Cloud Security Implementation Report – Task 4

Organization: **CODTECH IT SOLUTIONS PVT. LTD.**

Intern Name: **Krushnakant Sonawane**

Project Title**: IAM, Secure Storage, and Encryption on AWS**

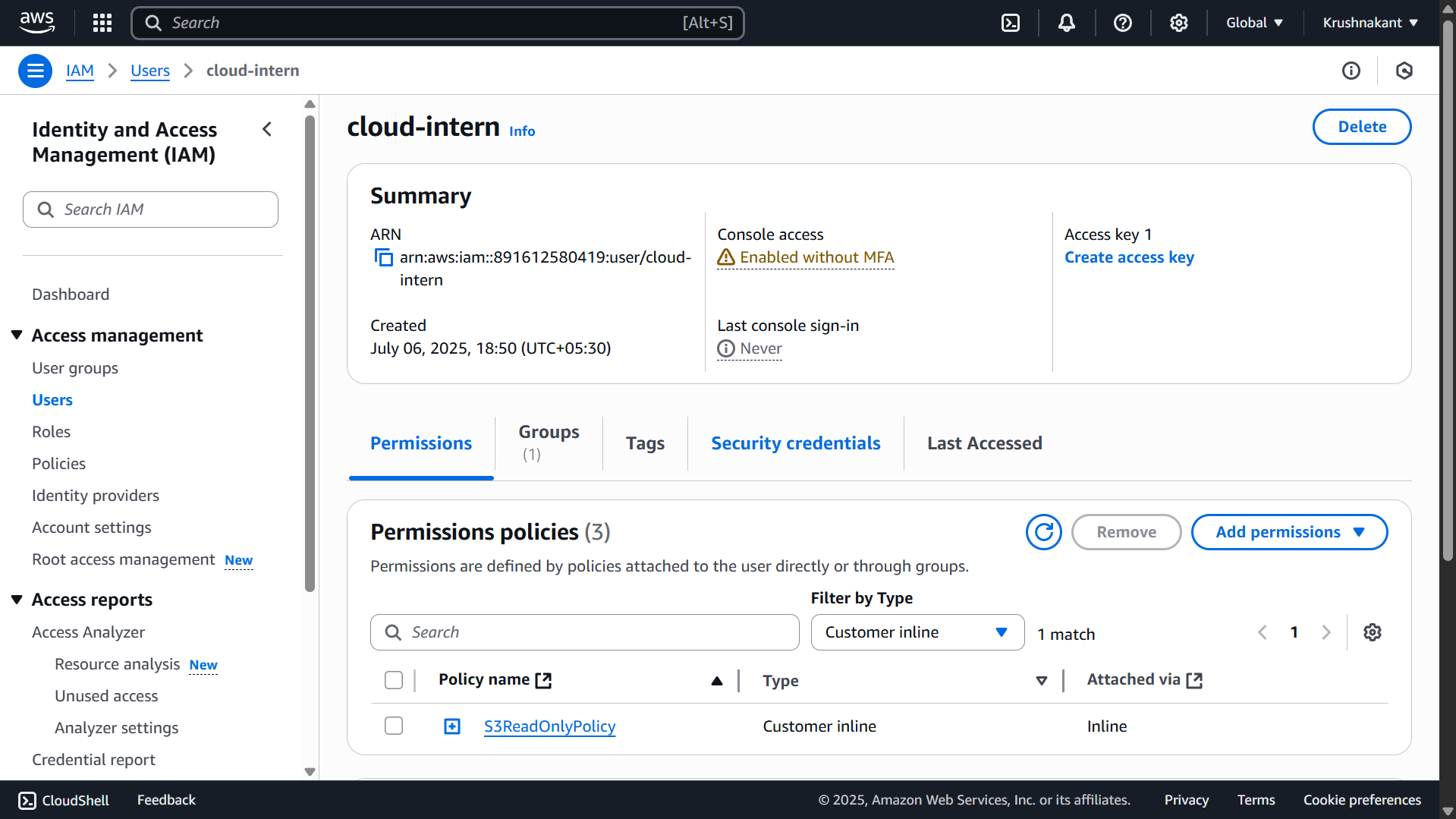
Internship Duration: May 20, 2025 – July 20, 2025

Report Date: June 26, 2025

# 1. Objective

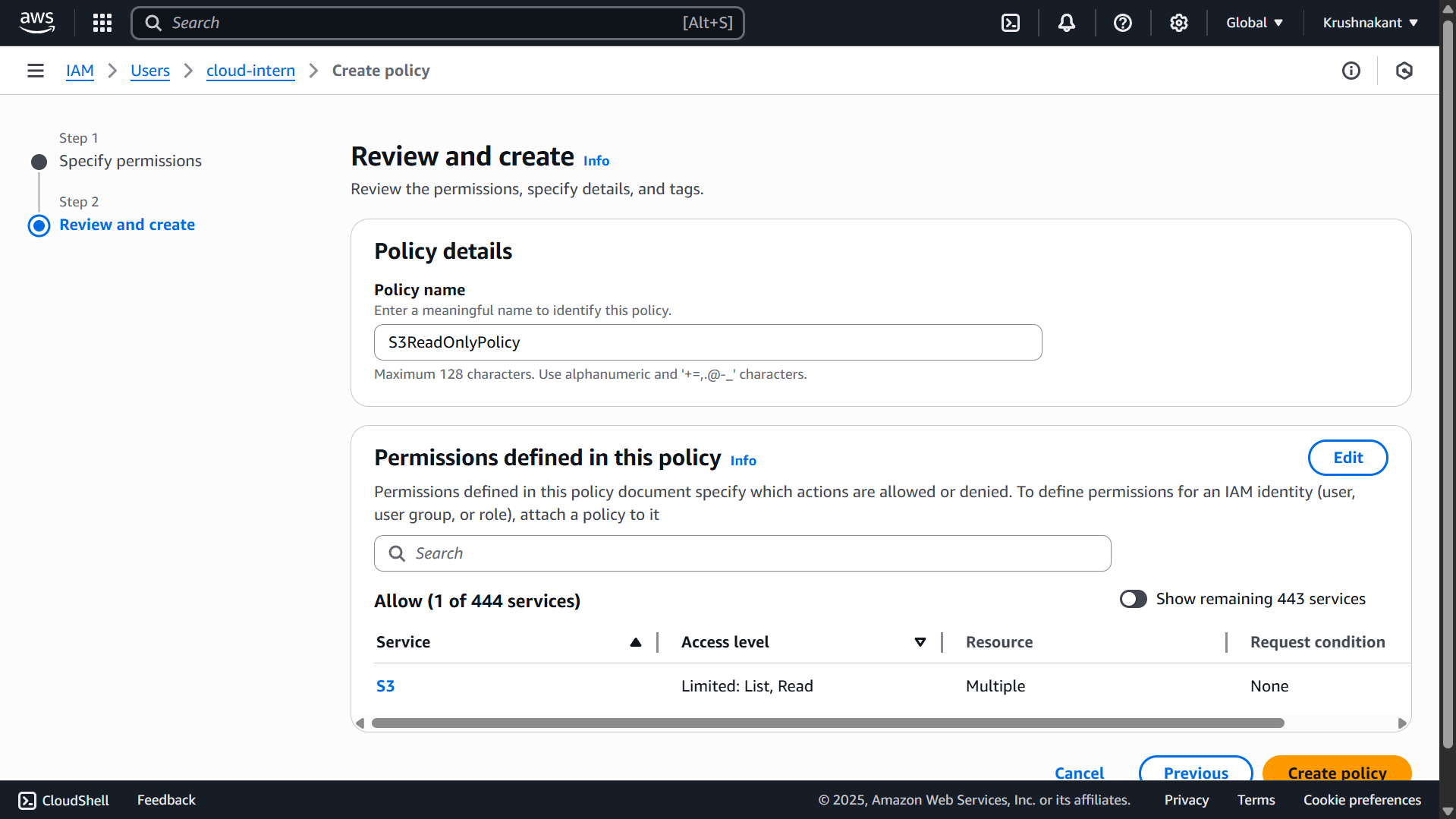
This document outlines the implementation of AWS IAM (Identity and Access Management) policies, S3 secure storage, and encryption mechanisms as part of Task 4 during the Cloud Computing Internship at CODTECH IT SOLUTIONS PVT. LTD.

# 2. IAM Policy Implementation

- Created an IAM user `secure-user` with programmatic and console access.

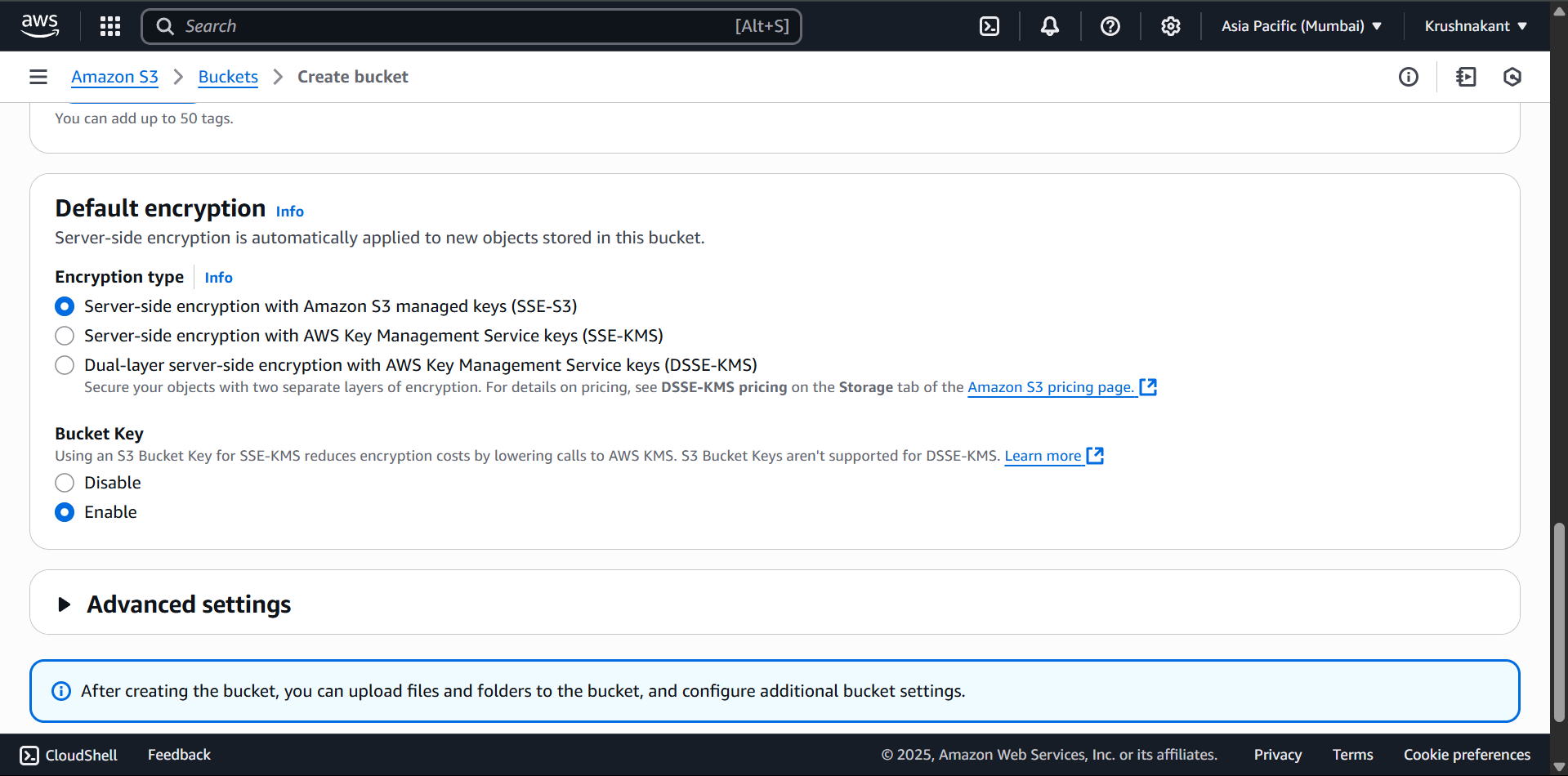
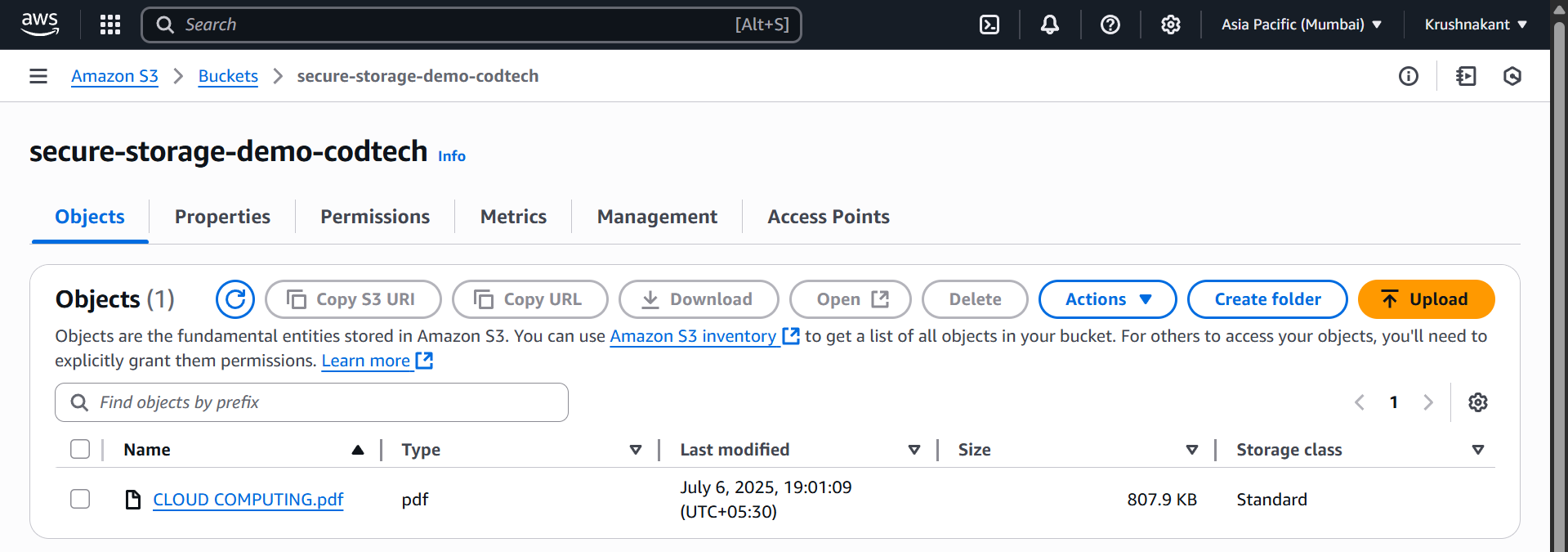
- Assigned a custom IAM policy with least privilege access to only one S3 bucket.

IAM Policy JSON:

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

# 3. Secure S3 Bucket Configuration

- Created S3 bucket named `secure-storage-demo`.

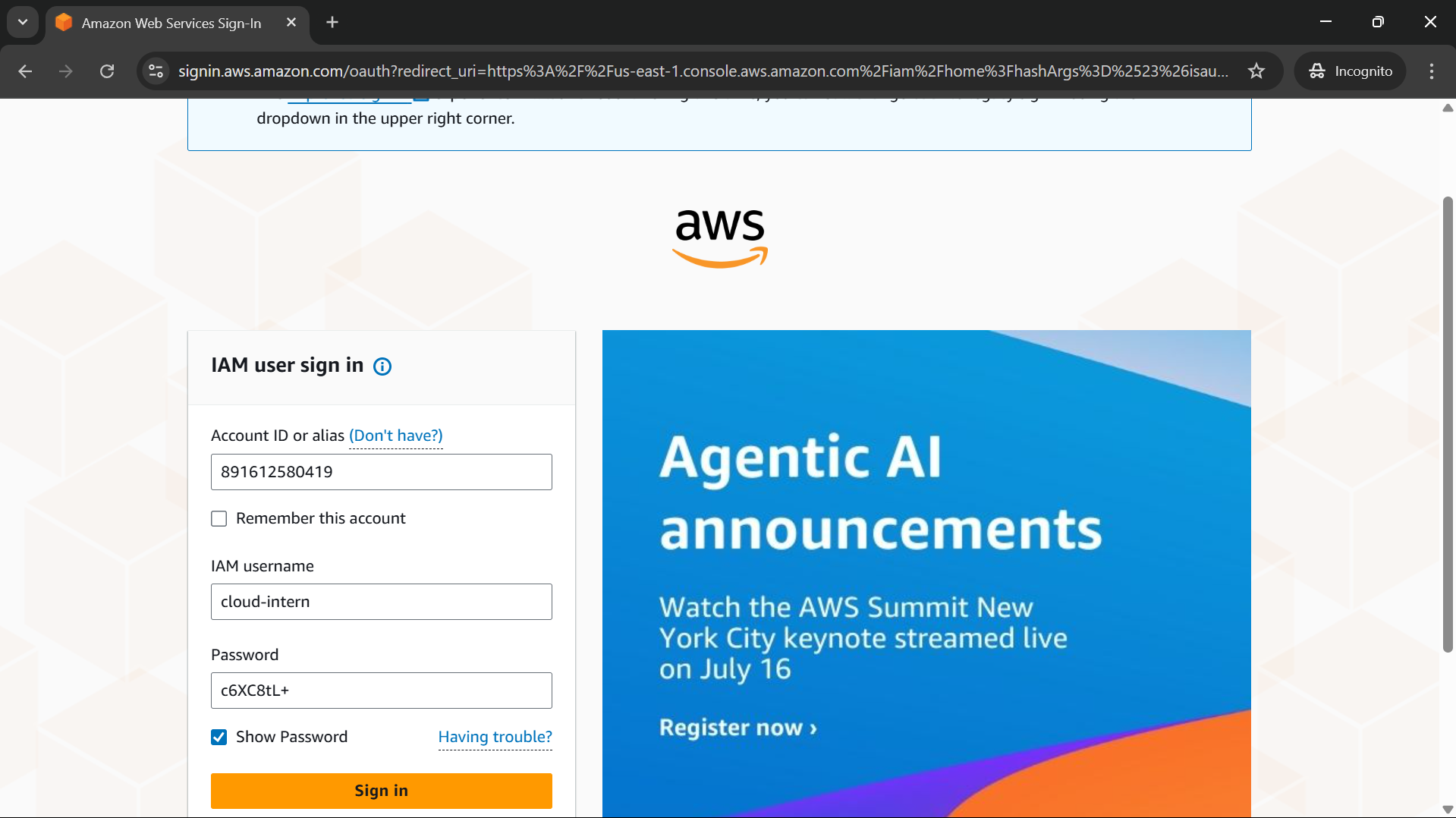
- Chose AWS-Managed Keys (**SSE-S3**) or Customer-Managed Keys (SSE-KMS).

