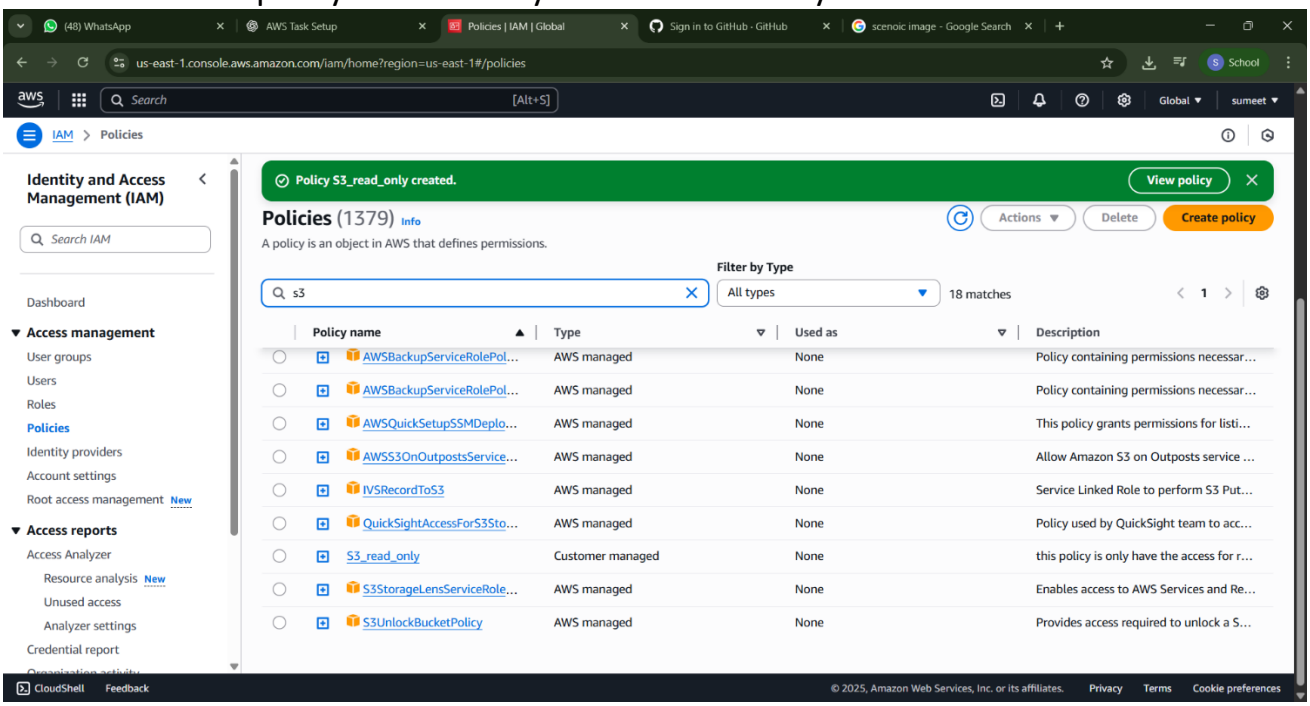
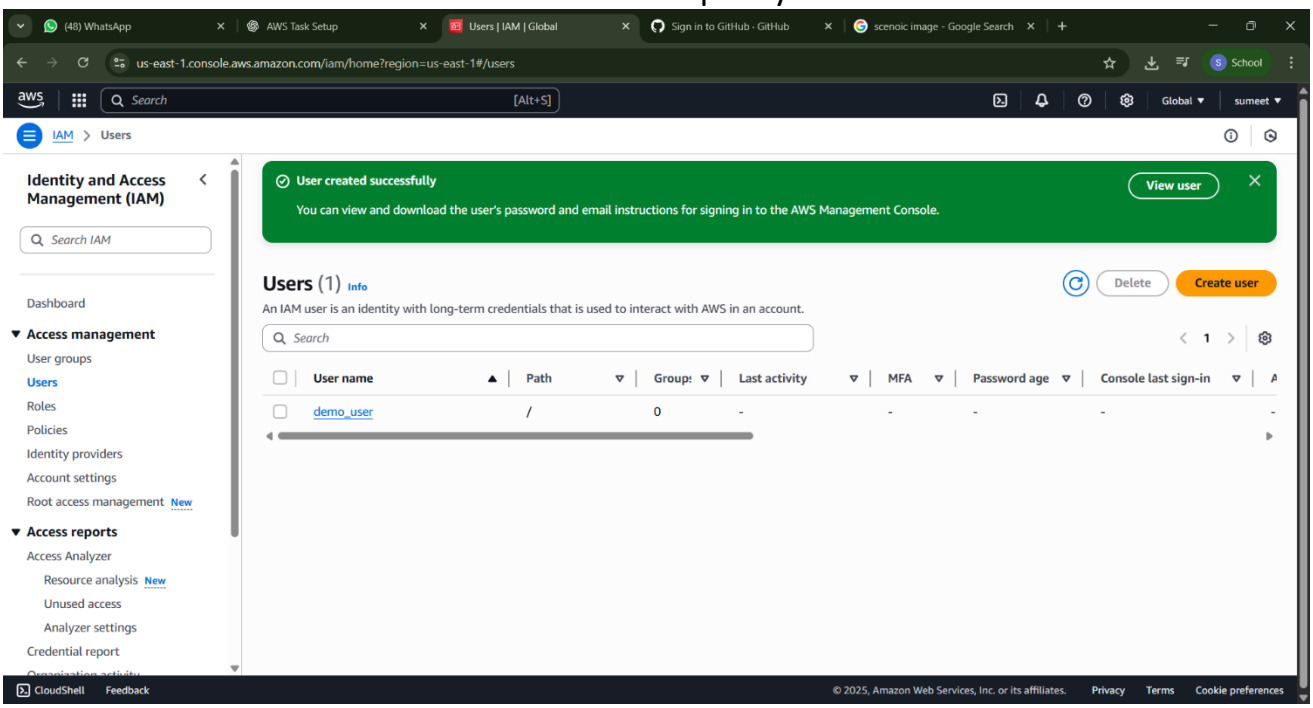
Task4: CLOUD SECURITY IMPLEMENTATION

AIM: IMPLEMENT IAM POLICIES, SECURE STORAGE, AND DATA ENCRYPTION ON A CLOUD PLATFORM.

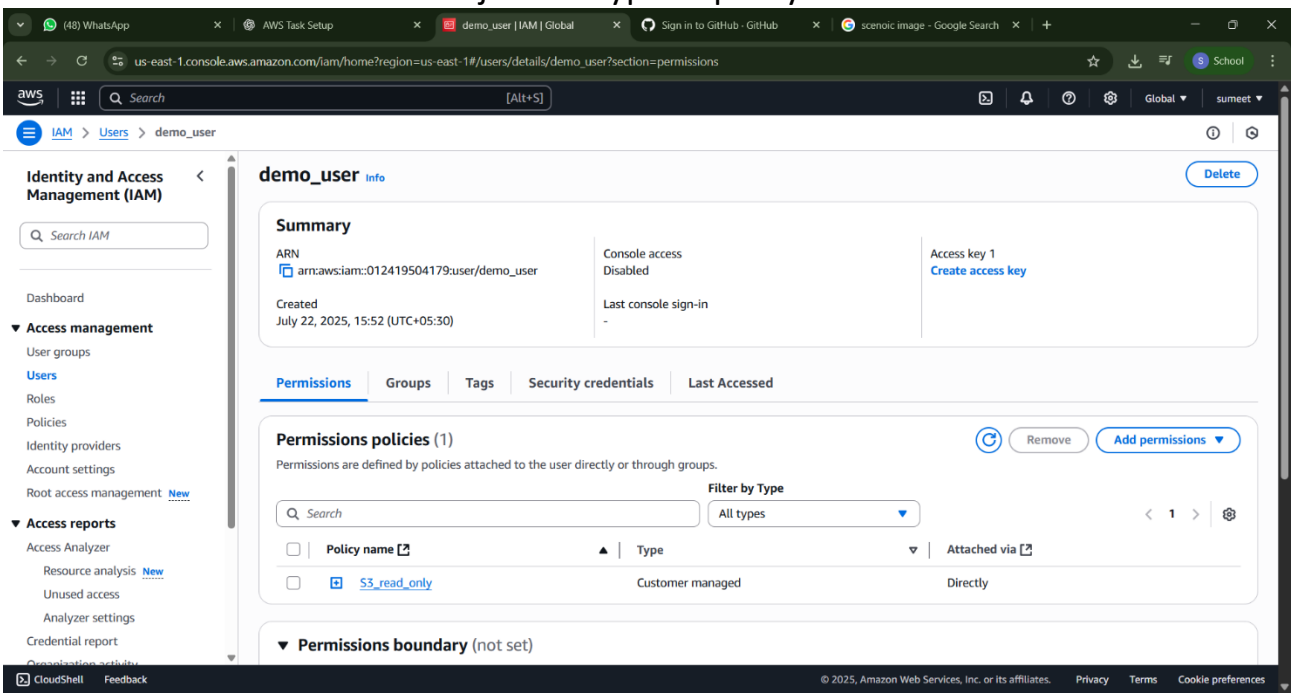
- Created a policy that the only it has S3 read only access



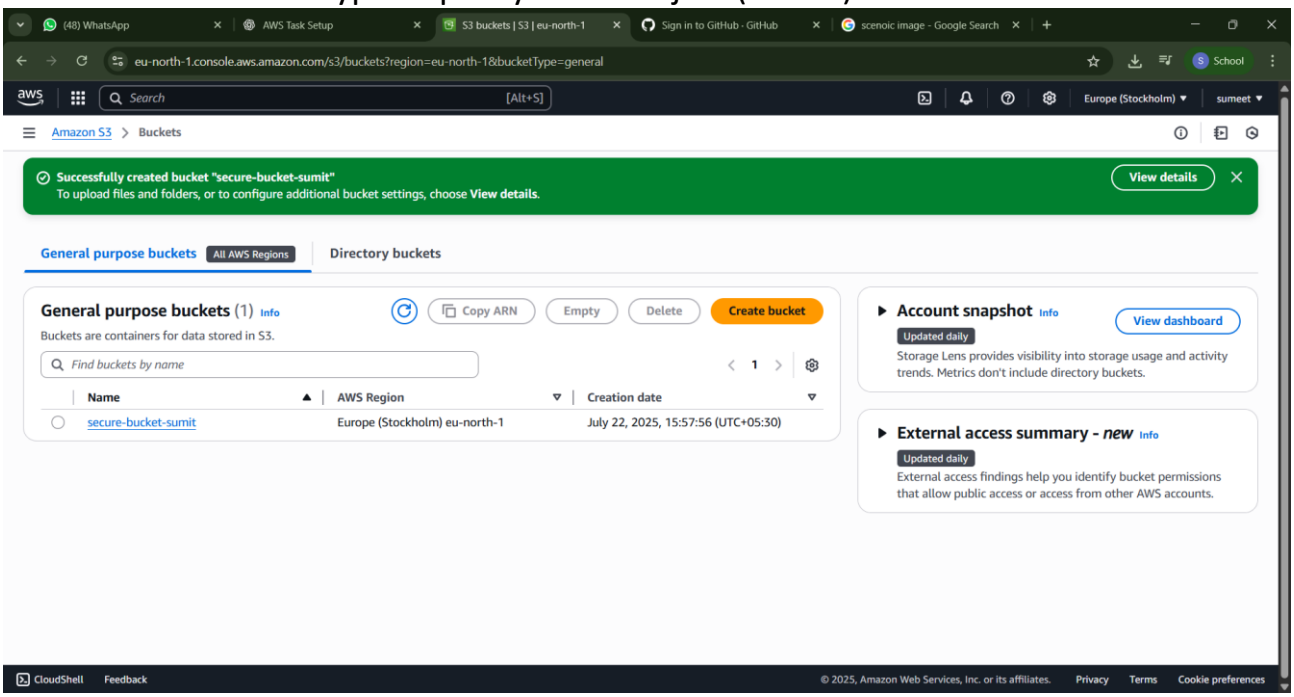
