|  |
| --- |
| Digital Egypt Pioneers Initiative |
| AWS Project: Securing Cloud Resources |
| Project Report |
|  |
| **Mohammed Ibrahim Hamissa**  **AWS Cloud Solutions Admin and Architect**  **ALX1-ISS4-M1e**  **October, 2024** |
|  |

|  |
| --- |
| This document provides a comprehensive overview of the steps taken to secure cloud resources at AnyCompany Financial. It covers the implementation of security measures in various phases, including data security, network security, and monitoring and logging. |

[Phase 1: Securing Data in Amazon S3 2](#_Toc179458358)

[Task 1.1: Creating a Bucket and Applying a Bucket Policy 2](#_Toc179458359)

[Task 1.2: Enabling Versioning and Object-Level Logging 2](#_Toc179458360)

[Task 1.3: Implementing S3 Inventory 2](#_Toc179458361)

[Task 1.4: Confirming Versioning and Object-Level Logging 2](#_Toc179458362)

[Task 1.5: Querying Access Logs Using Athena 2](#_Toc179458363)

[Phase 2: Securing VPCs 3](#_Toc179458364)

[Task 2.1: Reviewing LabVPC and Associated Resources 3](#_Toc179458365)

[Task 2.2: Creating a VPC Flow Log 3](#_Toc179458366)

[Task 2.3: Accessing the WebServer Instance and Reviewing VPC Flow Logs 3](#_Toc179458367)

[Task 2.4: Configuring Route Table and Security Group Settings 3](#_Toc179458368)

[Task 2.5: Securing the WebServerSubnet with a Network ACL 4](#_Toc179458369)

[Task 2.6: Reviewing NetworkFirewallVPC and Associated Resources 4](#_Toc179458370)

[Task 2.7: Creating a Network Firewall 5](#_Toc179458371)

[Task 2.8: Creating Route Tables 5](#_Toc179458372)

[Task 2.9: Configuring Logging for the Network Firewall 5](#_Toc179458373)

[Task 2.10: Configuring the Firewall Policy and Testing Access 5](#_Toc179458374)

[Phase 3: Securing AWS Resources Using AWS KMS 5](#_Toc179458375)

[Task 3.1: Creating a Customer Managed Key and Configuring Key Rotation 5](#_Toc179458376)

[Task 3.2: Updating the AWS KMS Key Policy and Analyzing an IAM Policy 5](#_Toc179458377)

[Task 3.3: Using AWS KMS to Encrypt Data in Amazon S3 6](#_Toc179458378)

[Task 3.4: Using AWS KMS to Encrypt the Root Volume of an EC2 Instance 7](#_Toc179458379)

[Task 3.5: Using AWS KMS Envelope Encryption to Encrypt Data in Place 8](#_Toc179458380)

[Task 3.6: Using AWS KMS to Encrypt a Secrets Manager Secret 8](#_Toc179458381)

[Phase 4: Monitoring and Logging 9](#_Toc179458382)

[Task 4.1: Using CloudTrail to Record Amazon S3 API Calls 9](#_Toc179458383)

[Task 4.2: Using CloudWatch Logs to Monitor Secure Logs 10](#_Toc179458384)

[Task 4.3: Creating a CloudWatch Alarm to Send Notifications for Security Incidents 11](#_Toc179458385)

[Task 4.4: Configuring AWS Config to Assess Security Settings and Remediate the Configuration of AWS Resources 12](#_Toc179458386)

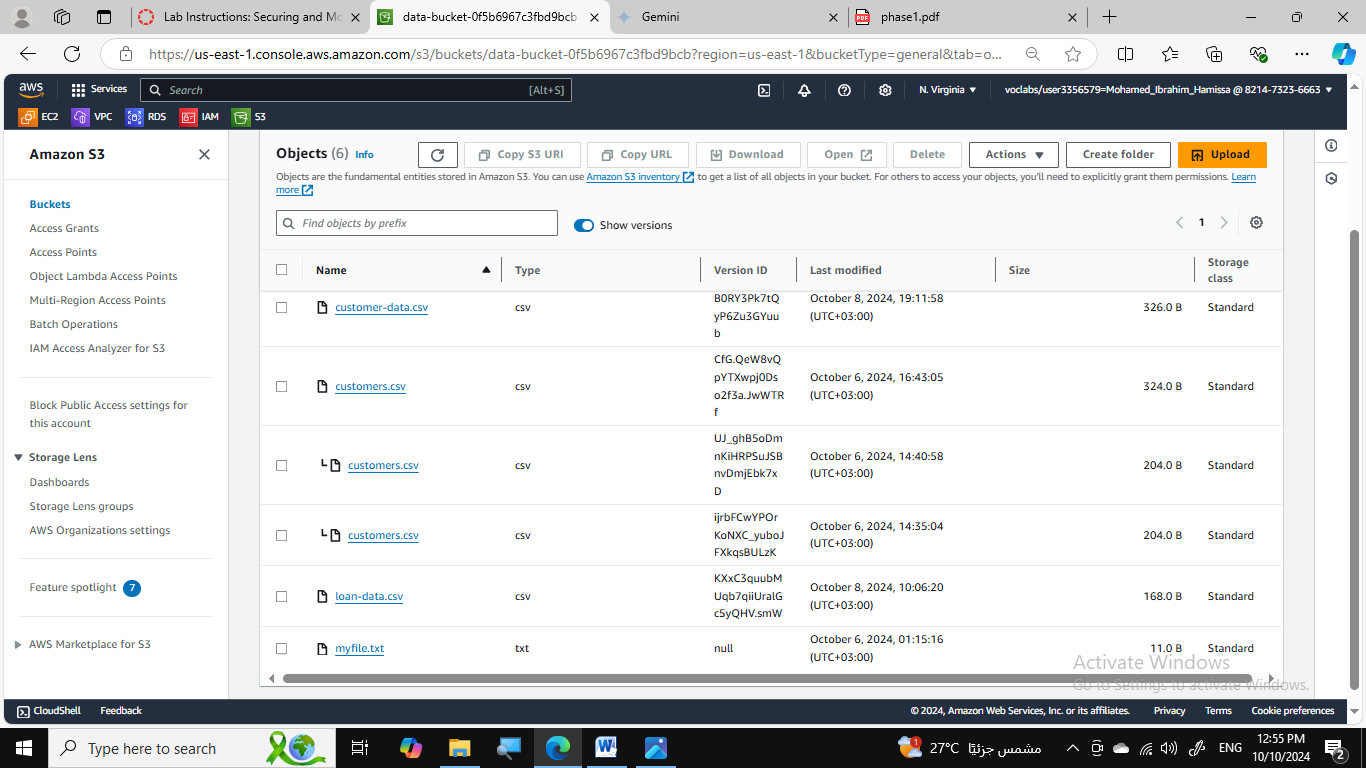
[5. Certificate 13](#_Toc179458387)

# Phase 1: Securing Data in Amazon S3

## Task 1.1: Creating a Bucket and Applying a Bucket Policy

* Created a new S3 bucket named data-bucket- [0f5b6967c3fbd9bcb](https://us-east-1.console.aws.amazon.com/s3/buckets/data-bucket-0f5b6967c3fbd9bcb?region=us-east-1)
* Applied a bucket policy to restrict access to authorized users.

## Task 1.2: Enabling Versioning and Object-Level Logging



* Enabled versioning on the data-bucket to track object changes.
* Enabled object-level logging to record detailed access information.

## Task 1.3: Implementing S3 Inventory

* Configured S3 Inventory to monitor object changes and generate reports.

## Task 1.4: Confirming Versioning and Object-Level Logging

* Verified that versioning and object-level logging are working as expected.
* Tested access to different versions of the customers.csv file.

## Task 1.5: Querying Access Logs Using Athena

* Created an Athena table to query access logs.
* Retrieved log data for specific actions, such as uploading and downloading the customers.csv file.

