Cloud Security Implementation – Task 4

# 1. Introduction

Cloud security is an essential part of any organization utilizing cloud computing platforms. This report presents the steps and configurations I implemented to secure cloud resources using AWS. The task involved creating IAM users with restricted access, applying proper permissions, securing S3 bucket storage, and enabling encryption to ensure data privacy and security.

# 2. IAM Policy and Role Creation

IAM (Identity and Access Management) enables secure control over AWS services and resources. As part of this task, I created an IAM user named 'limited-user' to demonstrate secure access control:

• IAM User: limited-user  
• Access: Programmatic (no console access)  
• Permissions: AmazonS3ReadOnlyAccess policy attached  
• Rationale: Restrict the user to read-only access to Amazon S3, ensuring no write, delete, or administrative actions are allowed.  
• Benefits: Follows the Principle of Least Privilege (PoLP), minimizing potential attack surface.

# 3. Securing Amazon S3 Bucket

To protect the data stored in Amazon S3, I applied the following security measures:

• Block Public Access: Ensured that the S3 bucket does not allow public access.  
• Server-Side Encryption: Enabled SSE-S3 (Amazon S3 managed keys) to ensure data at rest is encrypted.  
• Access Policy: Limited access only to authenticated IAM users with proper roles or policies.  
• Secure Upload: Ensured that any data uploaded to the bucket is encrypted and access-logged.

# 4. Access Key Generation (Optional)

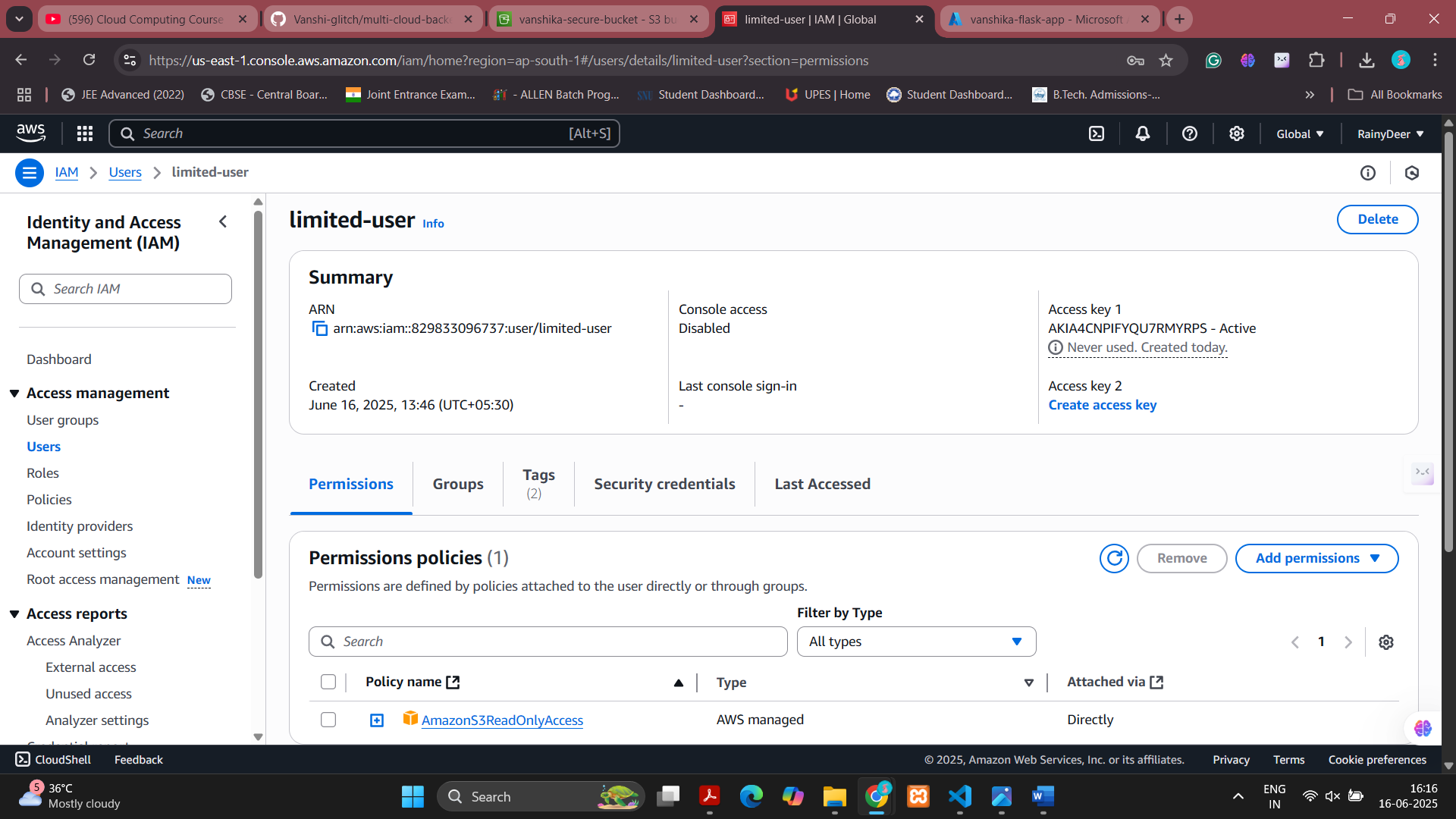
To allow secure programmatic access, an access key and secret key pair were generated for the limited-user. These keys allow the user to interact with AWS services (e.g., S3) using the AWS CLI or SDK. For enhanced security, these credentials are stored securely and rotated periodically.