- Created a user and attach the above S3 policy to that user



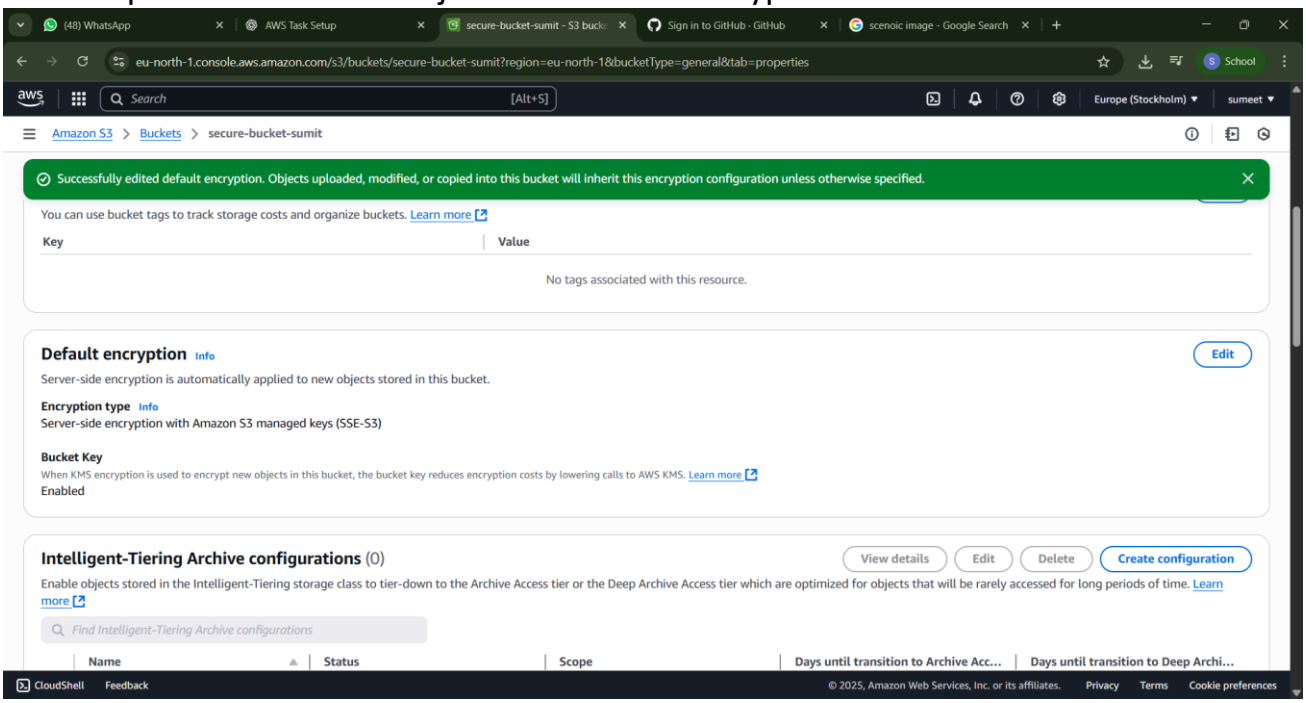
- Created a bucket with object encryption policy



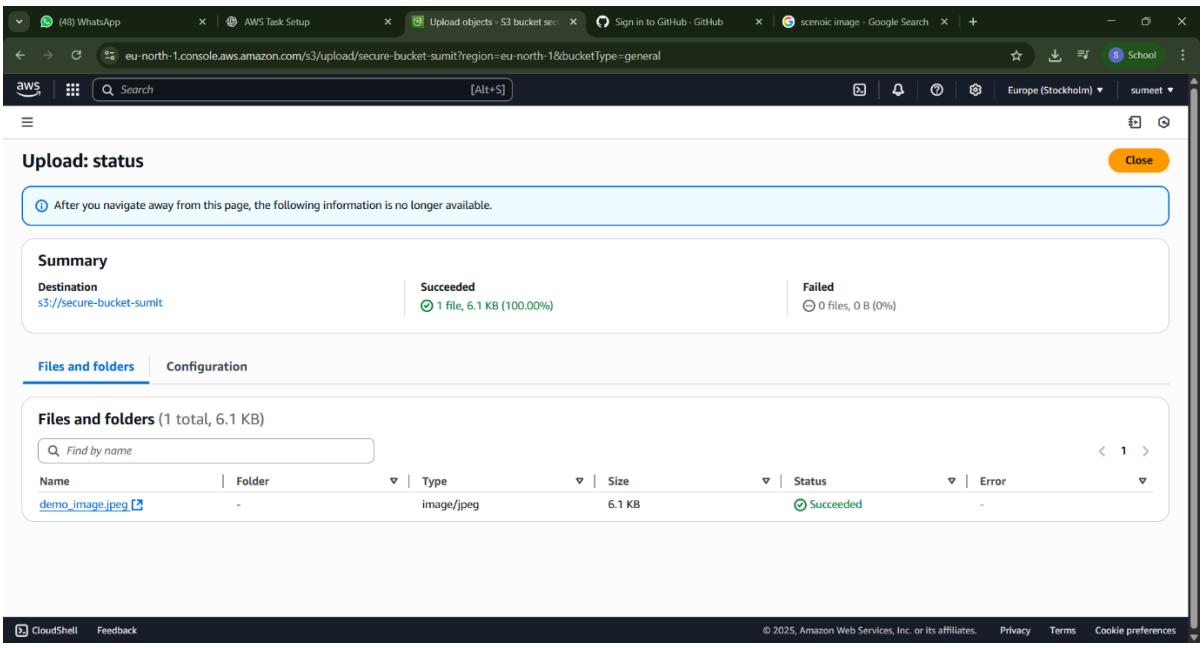
- Attach the encryption policy to the object (SSE S3)



- Uploaded an demo object with SSE S3 encryption



- **Short Description of this task:**
  Access and encryption were secured in AWS by implementing strict IAM policies that follow the principle of least privilege, ensuring only authorized users can access specific resources.
  S3 bucket public access was blocked, and object-level permissions were tightly controlled.
  To protect data at rest, default encryption was enabled using Server-Side Encryption (SSE-S3).
  For enhanced security, AWS KMS can also be used to manage encryption keys.
  These configurations ensure data is both securely stored and accessed only by verified users.


(48) WhatsApp
AWS Task Setup
Upload objects - S3 bucket sec
Sign in to GitHub · GitHub
scenoic image - Google Search
eu-north-1.console.aws.amazon.com/s3/upload/secure-bucket-sumit?region=eu-north-1&bucketType=general
School
aws
Search
[Alt+S]
Europe (Stockholm)
sumeet
Upload: status
Close
After you navigate away from this page, the following information is no longer available.
Summary
Destination
s3://secure-bucket-sumit
Succeeded
1 file, 6.1 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 6.1 KB)
Find by name
1
Name
Folder
Type
Size
Status
Error
demo_image.jpeg
-
image/jpeg
6.1 KB
Succeeded
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences