
CLOUD, MICROSERVICES, AND APPLICATION

LAB ASSIGNMENT





THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)



SUBMITTED TO: DR. SUMANA MAITI
SUBMITTED BY: DIVIJA 102018056 CSBS-3



Module 1- Global Infrastructure

Module 2- Structure of the cloud

Module 3- AWS console

▼ Module 1 - Global Infrastructure	Complete All Items	✓
 Student Guide		
 Module 1 Knowledge Check 100 pts Scored at least 70.0		✓

▼ Module 2 - Structures of the Cloud	Complete All Items	✓
 Student Guide		
 Module 2 Knowledge Check 100 pts Scored at least 70.0		✓

▼ Module 3 - AWS Console	Complete All Items	✓
 Student Guide		
 Module 3 Knowledge Check 100 pts Scored at least 70.0		✓

Recent Feedback

✓ [Module 1 Knowledge Check](#)
AICv1Sem1EN-18510
100 out of 100

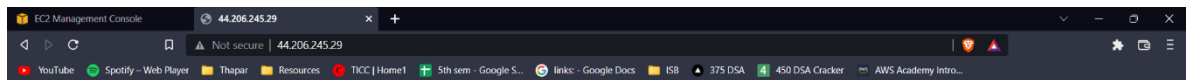
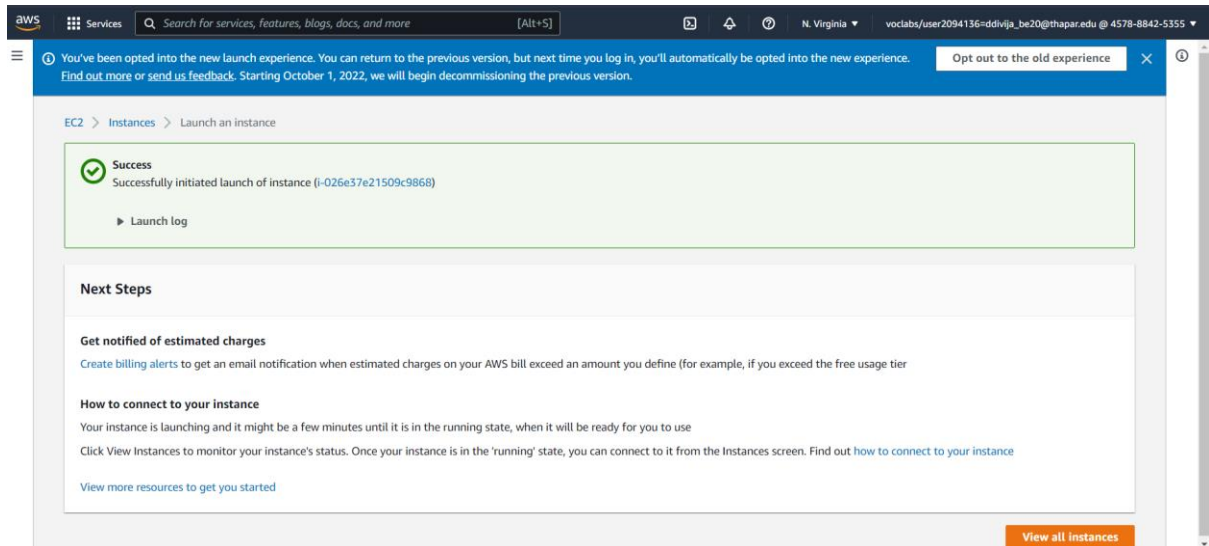
✓ [Module 2 Knowledge Check](#)
100 out of 100

✓ [Module 3 Knowledge Check](#)