# Phase 2: Securing VPCs

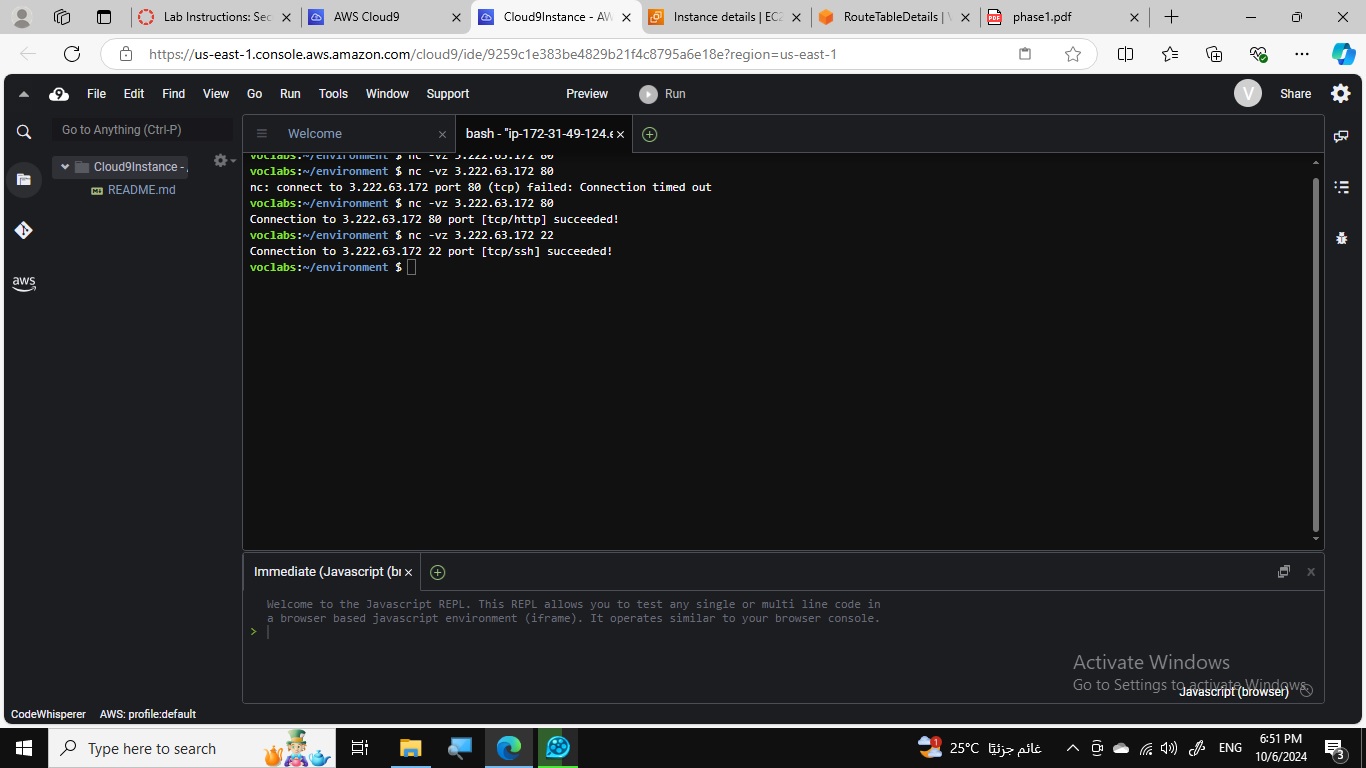
## Task 2.1: Reviewing LabVPC and Associated Resources

* Analyzed the existing LabVPC resources, including subnets, route table, and internet gateway.

## Task 2.2: Creating a VPC Flow Log

* Created a VPC flow log for LabVPC to capture network traffic information.

## Task 2.3: Accessing the WebServer Instance and Reviewing VPC Flow Logs



* Tested access to the WebServer instance from the internet.
* Reviewed VPC flow logs to analyze network traffic patterns.

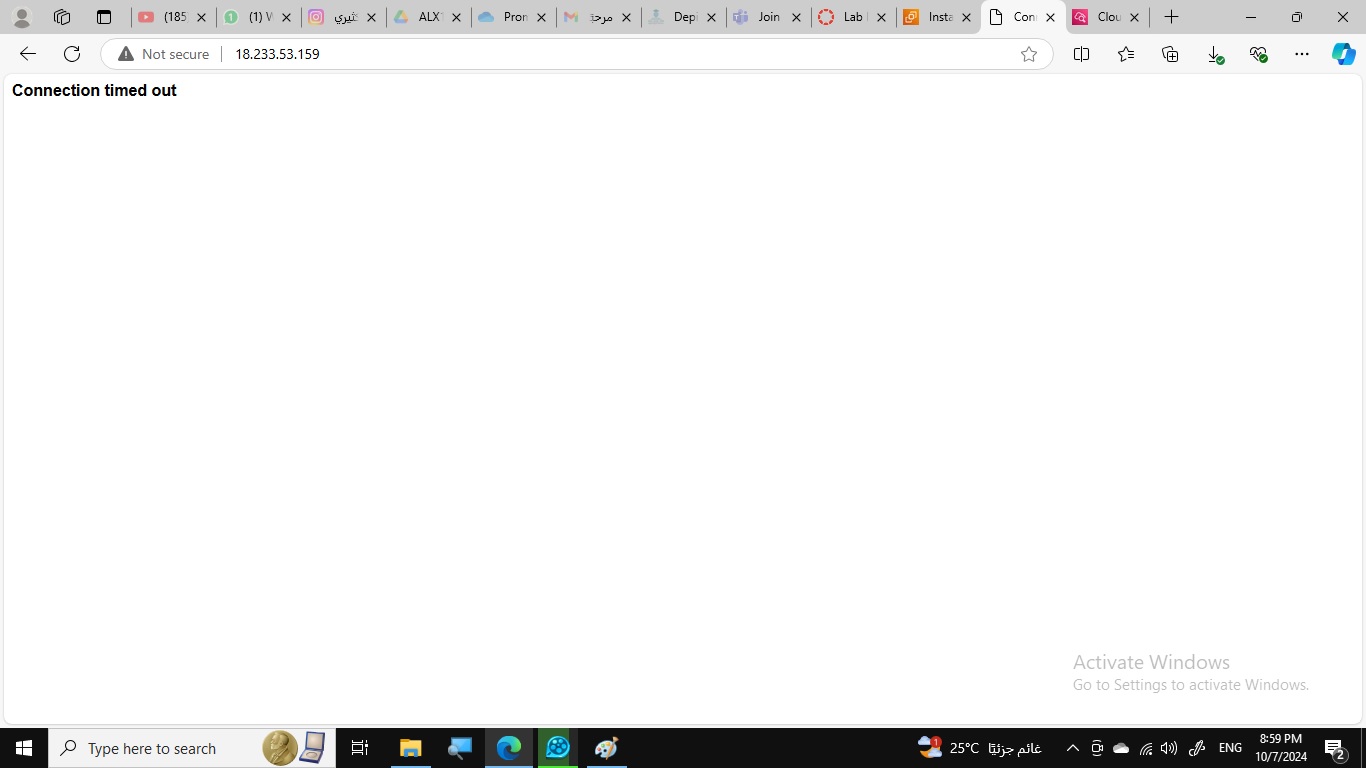
## Task 2.4: Configuring Route Table and Security Group Settings

