

Security in Cloud Computing and IoT

Lab 1

1. Title:

Use IAM to implement user authentication in AWS. Set up rules to require Multi-Factor Authentication (MFA) for every user.

2. Objective:

The goal of this task is to establish secure user access in AWS by creating IAM users, assigning the appropriate permissions, and requiring Multi-Factor Authentication (MFA) for every account, thereby enhancing security against unauthorized access.

3. Problem Statement:

Different users with various roles require authorized access to AWS accounts. Even default credential-based authentication (password-only) is prone to phishing, brute-force attacks, and credential theft. To guarantee that only authorized users can safely access AWS services, IAM-based identity management must be implemented, and MFA must be enforced.

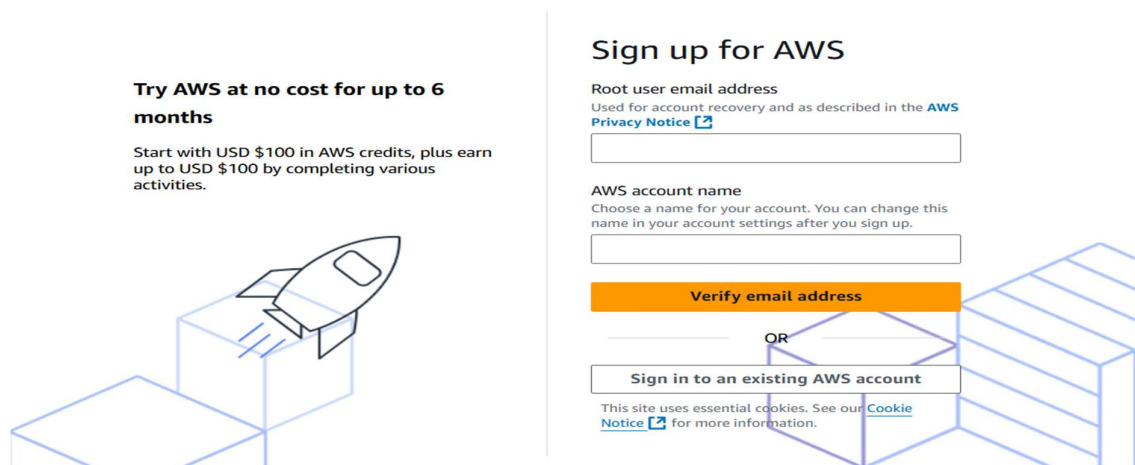
4. Implementation

AWS SIGN-UP GUIDE

Creating an AWS account involves several verification steps to ensure the account is linked to the correct user and can be billed properly. This document provides a clear, step-by-step explanation of the process for new users.

1. Visit the AWS Sign-Up Page:

To begin, visit the official AWS sign-up website and create an account.

A screenshot of the AWS Sign-Up page. On the left, there is a promotional banner for a free trial: "Try AWS at no cost for up to 6 months" and "Start with USD \$100 in AWS credits, plus earn up to USD \$100 by completing various activities." Below the text is an illustration of a rocket ship launching from a cube. On the right, the "Sign up for AWS" form is visible. It includes fields for "Root user email address" (with a link to the AWS Privacy Notice) and "AWS account name" (with instructions to choose a name that can be changed later). Below these fields is an orange "Verify email address" button. Underneath the button is an "OR" separator and a "Sign in to an existing AWS account" button. At the bottom of the form, there is a cookie notice: "This site uses essential cookies. See our Cookie Notice for more information." The background of the form area features a blue wireframe illustration of a server rack.

2. Enter Contact Information

Fill in your name, email as prompted.

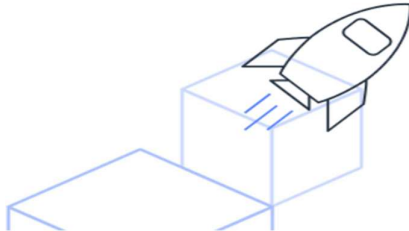
Security in Cloud Computing and IoT

Lab 1



Try AWS at no cost for up to 6 months

Start with USD \$100 in AWS credits, plus earn up to USD \$100 by completing various activities.



Sign up for AWS

Root user email address

Used for account recovery and as described in the [AWS Privacy Notice](#)

timothy_jalli@srmap.edu.in

AWS account name

Choose a name for your account. You can change this name in your account settings after you sign up.

timothyjalli

Verify email address

OR

Sign in to an existing AWS account

This site uses essential cookies. See our [Cookie Notice](#) for more information.

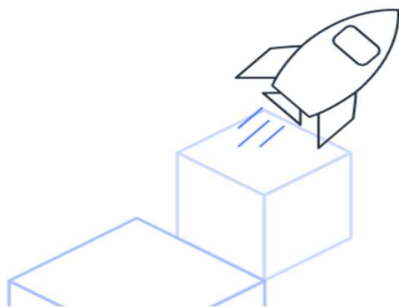
3. Verify Email

A verification code will be sent to your email address. Enter the code to proceed.



Try AWS at no cost for up to 6 months

Start with USD \$100 in AWS credits, plus earn up to USD \$100 by completing various activities.



Sign up for AWS

Confirm you are you

Making sure you are secure -- it's what we do.

We sent an email with a verification code to **timothy_jalli@srmap.edu.in**. (not you?)

Enter it below to confirm your email.

Verification code

069113

Verify

Resend Code 26

Didn't get the code?