100 out of 100

Module 4 – Virtual Servers

1. Lab 4.1 EC2

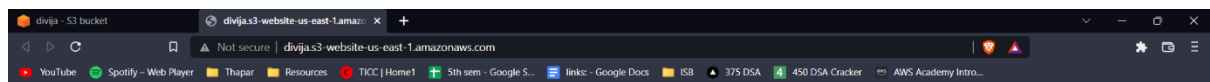
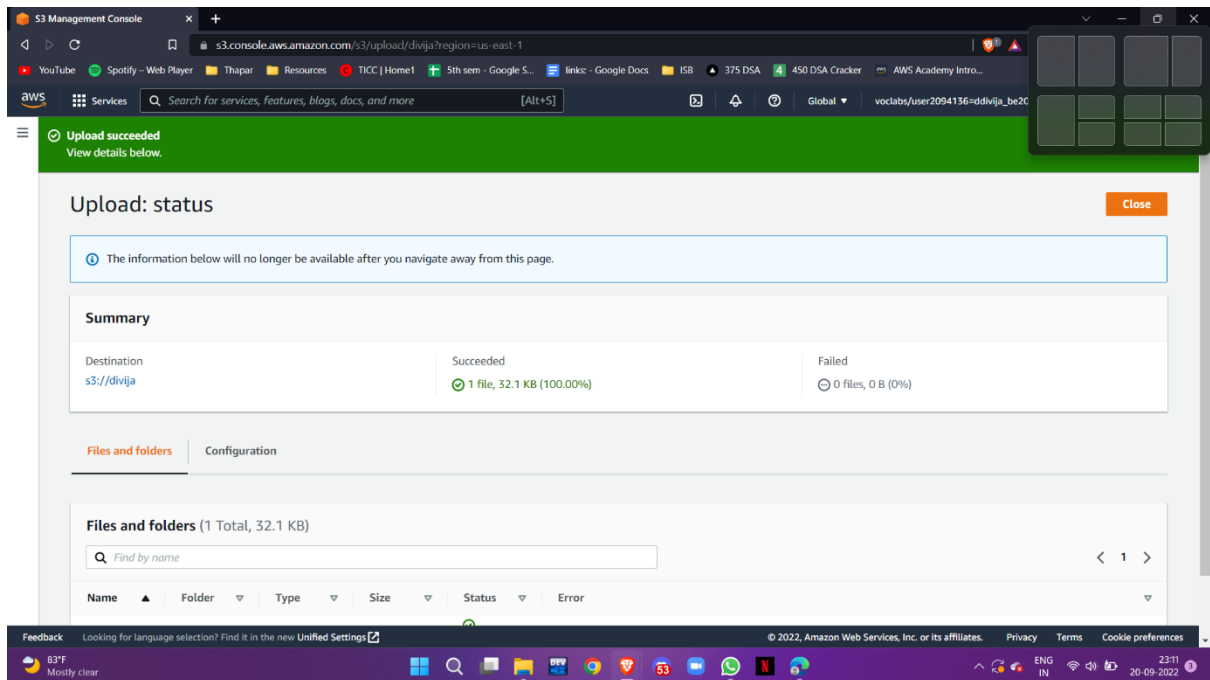


2. Lab 4.2 S3

The screenshot shows the AWS Management Console interface. A green notification banner at the top states: "Successfully created bucket 'divijabucket'. To upload files and folders, or to configure additional bucket settings choose View details." Below this, the "Amazon S3" console is open, displaying the "Buckets" section. A table lists the bucket "divijabucket" in the "US East (N. Virginia) us-east-1" region, with "Objects can be public" access and a creation date of "September 19, 2022, 15:07:19 (UTC+05:30)".

Name	AWS Region	Access	Creation date
divijabucket	US East (N. Virginia) us-east-1	Objects can be public	September 19, 2022, 15:07:19 (UTC+05:30)

The screenshot shows the "Permissions overview" for the "divijabucket". The bucket is marked as "Publicly accessible". The "Block public access (bucket settings)" section is visible, with a note: "Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases." The "Block all public access" checkbox is currently unchecked.