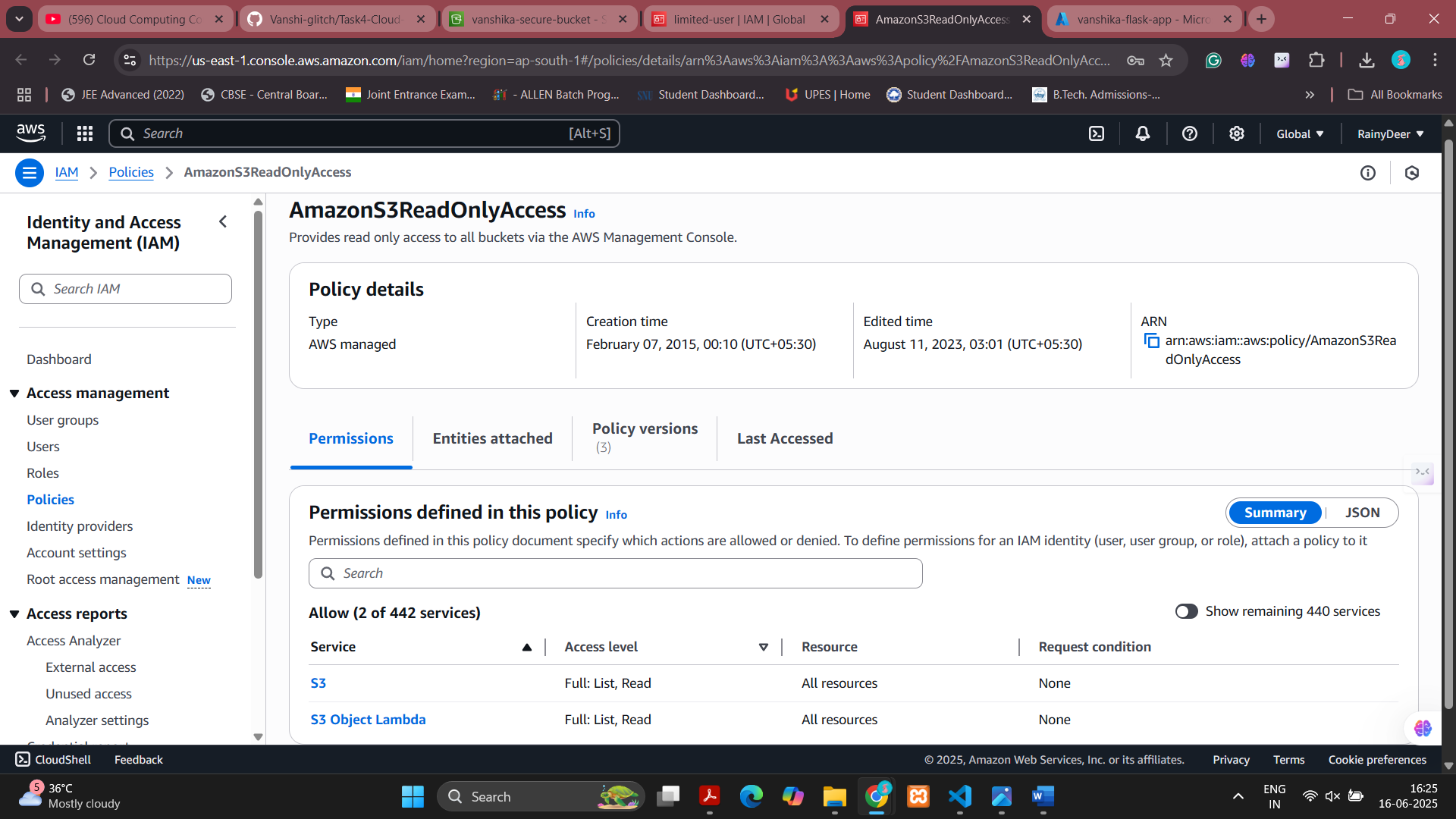
# 5. Tools & AWS Services Used

• IAM (Identity and Access Management): For user and permission management.  
• Amazon S3: Cloud storage platform where security was configured.  
• AWS Console: Used for managing policies, encryption, and user setup.  
• AWS CLI (optional): For verifying IAM and bucket permissions using command line interface.