- Codes can take up to 5 minutes to arrive.
- Check your spam folder.

This site uses essential cookies. See our [Cookie Notice](#) for more information.

4. Create Root Password

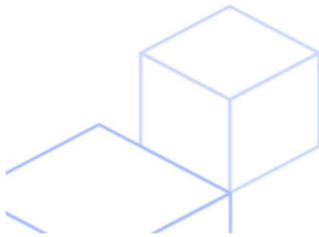
Set a secure password following AWS password requirements.

Security in Cloud Computing and IoT

Lab 1

Try AWS at no cost for up to 6 months

Start with USD \$100 in AWS credits, plus earn up to USD \$100 by completing various activities.



Sign up for AWS

Create your password

✔ It's you! Your email address has been successfully verified. ✕

Your password provides you with sign in access to AWS, so it's important we get it right.

Root user password

.....

Confirm Password
Passwords must be at least 8 characters long and contain at least 3 of the following:

- ☒ Uppercase letters
- ☒ Lowercase letters
- ☒ Numbers
- ☒ Non-alphanumeric characters

OR

[Sign in to an existing AWS account](#)

This site uses essential cookies. See our [Cookie Notice](#) for more information.

5. Identity Confirmation

Confirm your identity again using a verification code sent to your email.

Confirm you're you

We sent an email with a verification code to **timothy_jalli@srmmap.edu.in**

To continue, confirm your identity using the code below.

Verification code

167892

[Verify and continue](#)

[Resend code \(37\)](#)

Didn't get the code?

- Codes can take up to 5min to arrive.
- Check your spam folder.
- Still having [problems signing in?](#)

Run models at scale with cost-effective chips

Our new AI chip, EC2 Trn3 UltraServer, delivers the best token economics for AI applications.

[Explore Trn3](#)

6. Choose Account Type

Select Personal or Business based on usage.

Security in Cloud Computing and IoT

Lab 1



Earn additional AWS credits

Complete various activities to earn up to an additional USD \$100 in credits, such as creating your first AWS budget to monitor cloud costs.



Sign up for AWS

Contact Information

How do you plan to use AWS?

- ☐ Business - for your work, school, or organization
- ☐ Personal - for your own projects

Who should we contact about this account?

Full Name

Country Code

Phone Number

+1

222-555-4444

Country or Region

United States

Address line 1

Address line 2 - optional

Apartment, suite, unit, building, floor, etc.

City

State, Province, or Region

Postal Code

☐ I have read and agree to the terms of the [AWS Customer Agreement](#).

Agree and Continue (step 2 of 5)

7. Provide Address & Phone Details

Enter:

- Full name
- Country
- Address
- Phone number

Agree to terms to continue.

Security in Cloud Computing and IoT

Lab 1



Earn additional AWS credits

Complete various activities to earn up to an additional USD \$100 in credits, such as creating your first AWS budget to monitor cloud costs.



Sign up for AWS

Contact Information

How do you plan to use AWS?

- ☐ Business - for your work, school, or organization
- ☒ Personal - for your own projects

Who should we contact about this account?

Full Name

Timothy_jalli

Country Code Phone Number

+91

8121934555

Country or Region

India

Address line 1

HIG 296, HB Colony, Bhavanipuram

Address line 2 - optional

Apartment, suite, unit, building, floor, etc.

City

Vijayawada

State, Province, or Region

Andhra Pradesh

Postal Code

520012

Nearby AWS Region selection - optional

Enabling nearby AWS Regions can provide benefits including improved performance. Uncheck the Region to prevent its usage. [Learn more](#)

- ☒ Enable Asia Pacific (Hyderabad) Region

Customers with an Indian contact address are served by Amazon Web Services India Private Limited, the local seller for AWS services in India.

- ☐ I have read and agree to the terms of the [AWS Customer Agreement](#)

Agree and Continue (step 2 of 5)

8. Payment Verification

Decide on a payment option. UPI Autopay is available for India.

Use your UPI app to verify payment after entering your UPI ID.

Security in Cloud Computing and IoT Lab 1

The image shows two side-by-side screenshots of the AWS Sign up for AWS page. Both screenshots are identical and show the 'Billing Information' and 'UPI AutoPay' sections. The 'Billing Information' section includes a 'Billing country' dropdown set to 'India', a 'Payment method type' section with 'UPI AutoPay' selected, and a 'UPI AutoPay information' section with a 'UPI ID' field containing '812195455@ybl'. The 'Billing address' section is also visible, showing a contact address in Vijayawada, Andhra Pradesh. A 'Verify and continue (step 3 of 5)' button is at the bottom of each section. A blue shield icon with a checkmark is positioned between the two screenshots.

9. Account Successfully Created

AWS verifies that your account was successfully created and authorized after completing UPI verification.

The image shows two side-by-side screenshots of the Amazon Pay verification process. The left screenshot is a 'Verify your payment method' dialog box with a 'Verify' button and a 'Cancel' button. The right screenshot is the 'Complete your payment' screen, which includes a note: 'Note: Please do not press back button or close the screen until the payment is complete'. It lists steps: 'Go to UPI ID linked mobile app or Click on the notification from your UPI ID linked mobile app', 'Check pending transactions', and 'Complete the payment by selecting the bank and entering UPI PIN'. A progress bar at the bottom indicates 'This page will automatically expire in 10 mins.'.