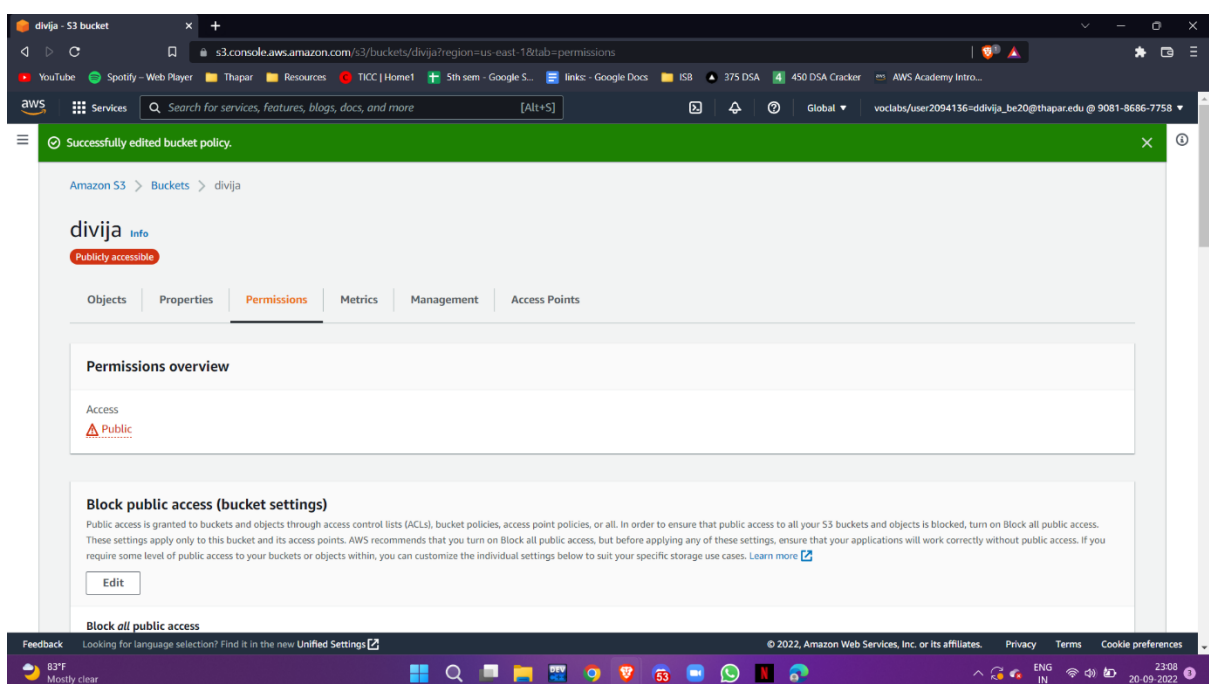
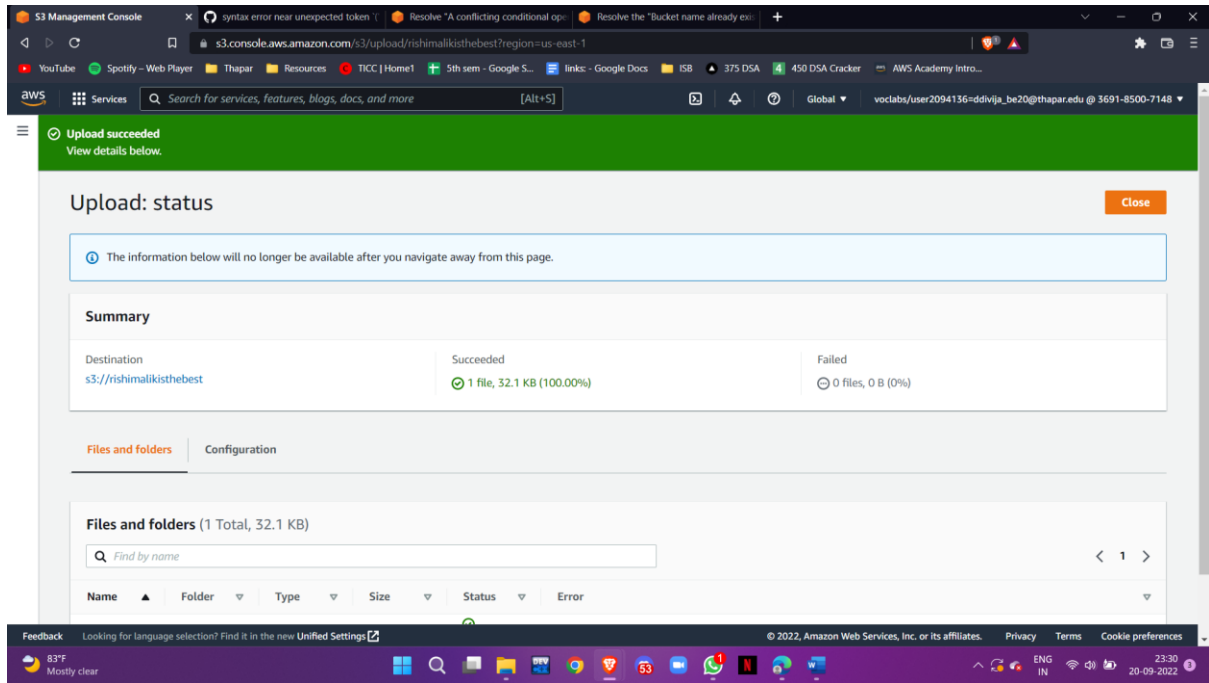