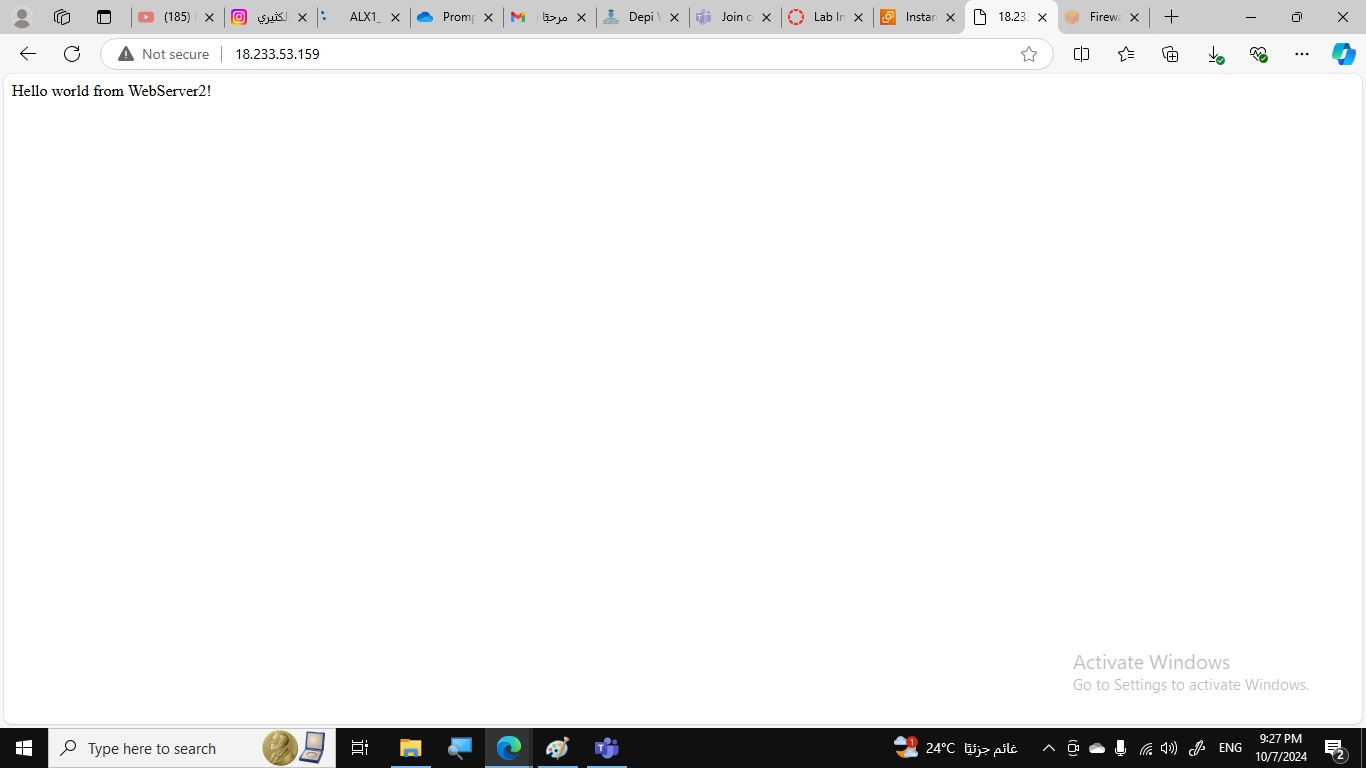
* Modified the route table to allow internet traffic to the WebServerSubnet.
* Configured the security group to allow inbound traffic on ports 80 and 22.

## Task 2.5: Securing the WebServerSubnet with a Network ACL

* Created a network ACL for the WebServerSubnet to provide an additional layer of security.

## Task 2.6: Reviewing NetworkFirewallVPC and Associated Resources





* Analyzed the NetworkFirewallVPC resources, including subnets, internet gateway, and network ACL.

## Task 2.7: Creating a Network Firewall

* Created a network firewall named NetworkFirewall for the NetworkFirewallVPC.

## Task 2.8: Creating Route Tables

* Created route tables for the FirewallSubnet and WebServer2Subnet.
* Configured routes to direct traffic to the internet gateway through the firewall.

## Task 2.9: Configuring Logging for the Network Firewall

* Configured logging for the network firewall to monitor network traffic requests.

## Task 2.10: Configuring the Firewall Policy and Testing Access

* Created a stateful rule group with rules to allow specific traffic and deny others.
* Tested access to the WebServer2 instance after applying the firewall policy.

# Phase 3: Securing AWS Resources Using AWS KMS

## Task 3.1: Creating a Customer Managed Key and Configuring Key Rotation

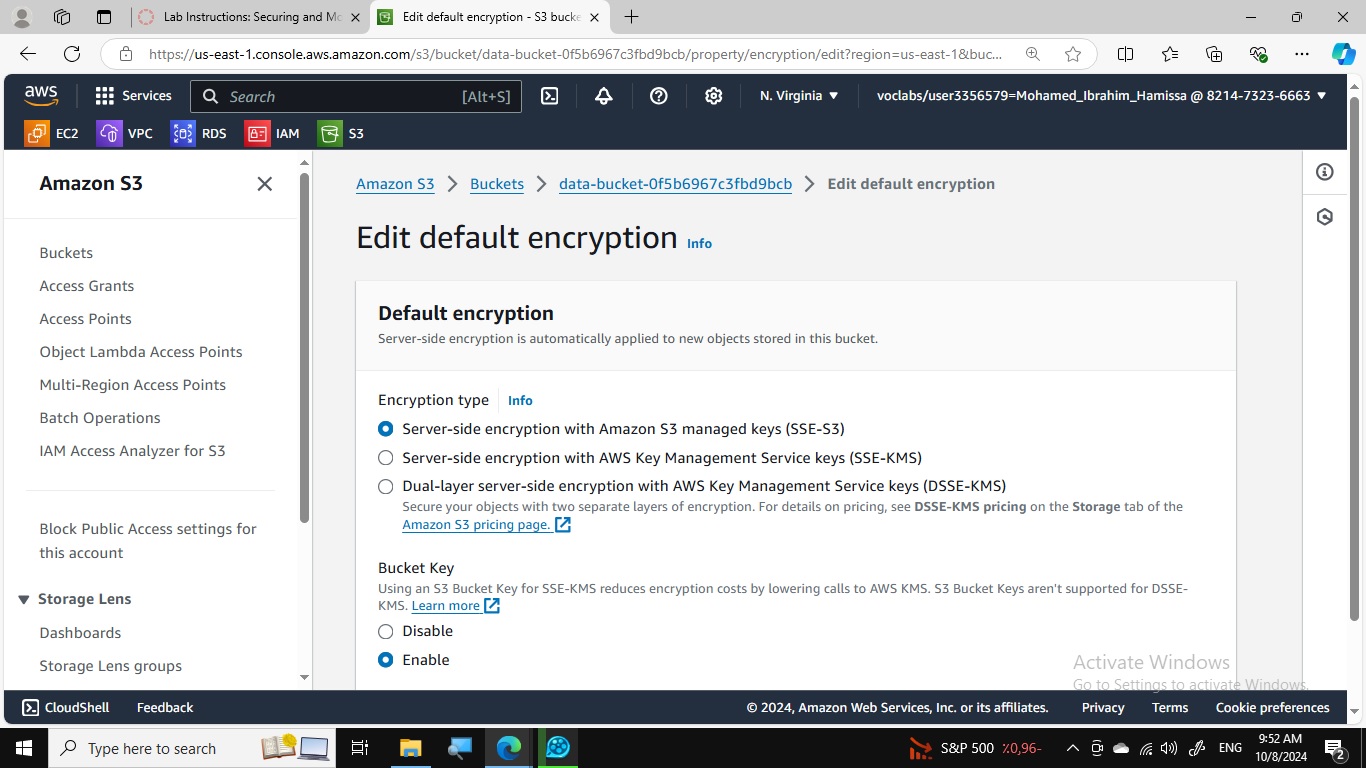
* Created a customer managed key named MyKMSKey.
* Configured automatic key rotation for the key.