10. Complete Identity Verification (PAN)

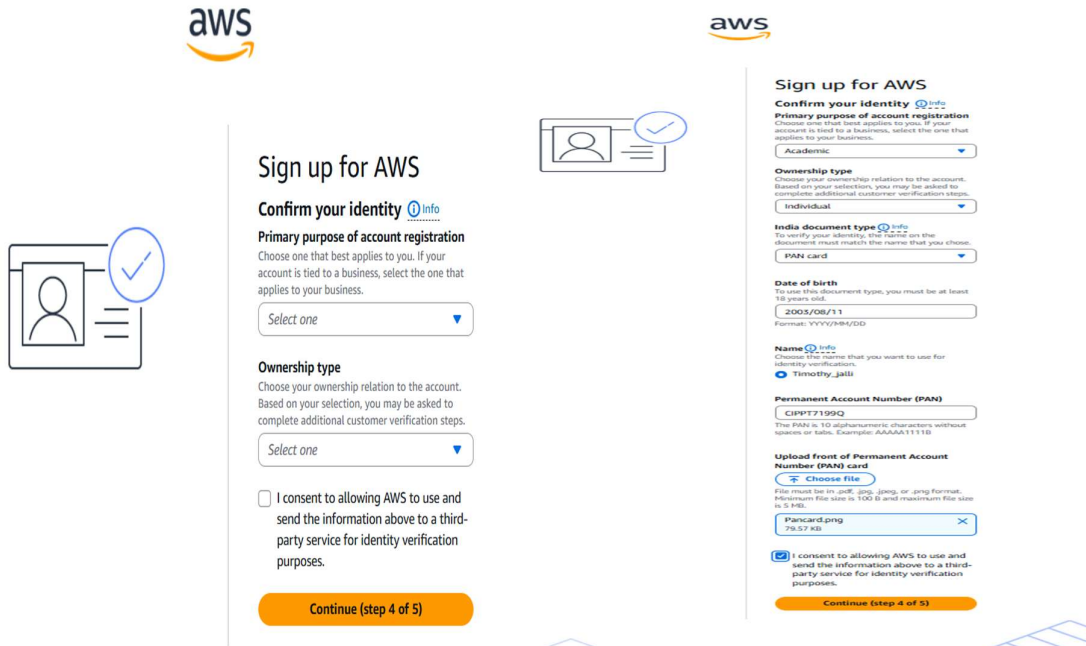
Security in Cloud Computing and IoT

Lab 1

You will be asked to verify your identity using a government-issued document such as PAN.

Steps:

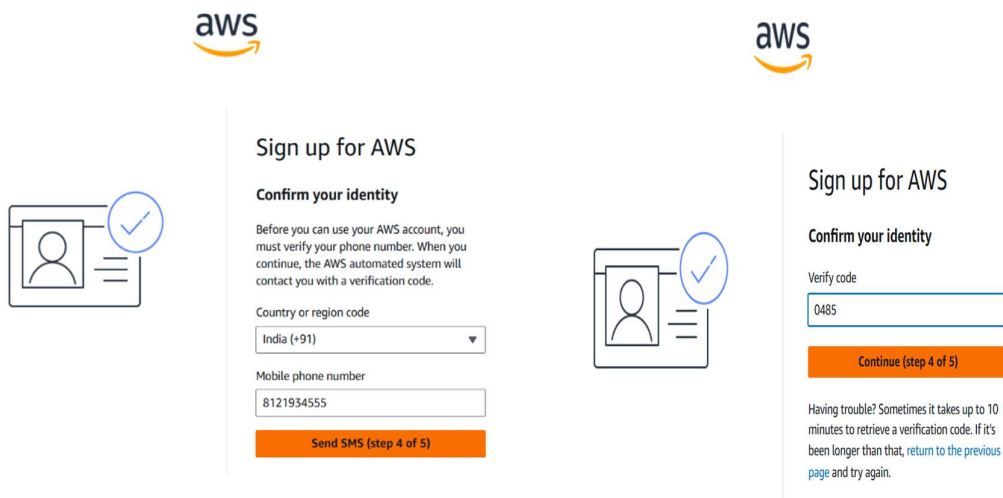
- Select Primary purpose (e.g., Academic)
- Select Ownership type (e.g., Individual)
- Select Document type (e.g., PAN Card)
- Enter Date of birth
- Upload front image of PAN card
- Provide consent and continue



11. Phone Number Verification

AWS will request your mobile number for verification.

- Enter country code
- Enter mobile number
- Click Send SMS
- Enter the OTP received and continue.