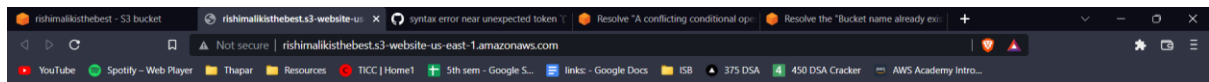
Hello World. Take me to your leader.



Module 5- Content Delivery

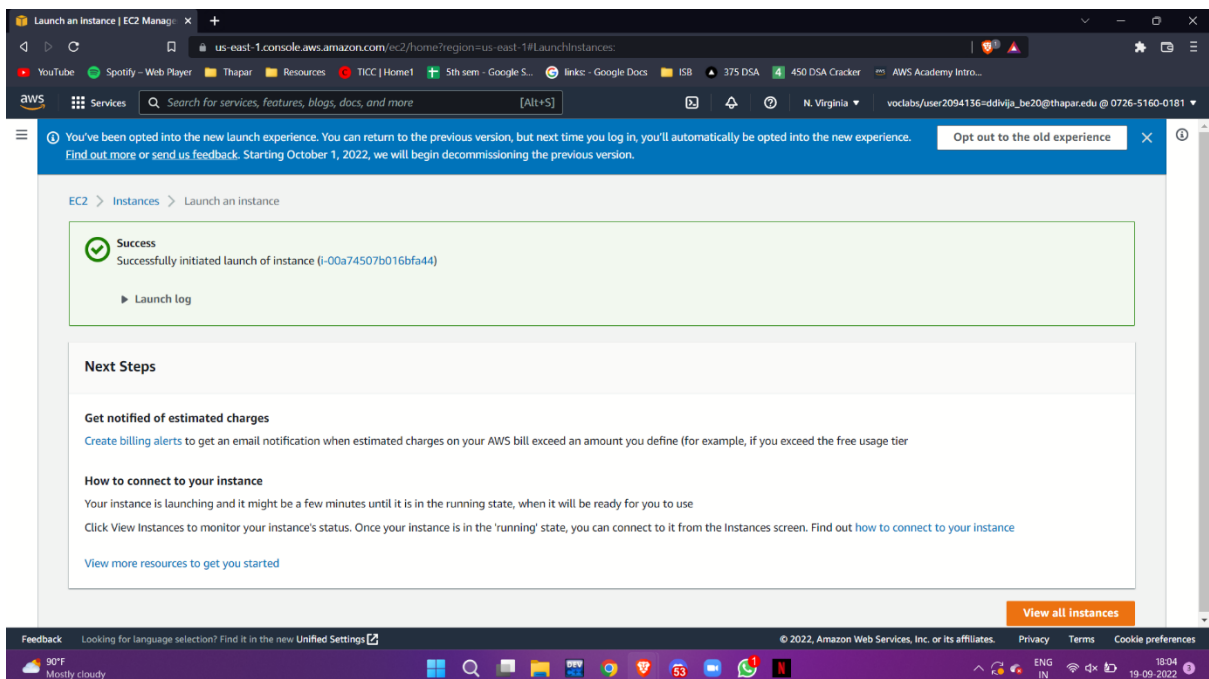
Lab 5 – CloudFront

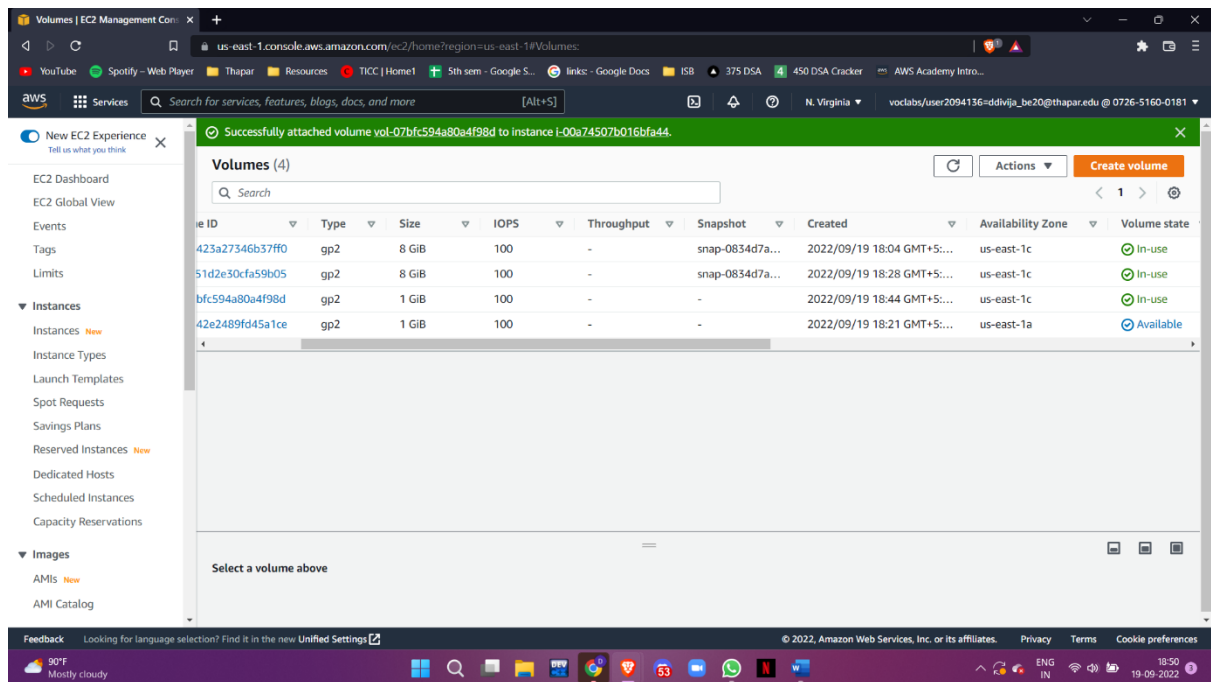




Module 6 – Virtual Storage

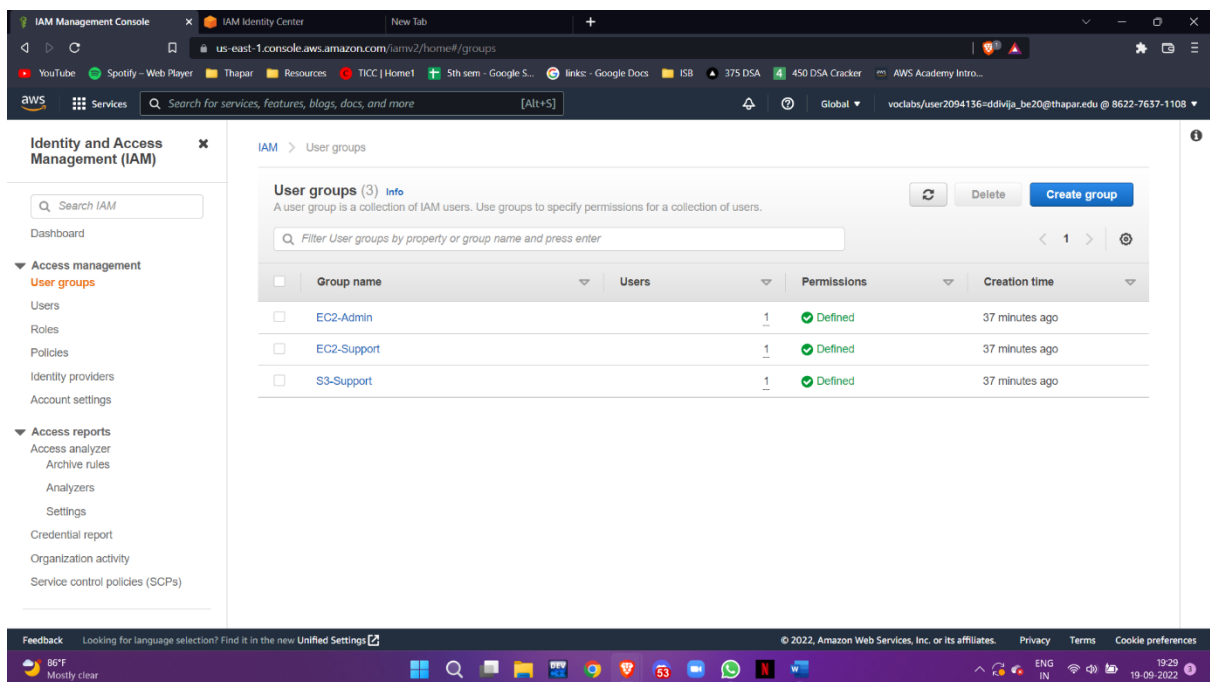
Lab 6 – EBS





Module 7 – Security1

Lab 7 - IAM



The image shows two screenshots of the AWS Management Console. The top screenshot displays the S3 Buckets page in the ap-northeast-1 region. It features a sidebar with navigation options like Buckets, Access Points, and Storage Lens. The main content area shows an 'Account snapshot' and a table of buckets. One bucket is listed with the name 'c53426a85497812675015t1w862276371108-s3bucket-rx6q7s25p3dn', located in the US East (N. Virginia) us-east-1 region, with a creation date of September 19, 2022. The bottom screenshot shows the IAM dashboard. It includes a sidebar for