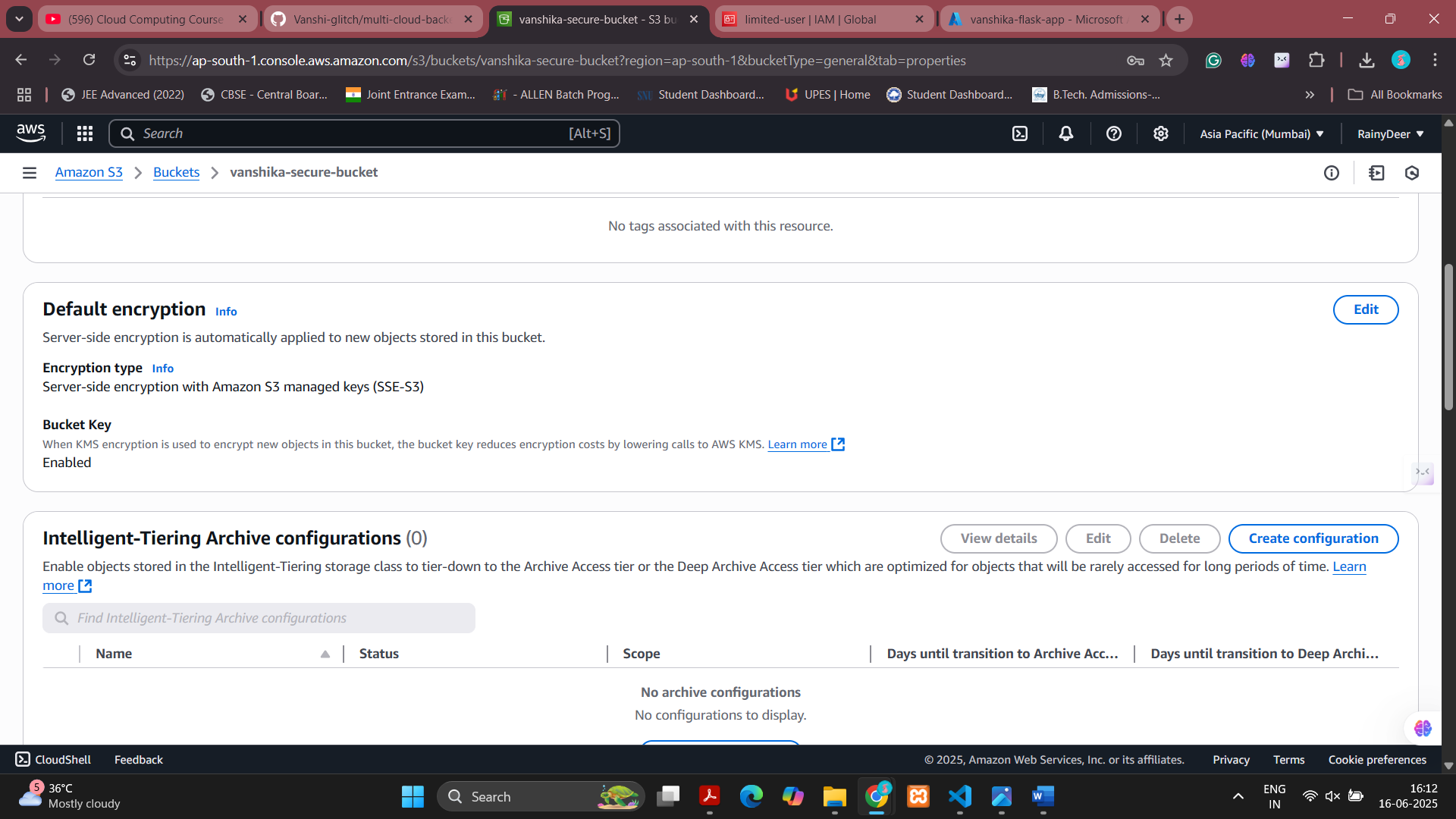
# 6. Screenshots and Evidence

Screenshots captured during the task include:  