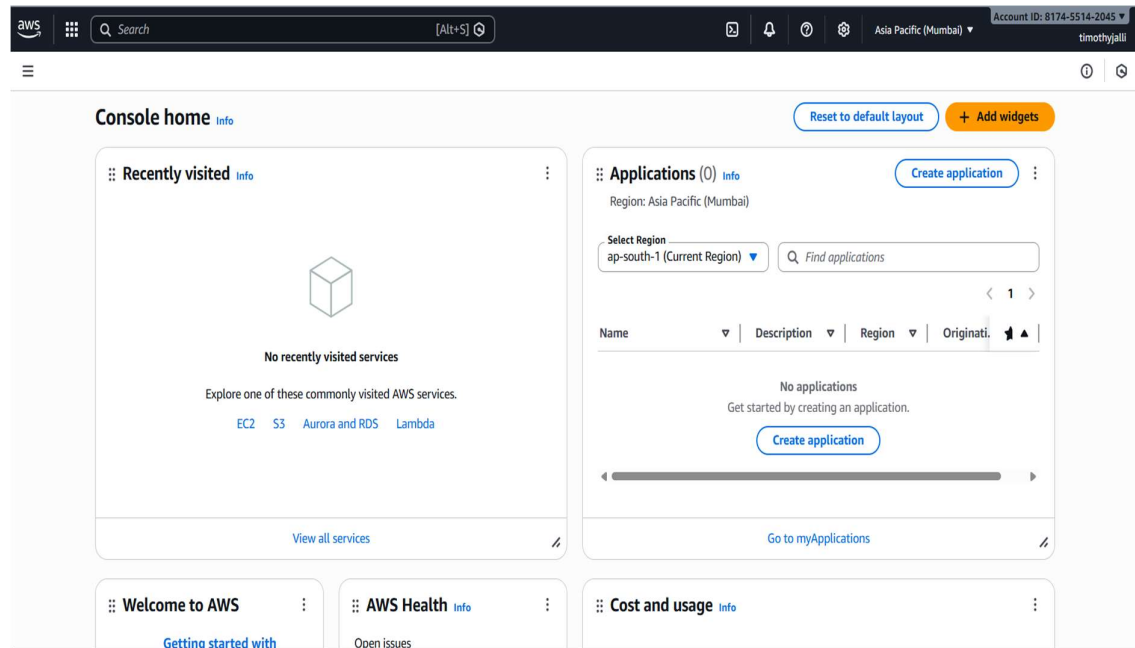


Security in Cloud Computing and IoT

Lab 1

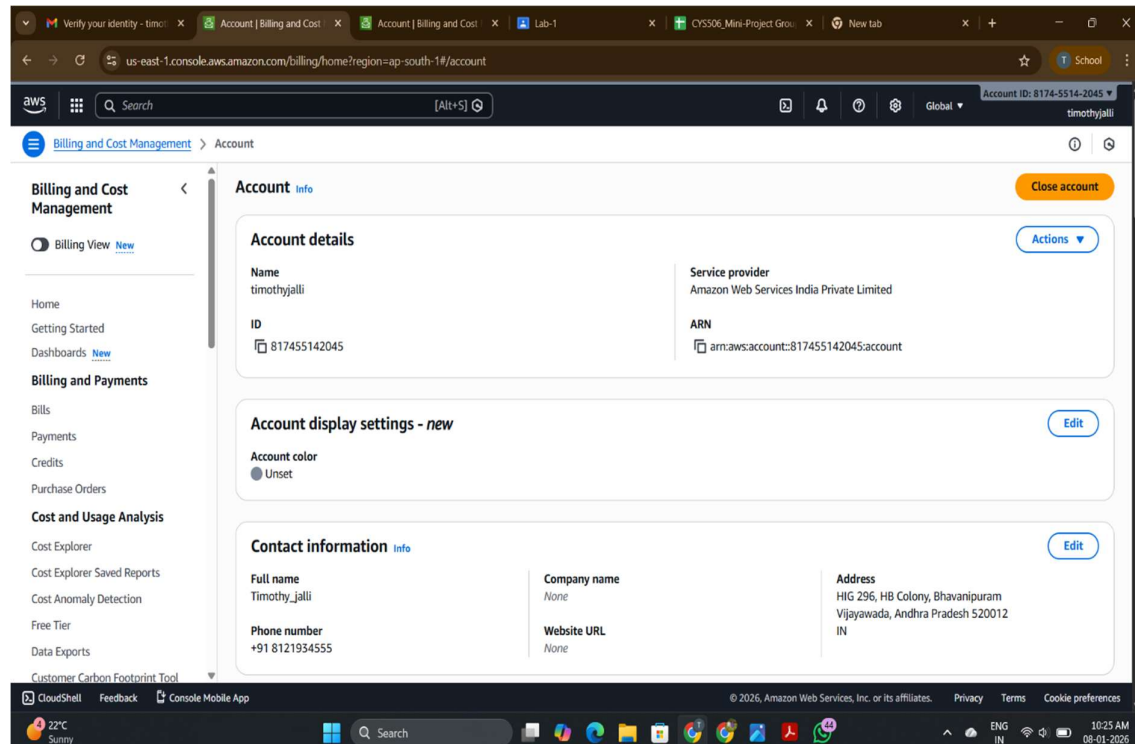
12.AWS Console Access

Once identity verification is completed, you can log in to AWS Management Console. The console provides dashboards for services such as EC2, S3, Lambda, etc.



13.Billing & Account Management

After login, you can view your account details, billing, credits, payment methods, and address under Billing and Cost Management.



Security in Cloud Computing and IoT

Lab 1

14.AWS Login Options

Once everything is set up, AWS gives you two ways to sign in:

- **Root User** – Full administrative access for managing billing, credentials, and critical configurations.
- **IAM User** – Restricted access for daily tasks without exposing sensitive account control.

This completes the AWS sign-up and onboarding flow.

Sign In

Access your AWS account by user type.

User type (not sure?)

☒ **Root user**
Account owner that performs tasks requiring unrestricted access.

☐ **IAM user**
User within an account that performs daily tasks.

Email address
username@example.com

Next

OR

New to AWS? Sign up

By continuing, you agree to [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#).