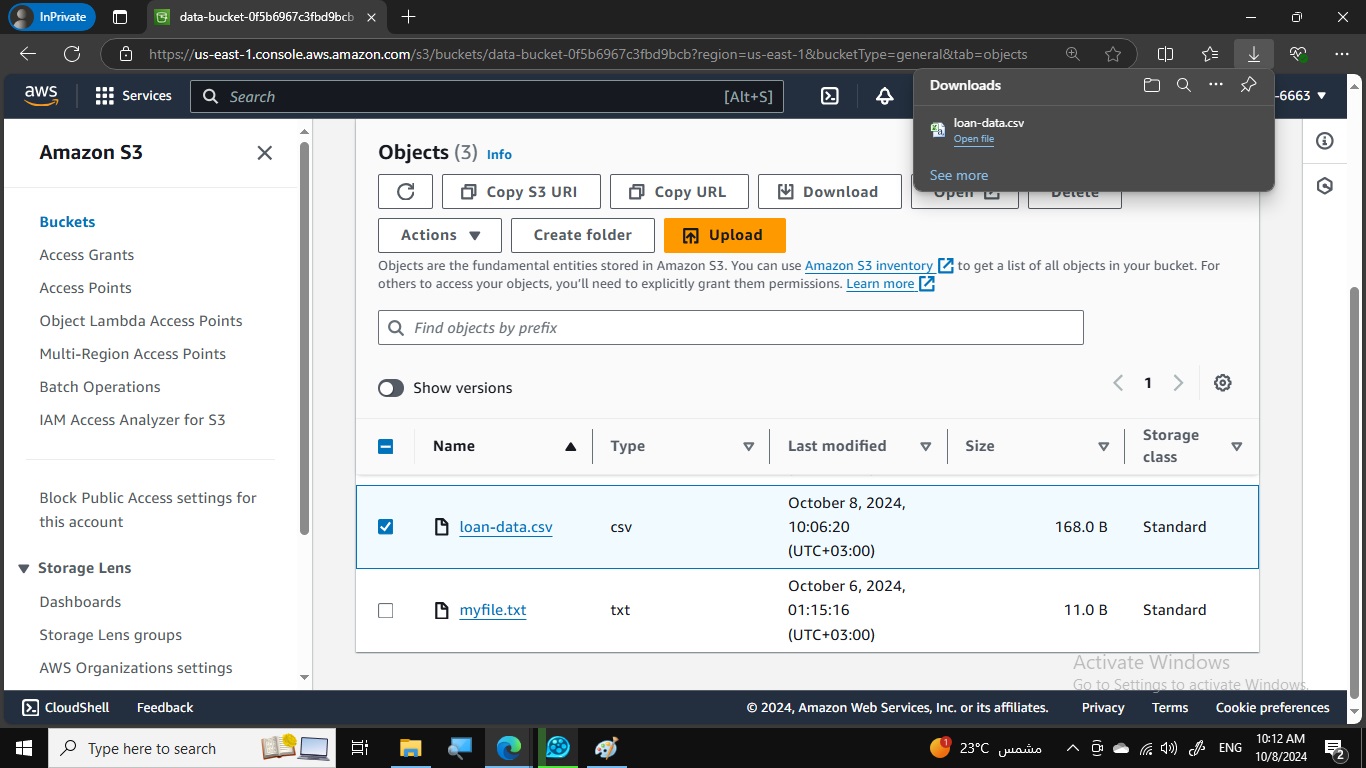
## Task 3.2: Updating the AWS KMS Key Policy and Analyzing an IAM Policy

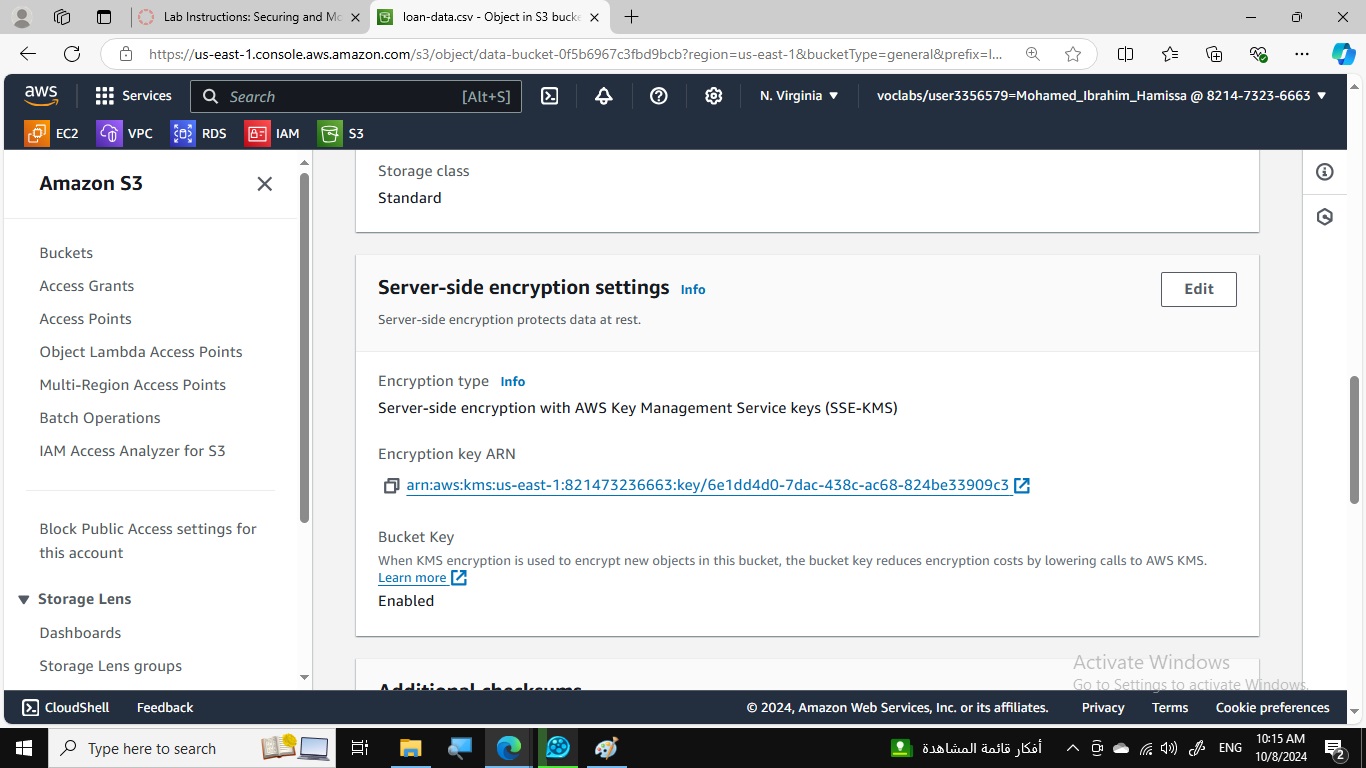
[Insert screenshot of KMS key policy] [Insert screenshot of IAM policy]