Identity and Access Management (IAM) with sections for Access management and Access reports. The main content area displays 'Security recommendations' (Add MFA for root user), 'IAM resources' (3 user groups, 4 users, 13 roles, 1 policy, 0 identity providers), and 'What's new' updates. A 'Sign-in URL Copied' notification is visible. The right sidebar shows the AWS Account details, including the Account ID 862276371108 and a link to the sign-in URL.

Amazon S3 Buckets

Account snapshot: Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets (1) [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Name	AWS Region	Access	Creation date
c53426a85497812675015t1w862276371108-s3bucket-rx6q7s25p3dn	US East (N. Virginia) us-east-1	Objects can be public	September 19, 2022, 18:52:12 (UTC+0)

Identity and Access Management (IAM)

Search IAM

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

IAM dashboard

Security recommendations 1

Add MFA for root user

Sign in as the root user (or contact your administrator) and register a multi-factor authentication (MFA) device for the root user to improve security for this account.

IAM resources

User groups	Users	Roles	Policies	Identity providers
3	4	13	1	0

What's new [View all](#)

Updates for features in IAM

- Right-size permissions for more roles in your account using IAM Access Analyzer to generate 50 fine-grained IAM policies per day. 10 months ago
- Amazon S3 Object Ownership can now disable access control lists to simplify access management for data in S3. 10 months ago
- Amazon Redshift simplifies the use of other AWS services by introducing the default IAM role. 10 months ago

AWS Account

Account ID: 862276371108

Account Alias: 862276371108 [Create](#)

[Sign-in URL Copied](#) IAM users in this account can use the sign-in URL to access the AWS console.

