

Security in Cloud Computing and IoT

Lab 1

Git Hub Link: https://github.com/charpitha-chavali/Security-in-Cloud-and-IOT/tree/main/06_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.

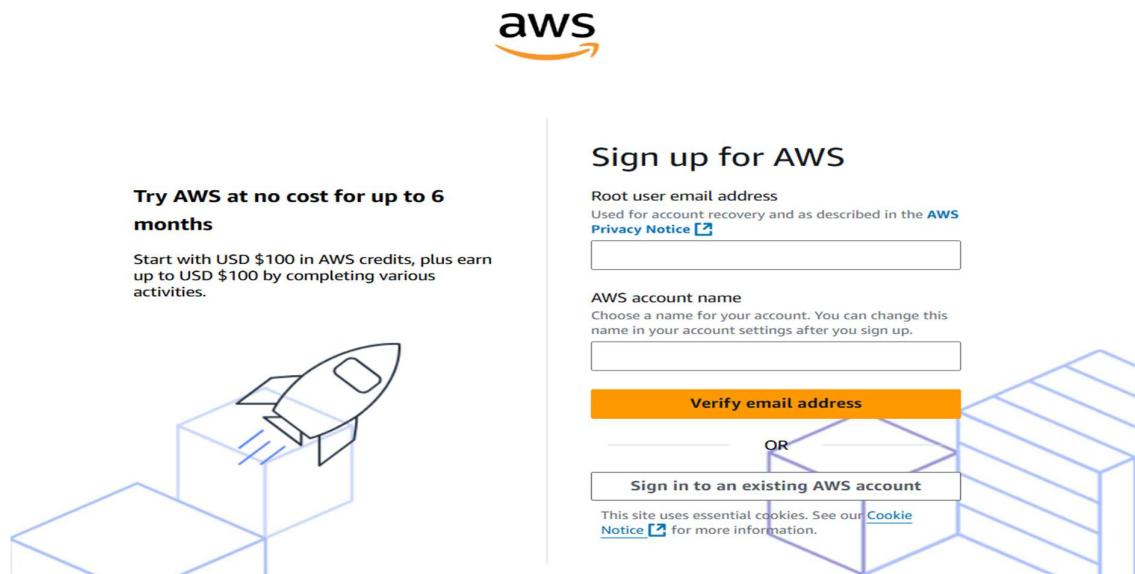
4. Implementation

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.



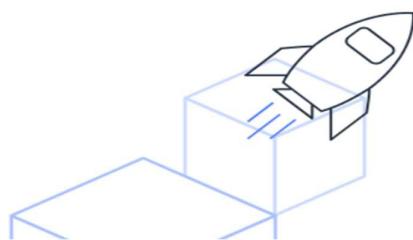
2. Enter Contact Information

Fill in your name, email as prompted.



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@srmep.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.

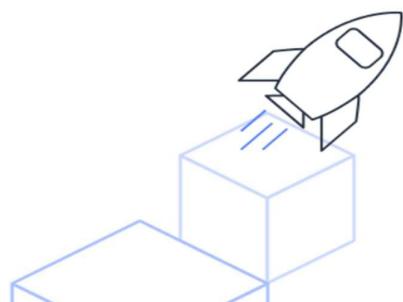
3. Verify Email

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@srmep.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

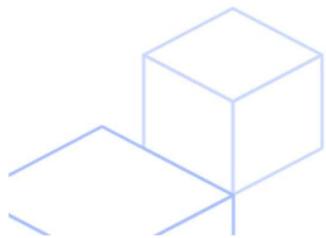
Set a secure password following AWS password requirements.

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.



5. Identity Confirmation

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

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

.....

Conf
 S

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.



aws

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?](#)



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

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 ↗](#).