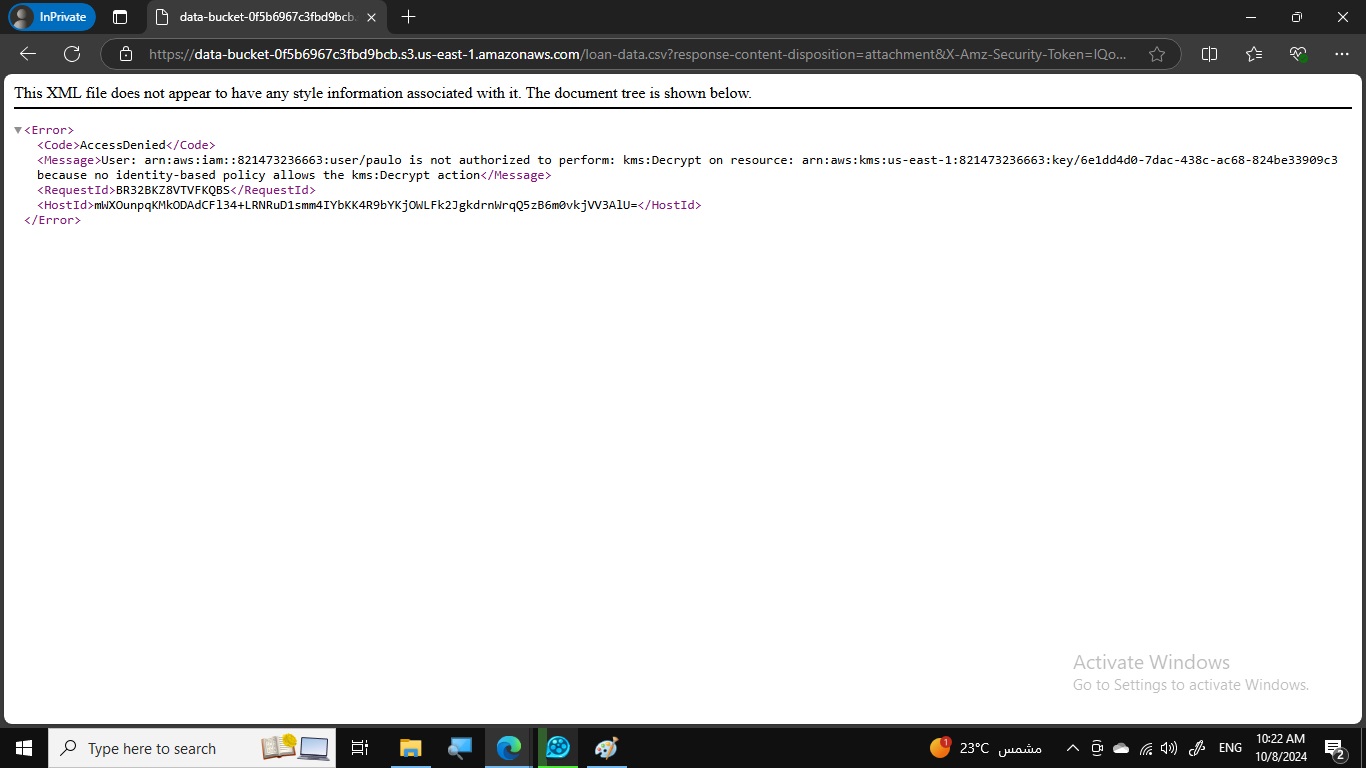
* Modified the key policy to allow the sofia user to use the key.
* Analyzed the IAM policy for the sofia user to verify permissions.

## Task 3.3: Using AWS KMS to Encrypt Data in Amazon S3







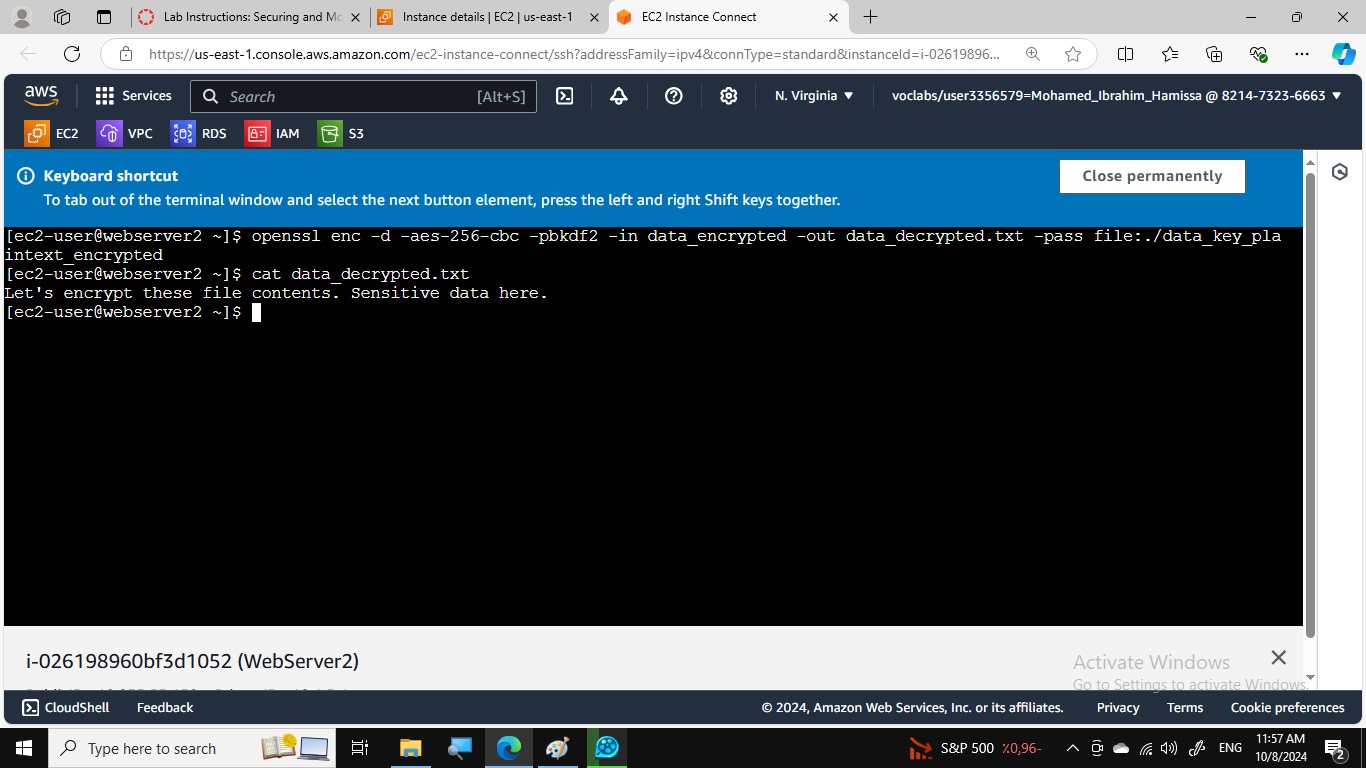


* Updated the data-bucket encryption settings to use SSE-KMS.
* Uploaded the loan-data.csv file to the data-bucket.