Get AI-ready, cost-optimized storage

Store and query billions of vectors at up to 90% lower cost for search, RAG, and agent workflows.

Discover S3 Vectors

15.Turn On MFA

AWS asks you to turn on Multi-Factor Authentication (MFA) to make your account safer.

MFA means you need two things to log in:

- Your password
- A code from your phone

To turn it on:

1. Open IAM Dashboard
2. Click Add MFA
3. Choose the phone/authenticator option
4. Scan the QR code and enter the code

IAM Dashboard

Security recommendations

- ⚠️ Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.
- ✅ Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

What's new

Updates for features in IAM

Amazon Q

Hello! I'm Amazon Q, your AWS generative AI assistant.

- Chatting about your resources
- Understanding and optimizing your costs
- Analyzing network troubleshooting
- Investigating operational issues
- Using third party plugins

Ask me anything about AWS

Security in Cloud Computing and IoT

Lab 1

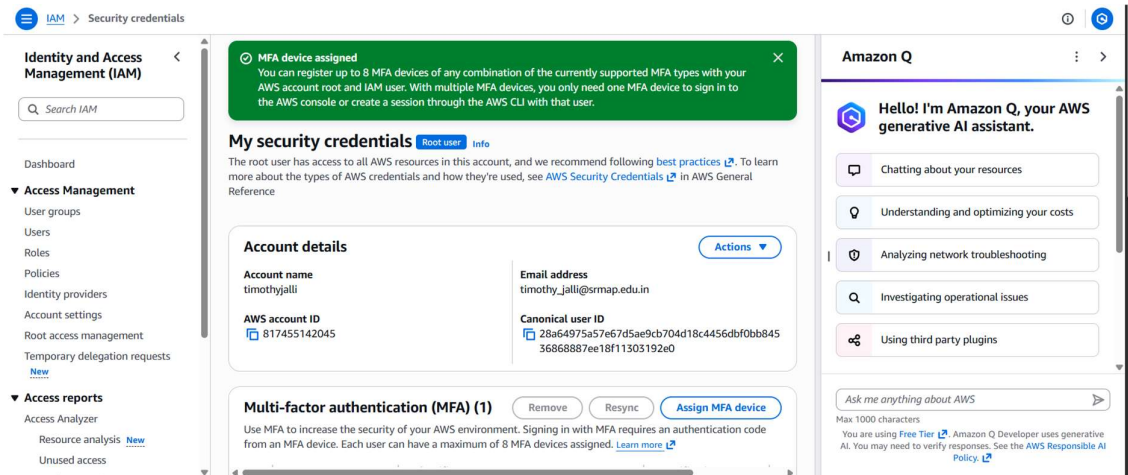
16. MFA Finished

MFA is now added to the root user.

From now on, when logging in as root you must enter:

- Password
- Phone code

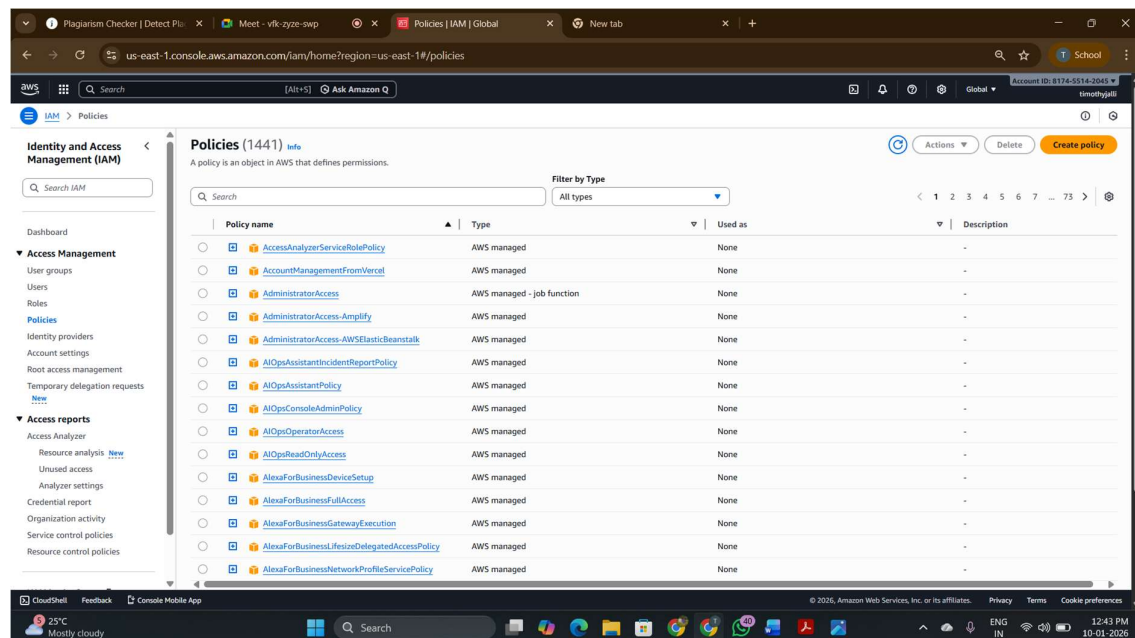
This keeps your AWS account more secure.



CREATING THE MFA ENFORCEMENT POLICY

1. Open IAM Policies

From the AWS Management Console, I opened the **IAM** service and clicked on the **Policies** section to view existing IAM policies.

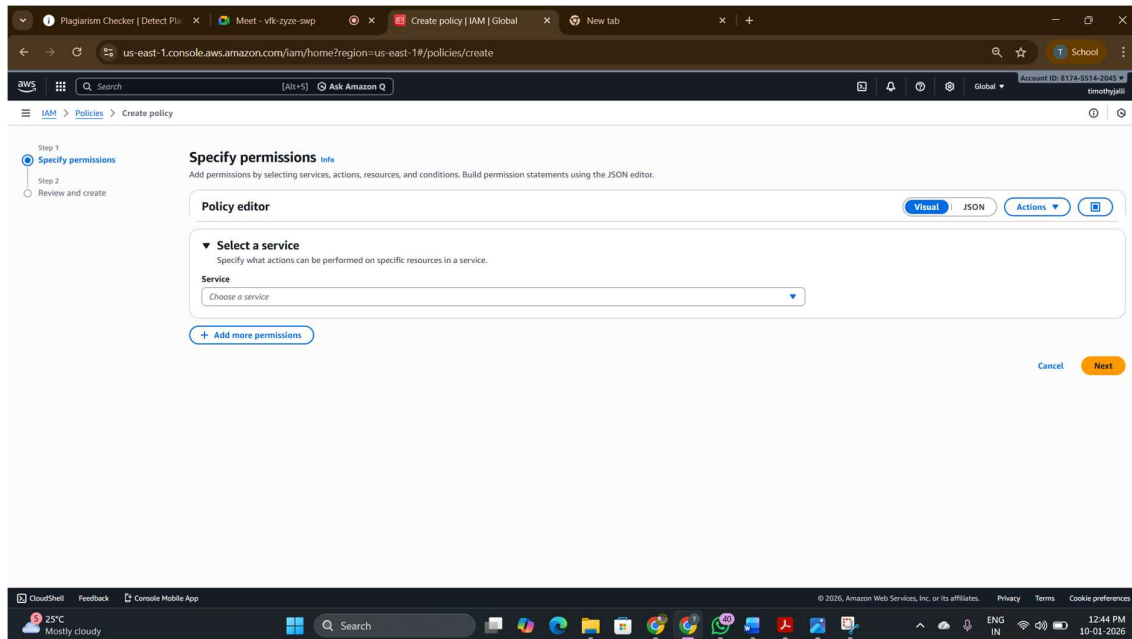


Security in Cloud Computing and IoT

Lab 1

2. Create a New Policy

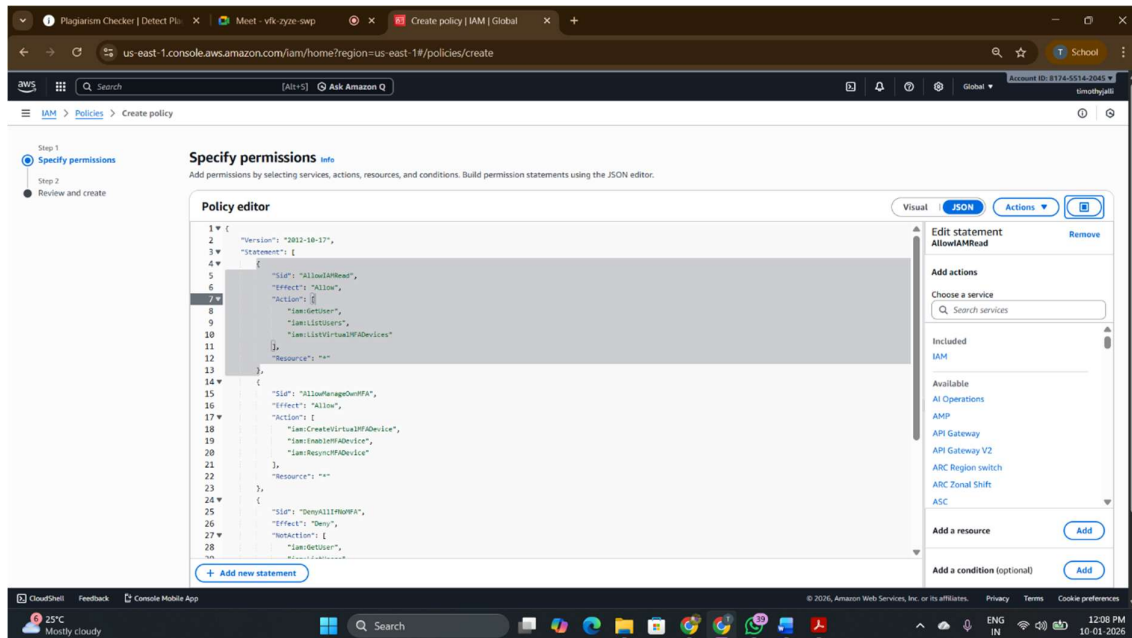
Next, I clicked on the **Create policy** button to start building a new custom IAM policy that will enforce MFA usage.



3. Specify Permissions Using JSON

On the **Specify permissions** page, I switched to the **JSON** tab. In the JSON editor, I added the JSON code that defines the permissions for MFA.

This JSON allows users to view their IAM details, configure their own MFA device, and denies access to other services if MFA is not enabled.



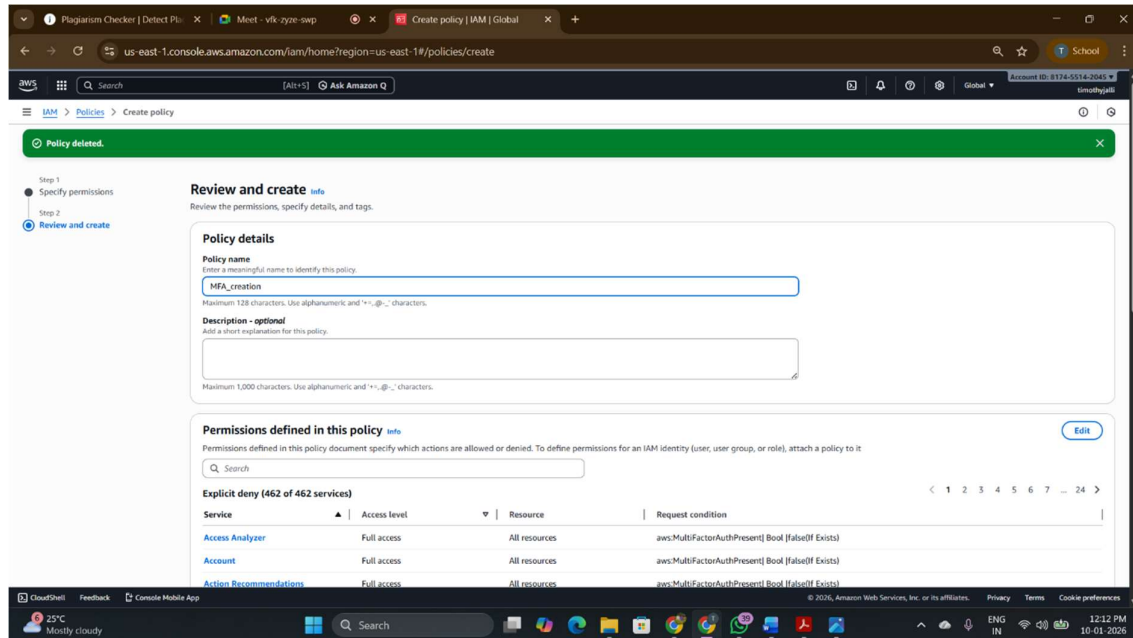
Security in Cloud Computing and IoT

Lab 1

4. Review and Name the Policy

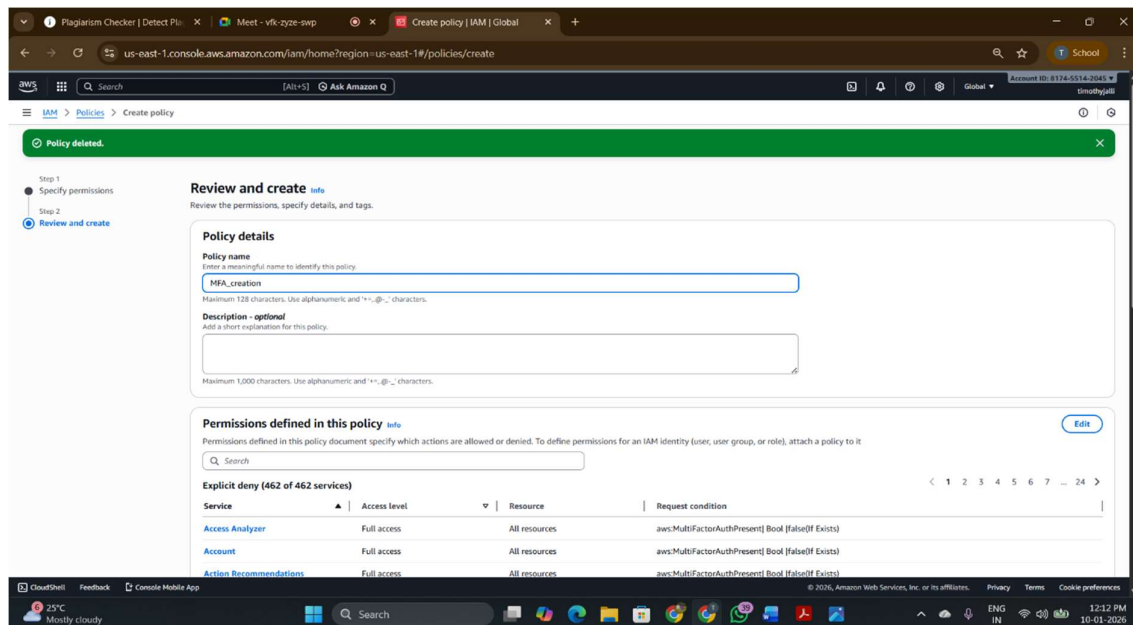
After adding the JSON, I clicked on **Next: Review**.

On the review page, I provided a name for the policy as **MFA_creation**. Adding a description was optional, so I left it blank.



5. Create the Policy

After reviewing the configuration, I clicked on **Create policy**. A confirmation message appeared at the top showing **Policy MFA_creation created**, which confirmed that the policy was successfully created.