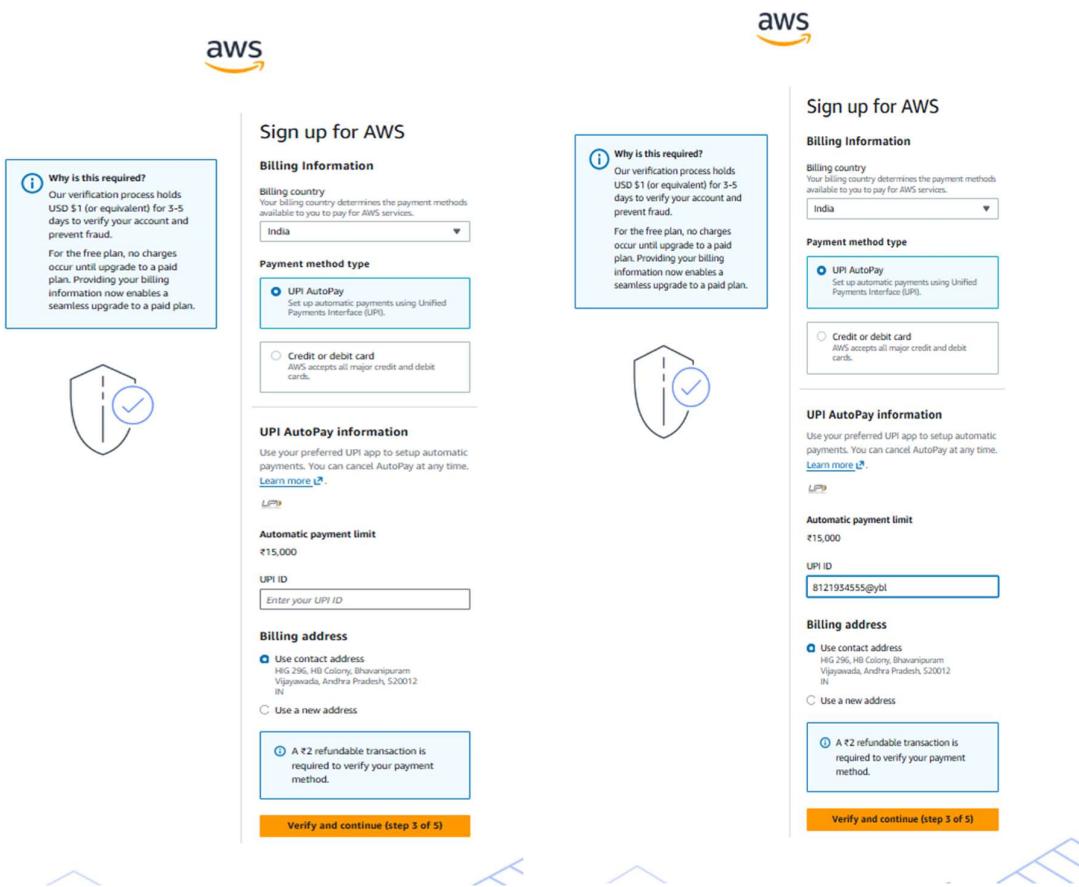
Agree and Continue (step 2 of 5)