• IAM User Creation Screen

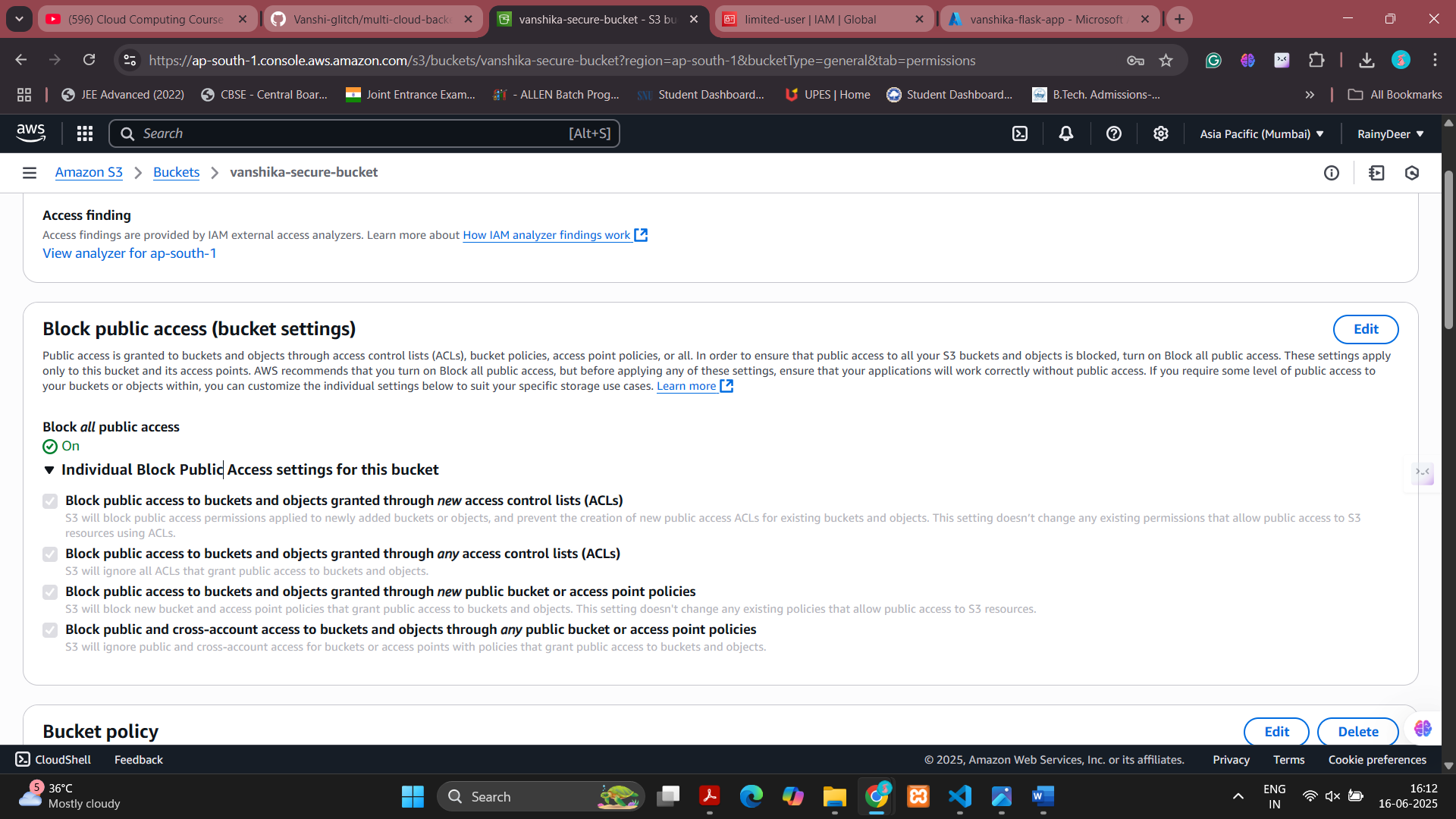


• IAM Policy Attachment (AmazonS3ReadOnlyAccess)