## Task 3.4: Using AWS KMS to Encrypt the Root Volume of an EC2 Instance

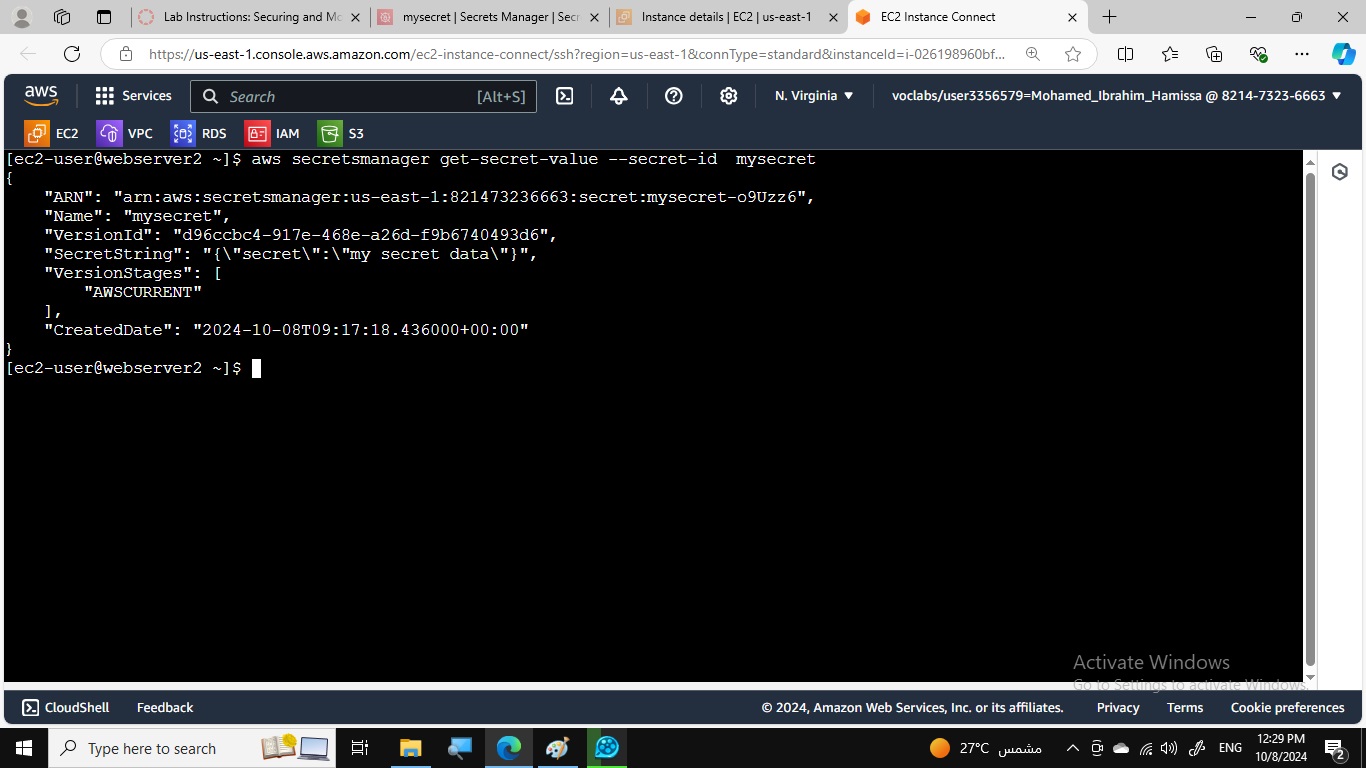
* Created an EC2 instance named EncryptedInstance with encrypted root volume.

## Task 3.5: Using AWS KMS Envelope Encryption to Encrypt Data in Place



* Generated a data key using AWS KMS.
* Encrypted and decrypted the data\_unencrypted.txt file using the data key.

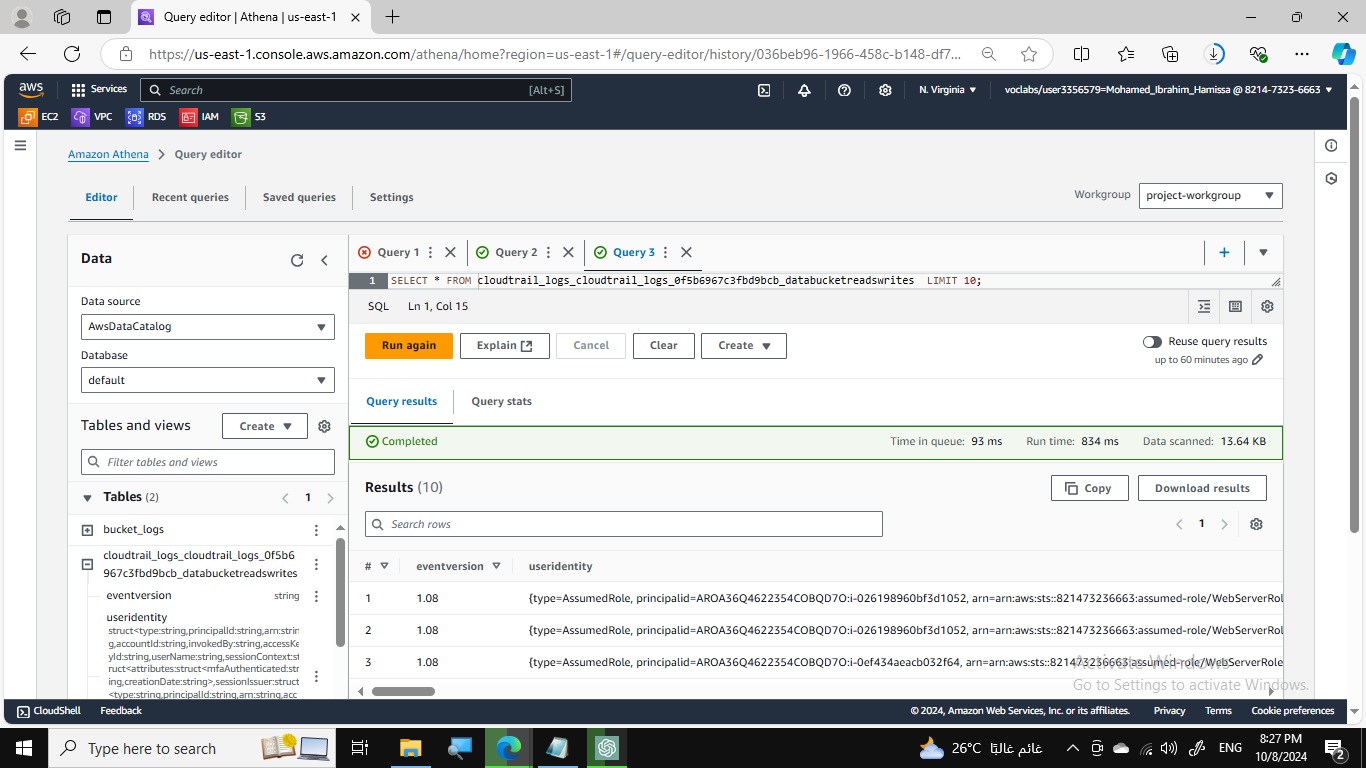
## Task 3.6: Using AWS KMS to Encrypt a Secrets Manager Secret

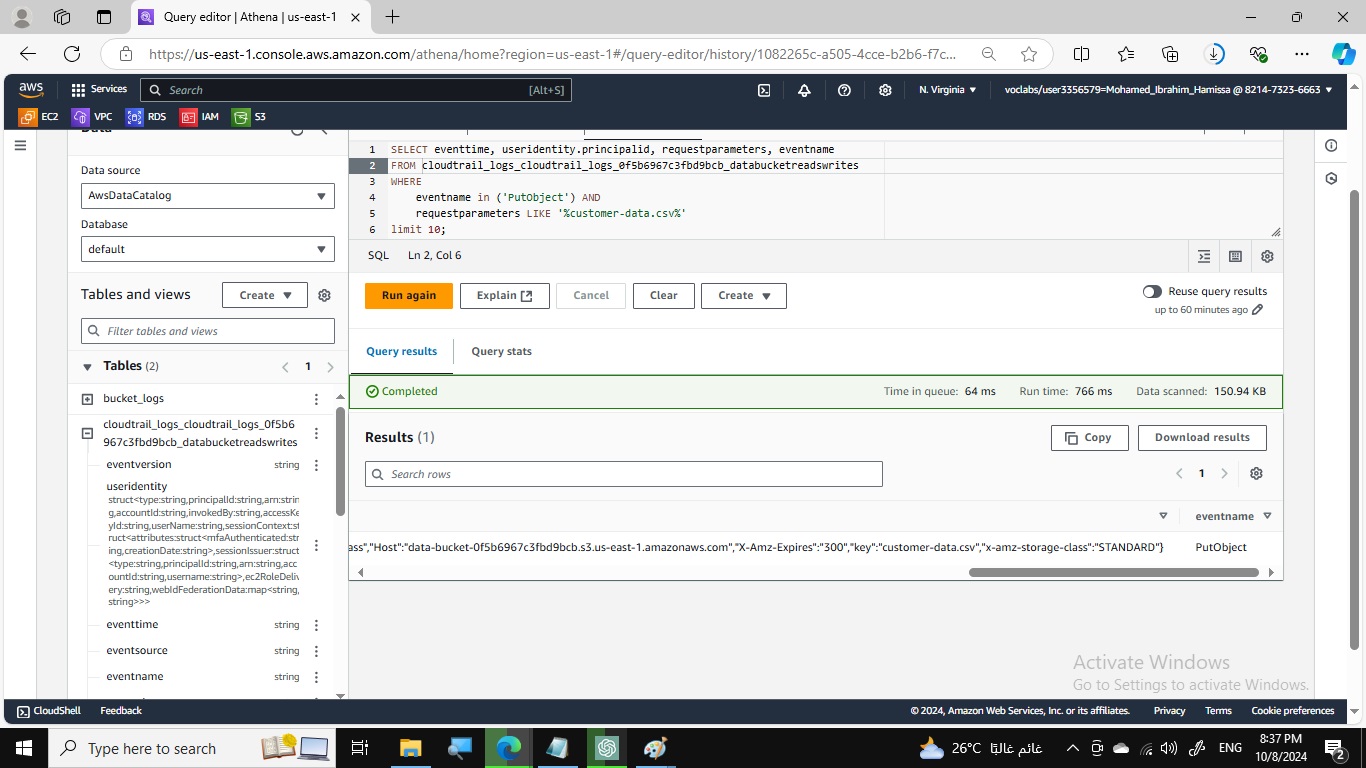


* Created a Secrets Manager secret and encrypted it with the KMS key.
* Retrieved the secret using the AWS CLI.