<https://862276371108.signin.aws.amazon.com/console>

Tools

Policy simulator

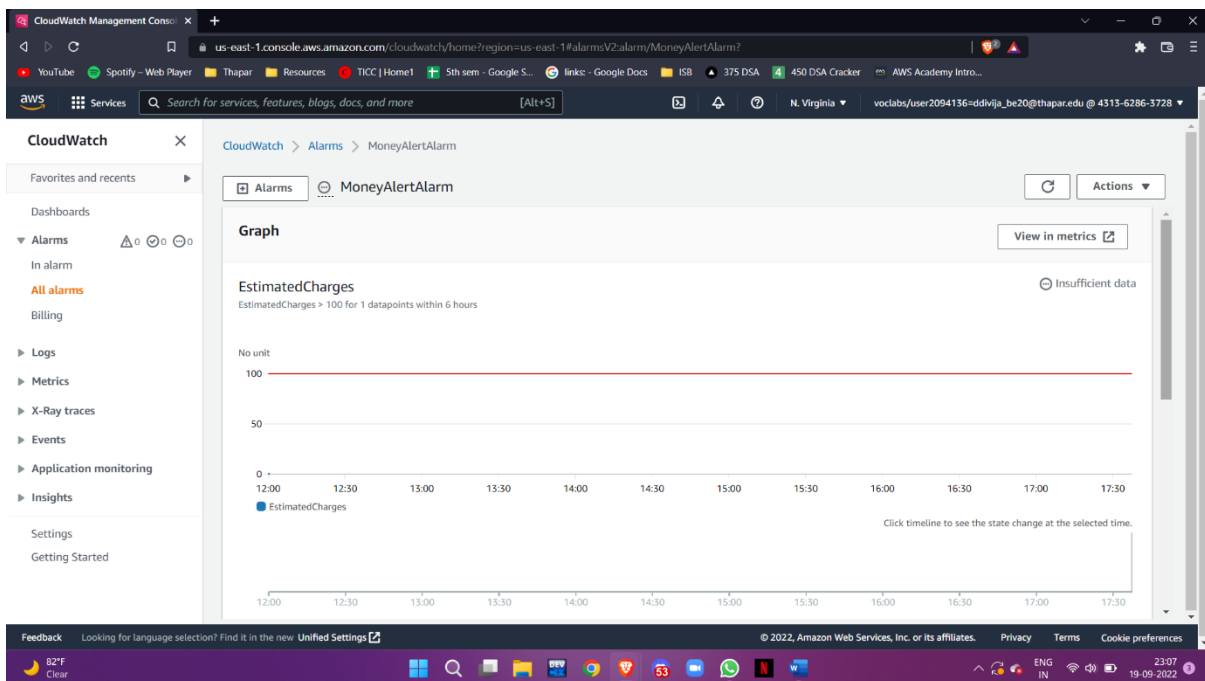
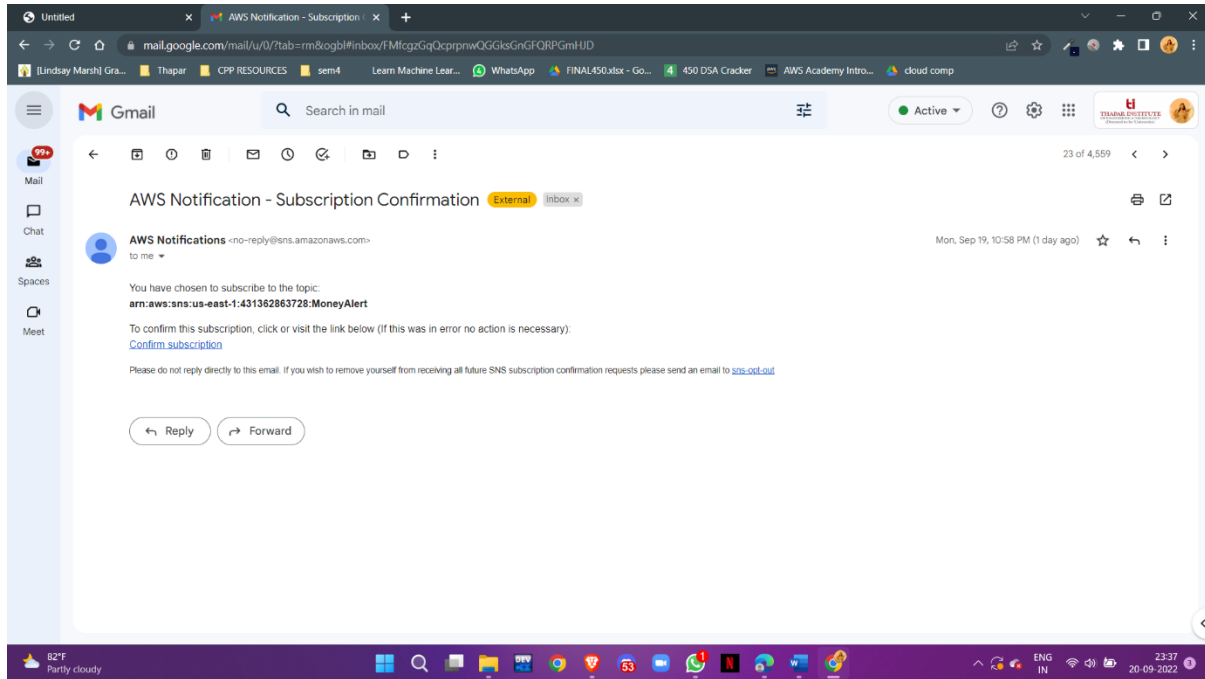
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Web identity federation playground

Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API using the credentials.

Module 9 – Monitoring the Cloud

Lab 9- Monitoring



Thank you