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

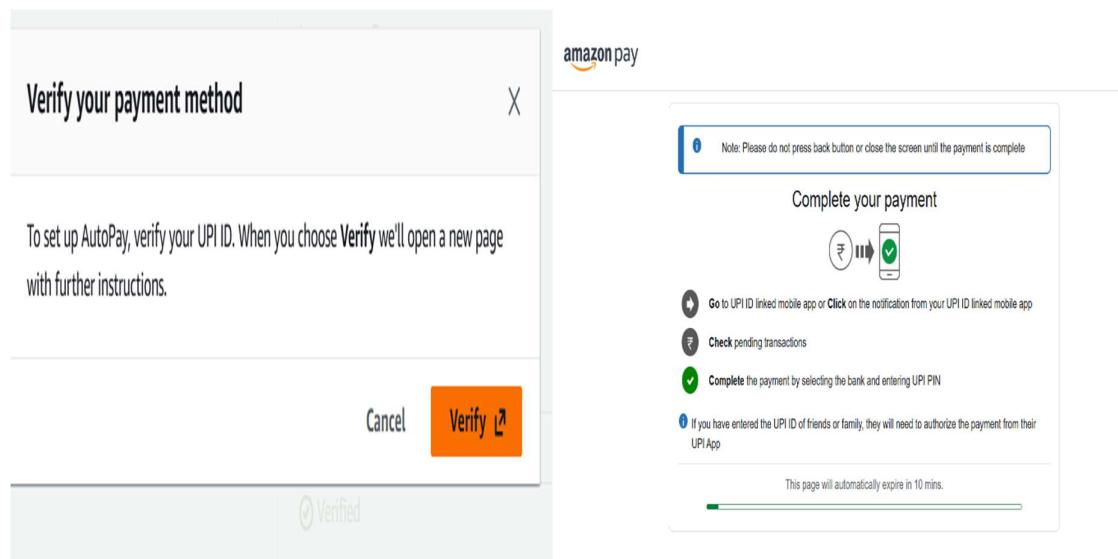
Lab 1



The screenshot shows the third step of the AWS sign-up process, titled "Sign up for AWS". The left panel is titled "Billing Information" and includes fields for "Billing country" (set to India), "Payment method type" (radio button selected for "UPI AutoPay"), and "UPI AutoPay information" (instructions to use a preferred UPI app). The right panel is also titled "Sign up for AWS" and includes "Billing Information" (set to India) and "Payment method type" (radio button selected for "UPI AutoPay"). Both panels have a "Verify and continue (step 3 of 5)" button at the bottom.

9. Account Successfully Created

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



The screenshot shows two Amazon Pay screens. The left screen is titled "Verify your payment method" and contains instructions to set up AutoPay by verifying a UPI ID. It has "Cancel" and "Verify" buttons. The right screen is titled "Complete your payment" and provides instructions: "Go to UPI ID linked mobile app or Click on the notification from your UPI ID linked mobile app", "Check pending transactions", "Complete the payment by selecting the bank and entering UPI PIN", and a note about friends/family authorizing the payment. It also includes a note about the page expiring in 10 minutes.