Security in Cloud Computing and IoT

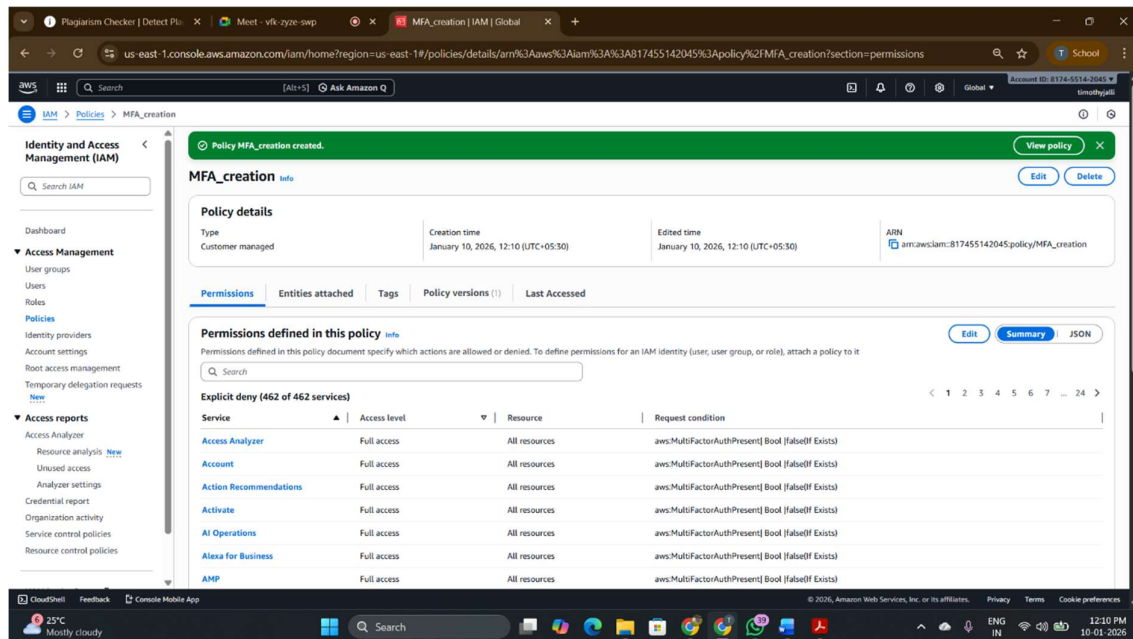
Lab 1

6. Verify Policy Details

I have accessed the policy subsequent to its creation in order to verify the information. The policy described the following information:

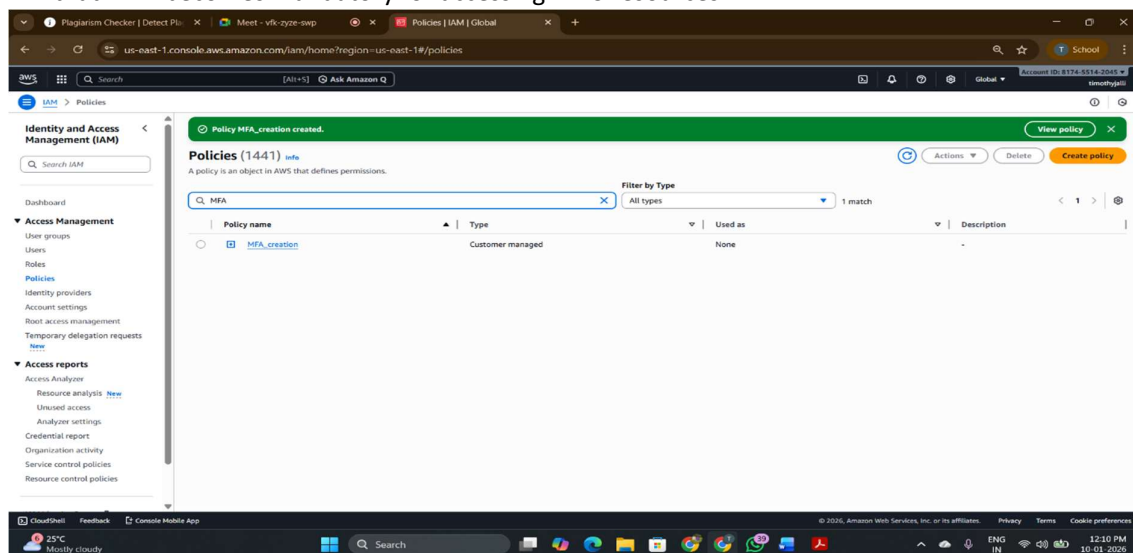
- Policy Name: MFA_creation
- Type: Customer-managed
- Permissions - Explicitly denies access to all services in case MFA is not activated.

The permissions tab listed the AWS services that would require MFA before users could access them.



7. Policy Ready for Use

Once the policy successfully created, it is now ready to be attached to IAM users or groups so that MFA becomes mandatory for accessing AWS resources.



5. Problems Faced During Development:

Various challenges arose during the implementation process. It took more time to sort out IAM policies and actually implement permissions between the different user roles. Also, there was confusion over the differentiation in the application of MFA between the root account and the normal IAM users. The application of MFA added to the delay because users had to pair their authenticator apps and manage time-based codes. After MFA was turned on, some users encountered some problems in logging in due to a lack of readily available verification codes. Also, some sections of the AWS console were not accessible until the correct policies were attached.

6. Conclusion:

Employing IAM in a configuration that implements MFA provides for added security when it comes to AWS environments. In the event of password compromise, unauthorized access is somewhat minimized because a second verification step is still required. IAM further allows detailed access control to be specified, including which AWS actions a principal—which may be an end user in a business or an application—can and cannot do. This prevents both unintentional error and intentional misuse. Overall, it follows the well-documented best practice of cloud security, protecting the critical cloud resource.