# Phase 4: Monitoring and Logging

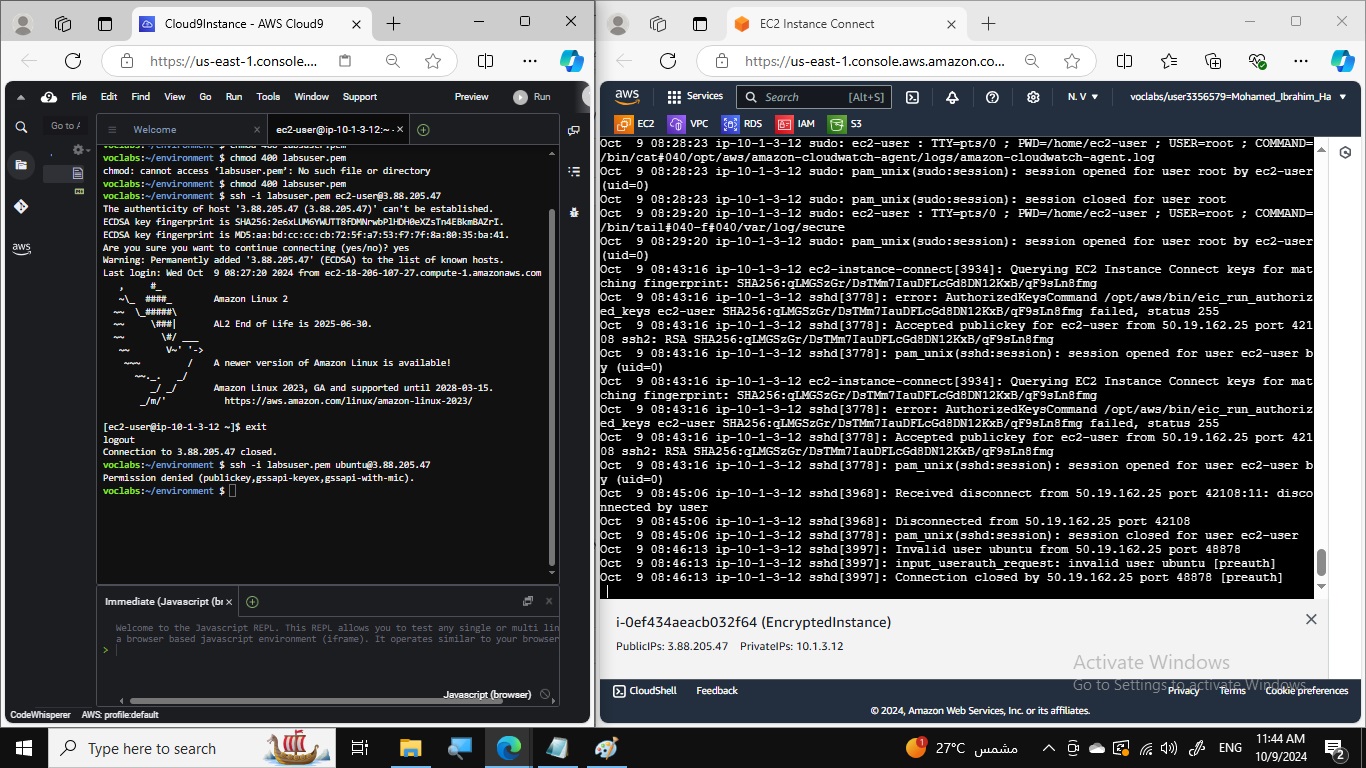
## Task 4.1: Using CloudTrail to Record Amazon S3 API Calls

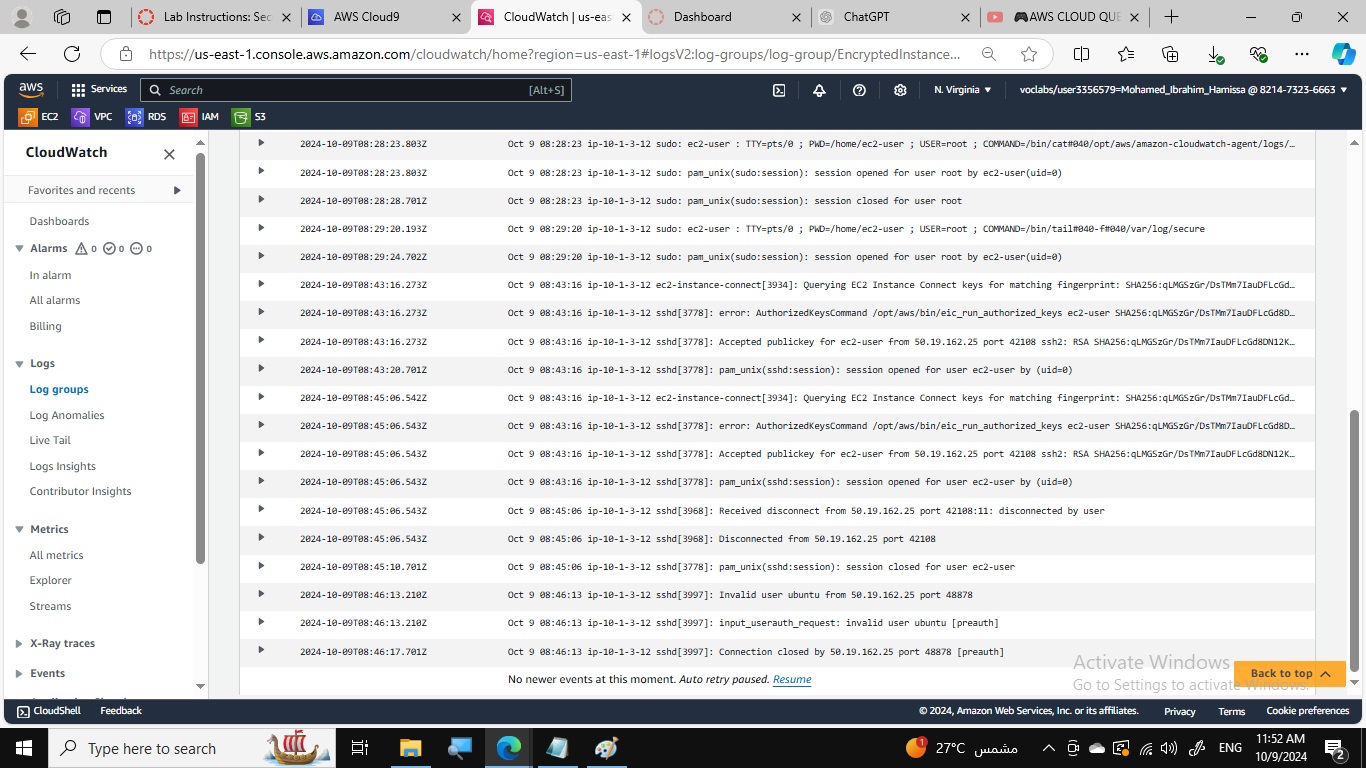




* Created a CloudTrail trail to record S3 API calls.
* Created an Athena table to query CloudTrail log data.