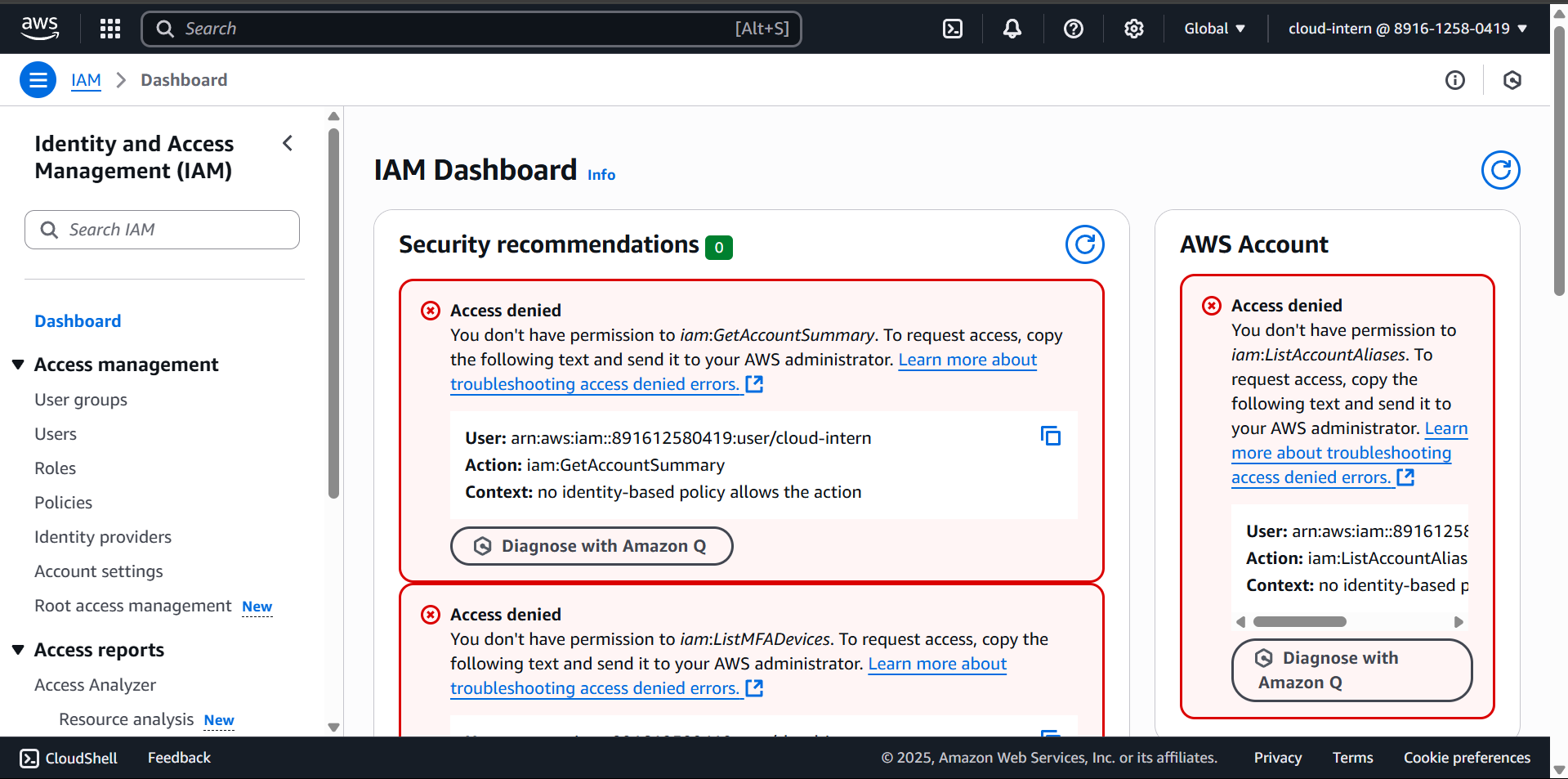
# 5. Testing & Validation

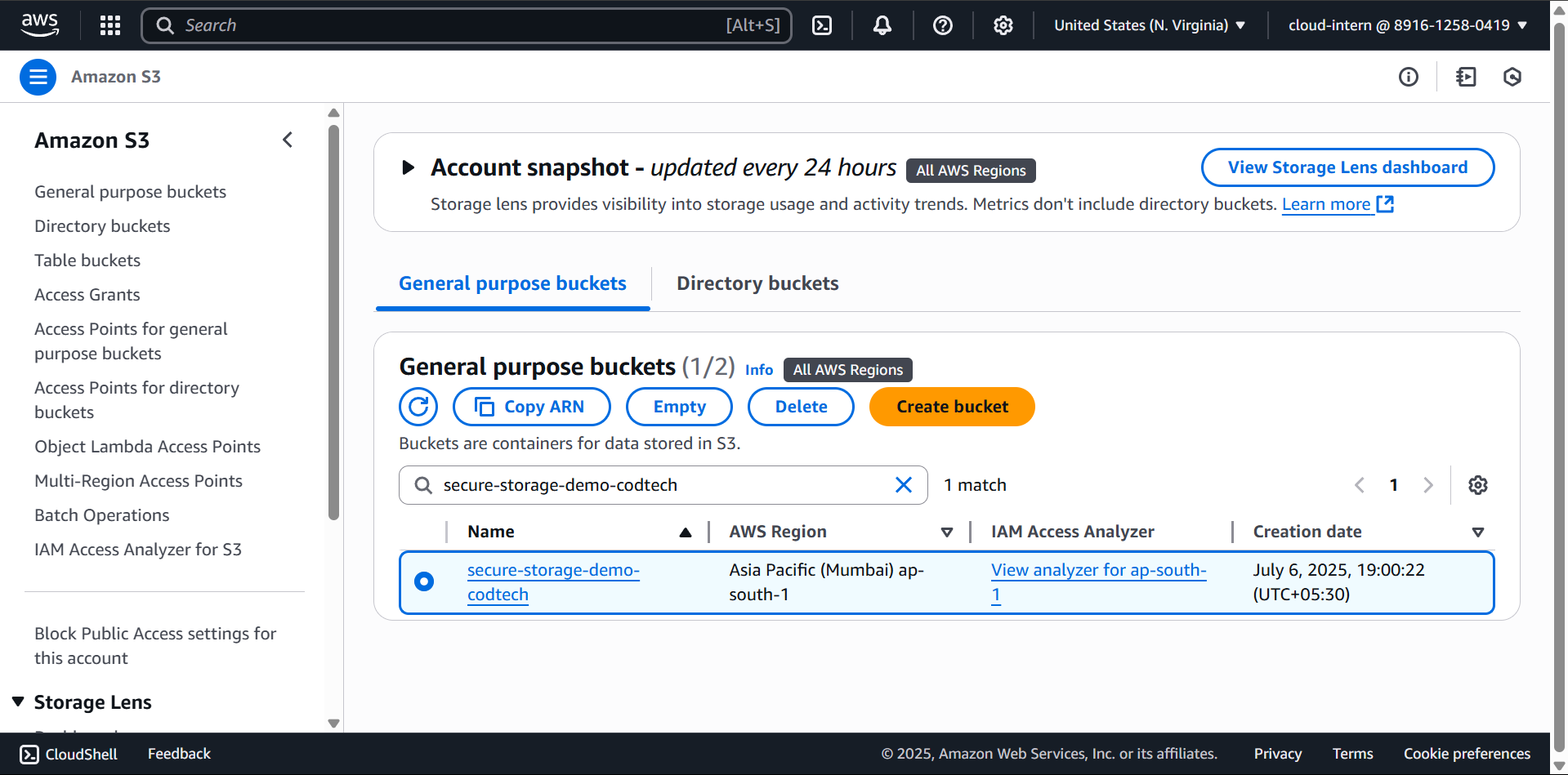
-Open a private/incognito browser.

-Use the IAM login URL.

-Log in as **cloud-intern**-user.

-Try to list objects from the bucket.





# 7. Conclusion

The implementation ensured secure cloud storage using AWS best practices. IAM policies enforced access control, S3 configuration enabled encrypted storage. This setup demonstrates a practical understanding of cloud security principles.