10. Complete Identity Verification (PAN)

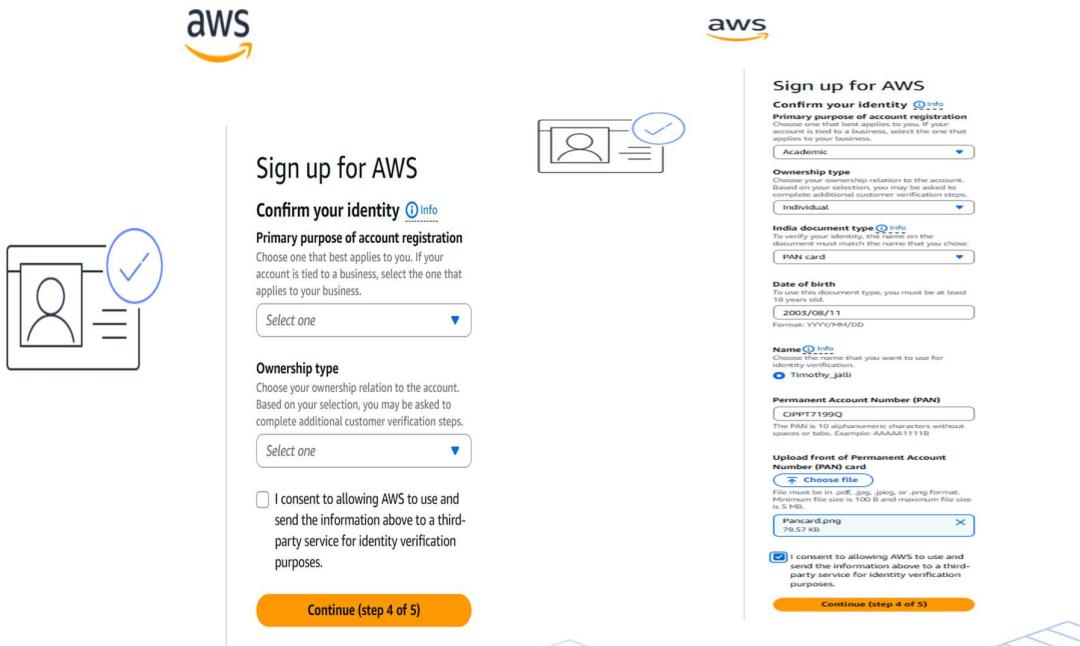
Security in Cloud Computing and IoT

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

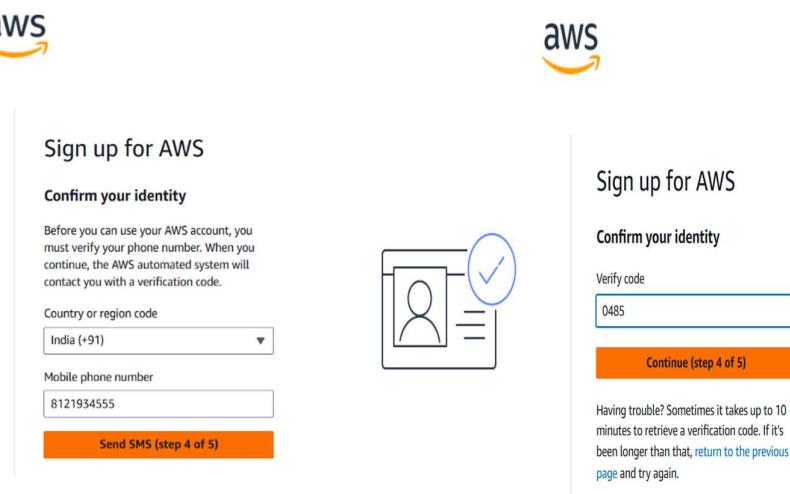


The screenshot shows the fourth step of the AWS sign-up process, titled "Sign up for AWS". It is specifically for "Identity verification". The page includes fields for "Primary purpose of account registration" (set to "Academic"), "Ownership type" (set to "Individual"), "India document type" (set to "PAN Card"), "Date of birth" (set to "2003/08/11"), "Name" (set to "Timothy_jalli"), "Permanent Account Number (PAN)" (set to "CIPPT71199Q"), and an "Upload front of Permanent Account Number (PAN) Card" field containing a file named "Pancard.png". A checkbox for "I consent to allowing AWS to use and send the information above to a third-party service for identity verification purposes." is checked. A large orange "Continue (step 4 of 5)" button is at the bottom.

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.



The screenshot shows the fourth step of the AWS sign-up process, titled "Sign up for AWS". It is specifically for "Phone number verification". The page includes fields for "Country or region code" (set to "India (+91)") and "Mobile phone number" (set to "8121934555"). A "Send SMS (step 4 of 5)" button is at the bottom. To the right, there is a note: "Having trouble? Sometimes it takes up to 10 minutes to retrieve a verification code. If it's been longer than that, [return to the previous page](#) and try again."

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.

The screenshot shows the AWS Management Console home page. At the top right, it displays the account ID: 8174-5514-2045 and the region: Asia Pacific (Mumbai). The main dashboard includes sections for 'Recently visited' services (empty), 'Applications' (empty), 'Welcome to AWS' (empty), 'AWS Health' (empty), and 'Cost and usage' (empty). A search bar at the top left and a navigation menu on the left side are also visible.