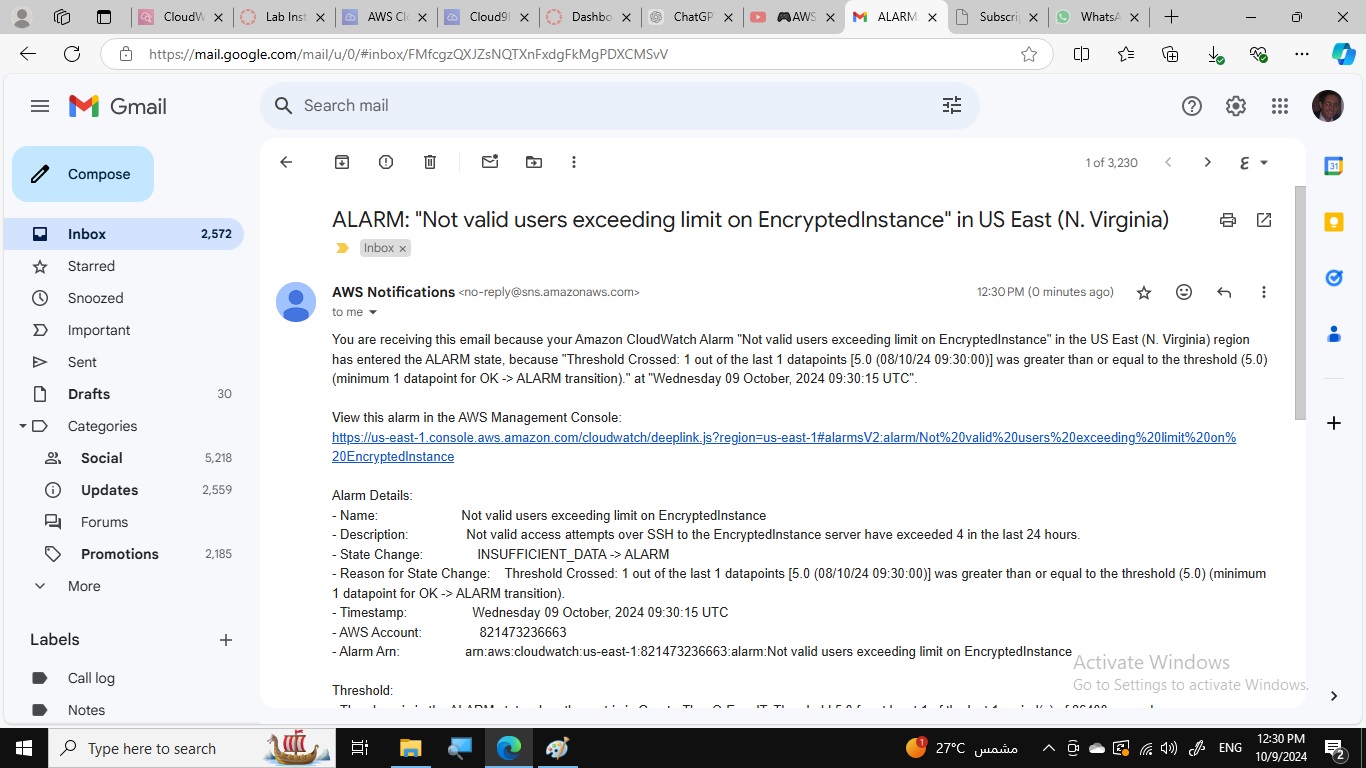
## Task 4.2: Using CloudWatch Logs to Monitor Secure Logs

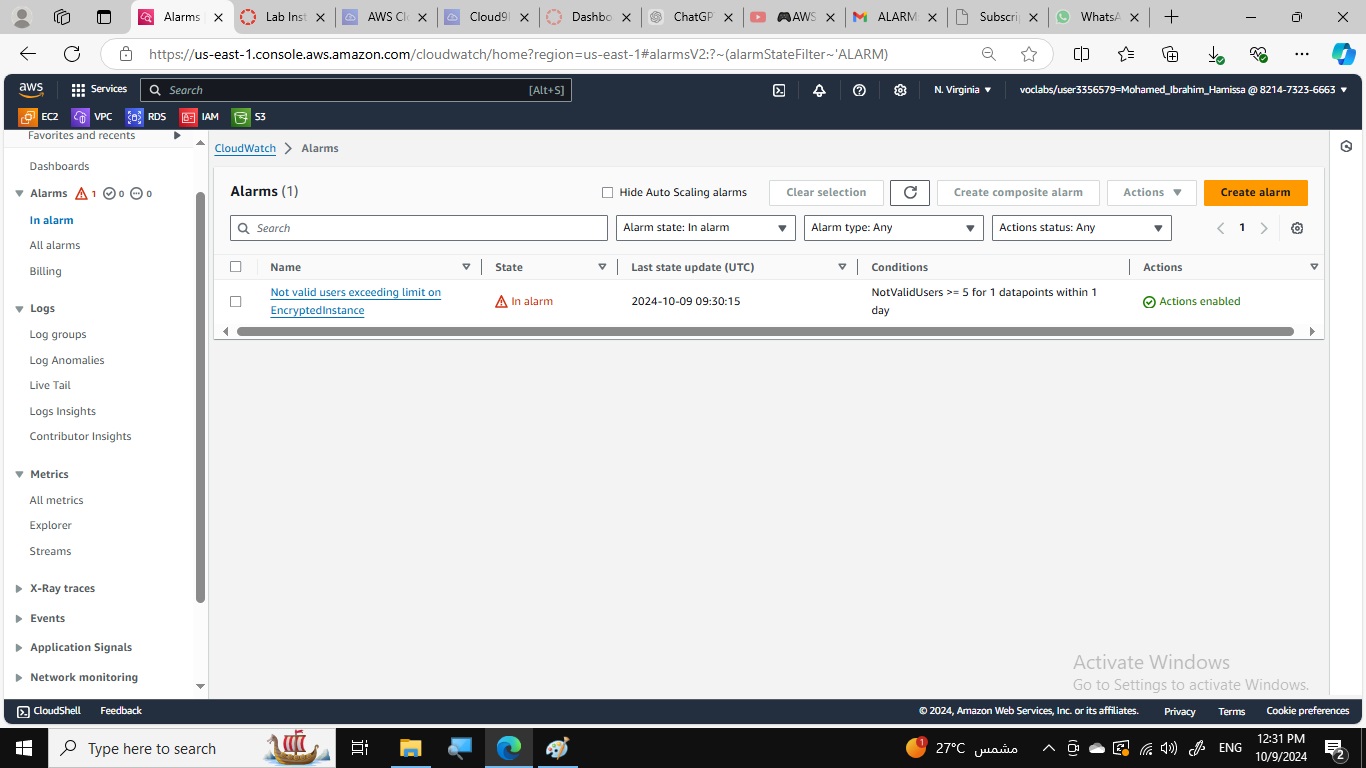




* Configured CloudWatch Logs to monitor secure logs from the EncryptedInstance.
* Collected and analyzed SSH access attempts.

## Task 4.3: Creating a CloudWatch Alarm to Send Notifications for Security Incidents





* Created a CloudWatch metric filter to detect invalid user access attempts.
* Created a CloudWatch alarm to send notifications when the alarm threshold is met.

## Task 4.4: Configuring AWS Config to Assess Security Settings and Remediate the Configuration of AWS Resources

* Configured AWS Config to assess security settings for S3 buckets.
* Created a remediation action to enable object logging on noncompliant buckets.

# 5. Certificate

