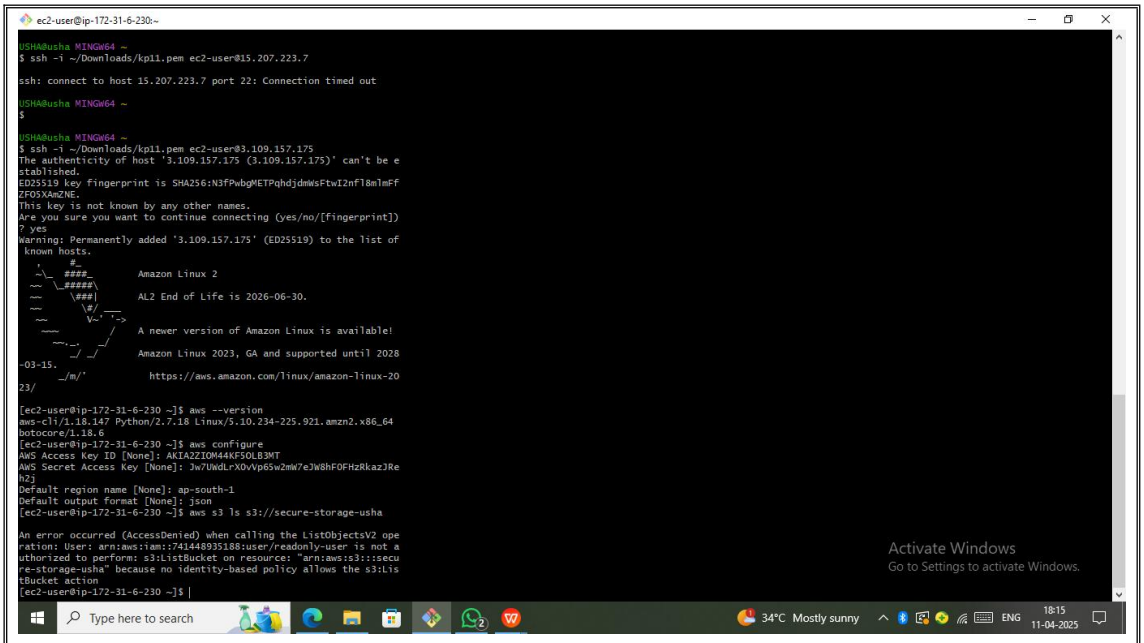


3. Created a Custom IAM Policy
Policy name: S3ReadOnlyPolicy
Allowed the following actions:
s3:GetObject – to read/download objects
JSON Policy:

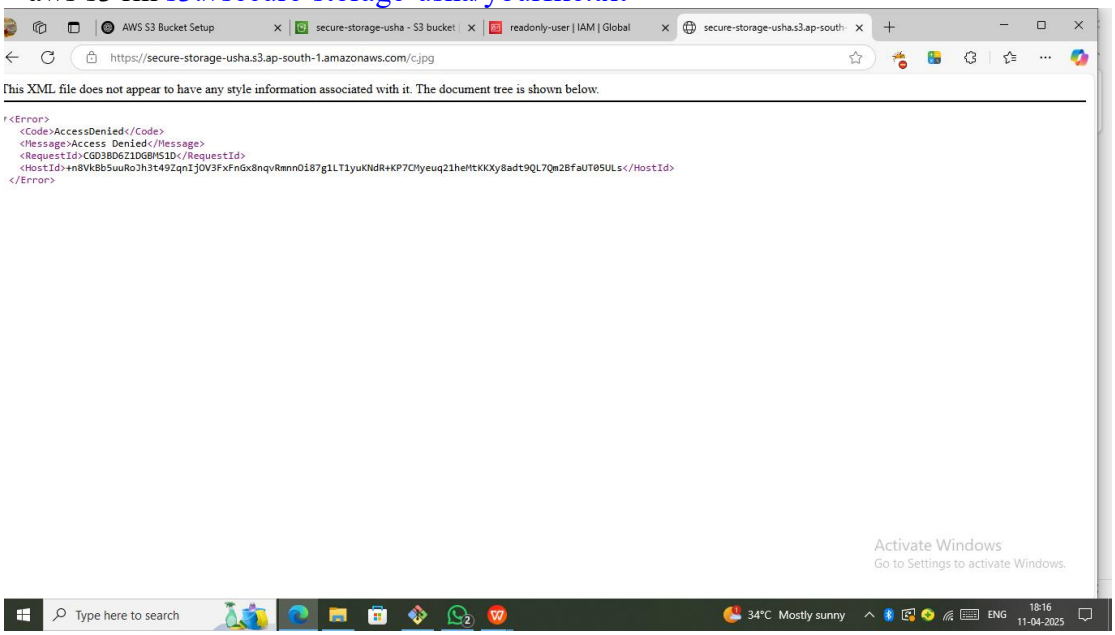
```
{
 "Version": "2012-10-17",
 "Statement": [
   {
    "Effect": "Allow",
    "Action": ["s3:GetObject"],
    "Resource": "arn:aws:s3:::secure-storage-usha/*"
   },
   {
    "Effect": "Allow",
    "Action": ["s3:ListBucket"],
    "Resource": "arn:aws:s3:::secure-storage-usha"
   }
 ]
}
```



4. Created a Secure IAM User
Username: readonly-user
Granted **programmatic access**
Attached S3ReadOnlyPolicy during creation
Downloaded **Access Key ID** and **Secret Access Key** for CLI testing



5. Tested Permissions Using AWS CLI
   Configured AWS CLI using readonly-user credentials on EC2
   Ran the following tests:
   aws s3 ls s3://secure-storage-usha
   aws s3 rm s3://secure-storage-usha/yourfile.txt



Conclusion:

Successfully implemented secure cloud storage using IAM policies for access control Server-side encryption (SSE-S3) Verified that access is correctly restricted to read-only for specific users