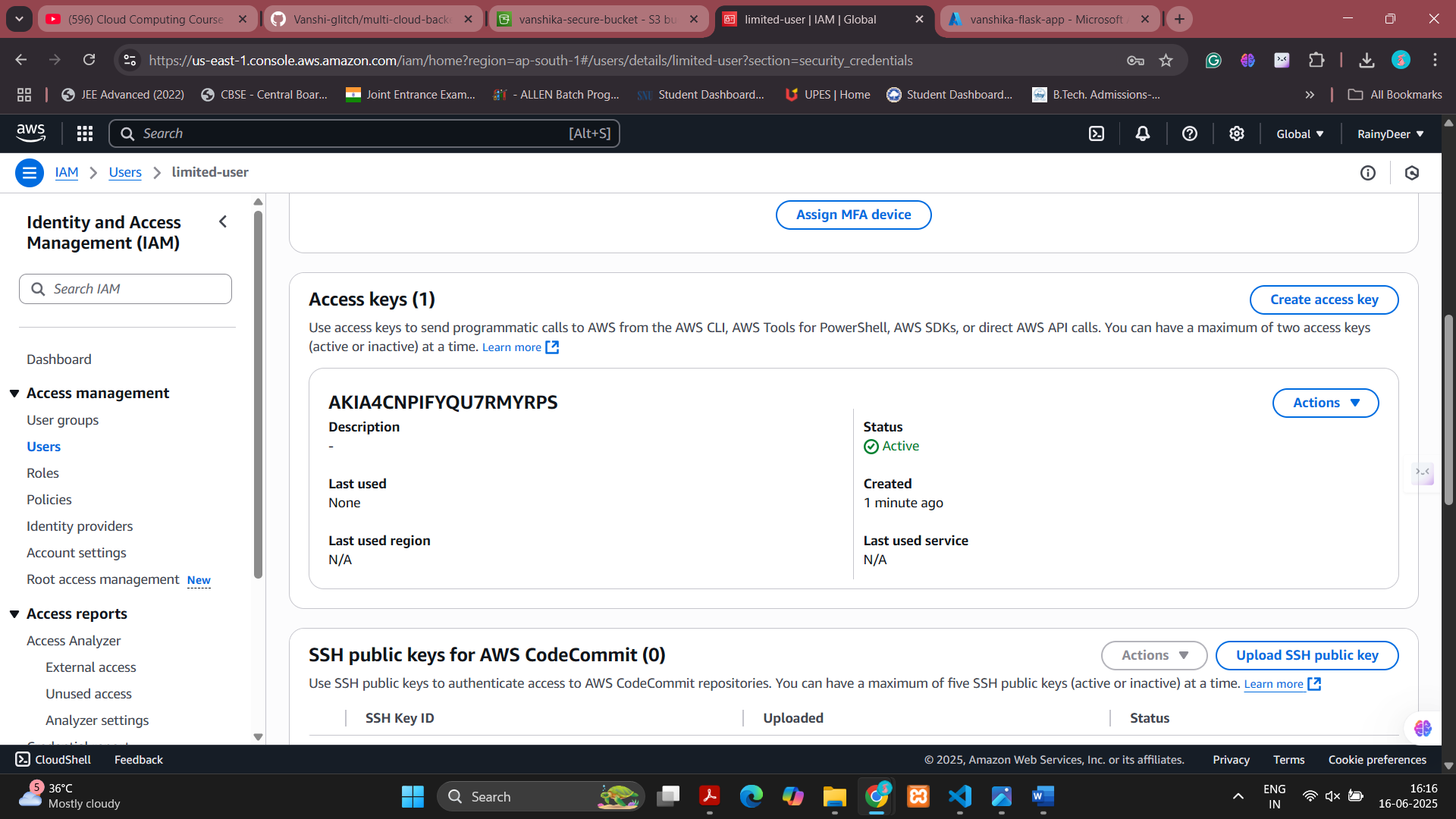
• S3 Bucket Encryption Settings



• S3 Public Access Configuration



• Access Key Generated



# 7. Learning and Takeaways

• Understood the core IAM concepts and how to assign policies effectively.  
• Gained practical experience in securing data in Amazon S3.  
• Learned how to manage user permissions securely without exposing resources.  
• Practiced implementing encryption and access logging mechanisms.  
• Developed confidence in using AWS security services for real-world applications.

# 8. Conclusion

Task 4 helped me grasp the importance of securing cloud infrastructure. By creating a limited IAM user, applying least-privilege policies, and configuring secure S3 storage, I ensured that data remains protected and access is tightly controlled. These are foundational steps in implementing a secure cloud environment.