13.Billing & Account Management

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

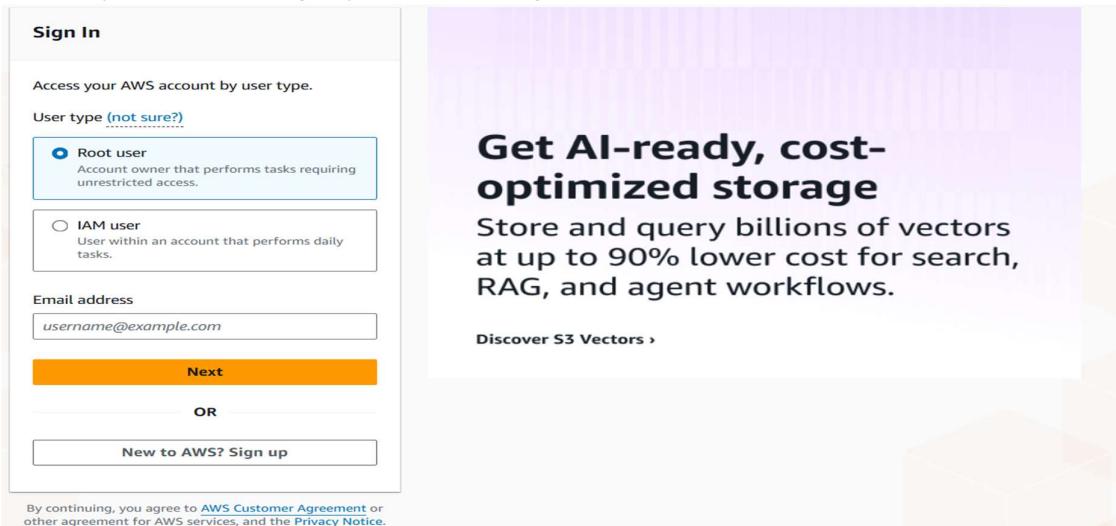
The screenshot shows the AWS Billing and Cost Management console. The left sidebar lists categories like 'Billing and Cost Management', 'Billing View', 'Home', 'Getting Started', 'Dashboards', 'Billing and Payments', 'Bills', 'Payments', 'Credits', 'Purchase Orders', 'Cost and Usage Analysis', 'Cost Explorer', 'Cost Explorer Saved Reports', 'Cost Anomaly Detection', 'Free Tier', 'Data Exports', and 'Customer Carbon Footprint Tool'. The main content area is titled 'Account' and shows 'Account details' (Name: timothyjalli, ID: 817455142045, Service provider: Amazon Web Services India Private Limited, ARN: arn:aws:account:817455142045:account) and 'Account display settings - new' (Account color: Unset). Below that is 'Contact information' (Full name: Timothy_jalli, Company name: None, Phone number: +91 8121934555, Website URL: None, Address: HIG 296, HB Colony, Bhavanipuram, Vijayawada, Andhra Pradesh 520012, IN).

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.



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

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.

The screenshot shows the AWS IAM Security credentials page. A green banner at the top states "MFA device assigned" with a note about registering up to 8 devices. Below this, the "My security credentials" section shows a "Root user" with an "Info" link. The "Account details" section lists the account name (timothy_jalli), email address (timothy_jalli@srmmap.edu.in), AWS account ID (817455142045), and canonical user ID (28a64975a57e67d5ae9cb704d18c4456dbf0bb84536868887ee18f11303192e0). The "Multi-factor authentication (MFA) (1)" section shows one MFA device assigned. On the right, the Amazon Q AI assistant is visible, providing various AI-generated responses about AWS resources, costs, troubleshooting, and operational issues.

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.

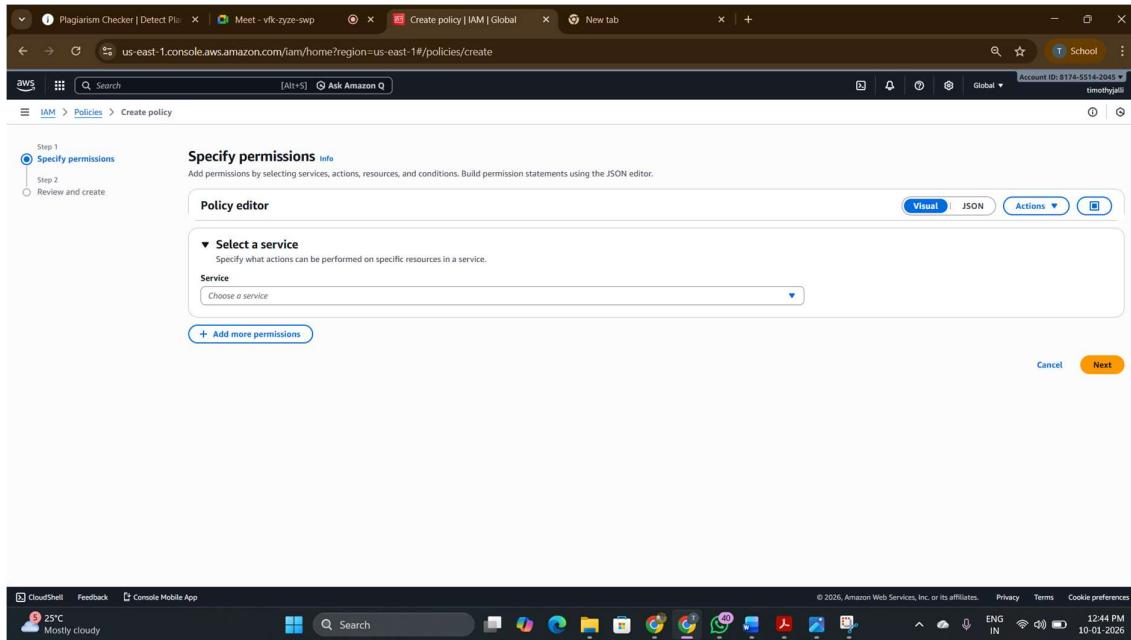
The screenshot shows the AWS IAM Policies page. The left sidebar navigation includes "Identity and Access Management (IAM)", "Access Management", "Policies", and "Access reports". The main content area displays a table titled "Policies (1441)" with a "Create policy" button. The table lists 1441 policies, filtered by type (AWS managed), showing columns for Policy name, Type, Used as, and Description. The table includes pagination and search functionality. The status bar at the bottom indicates the browser version (CloudShell Feedback - Console Mobile App), weather (25°C Mostly cloudy), and system information (Privacy Terms Cookie preferences, ENG IN, 10-01-2026).

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.

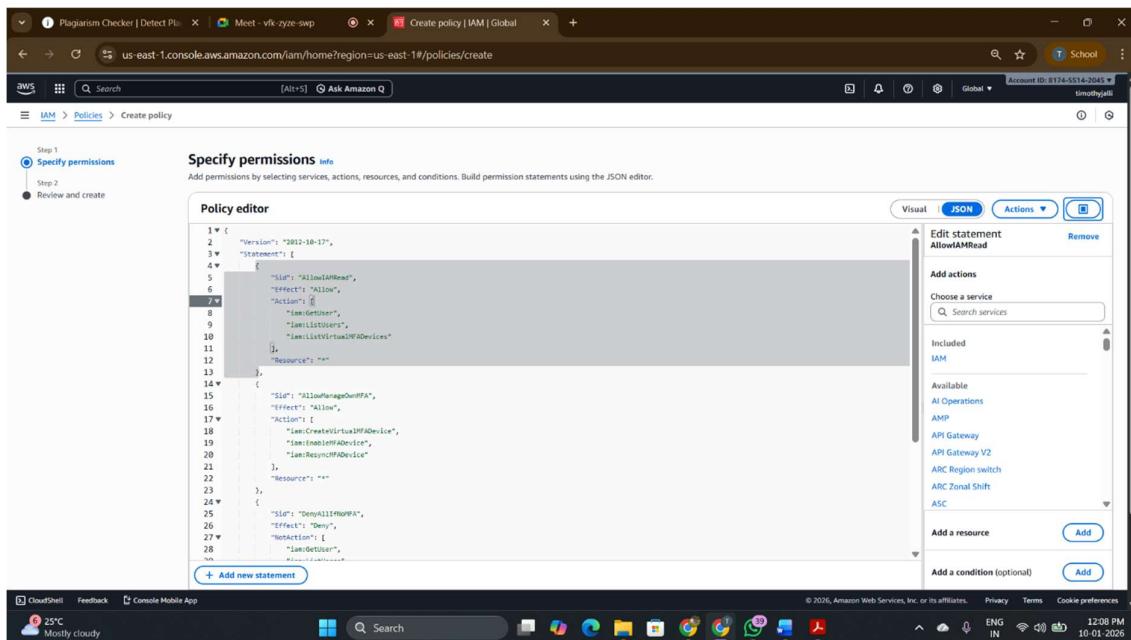


The screenshot shows the AWS IAM 'Create policy' wizard. The 'Specify permissions' step is active. In the 'Policy editor', the 'Select a service' dropdown is open, showing 'Choose a service'. Below it is a 'Add more permissions' button. At the bottom right are 'Cancel' and 'Next' buttons. The status bar at the bottom indicates a Windows desktop environment with various icons and a weather widget showing '25°C Mostly cloudy'.

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.



The screenshot shows the 'Specify permissions' page with the 'JSON' tab selected. A large block of JSON code is displayed:

```
1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Sid": "AllowMFARead",
5         "Effect": "Allow",
6         "Action": [
7             "iam:GetUser",
8             "iam:ListUsers",
9             "iam:ListVirtualMFADevices"
10            ],
11            "Resource": "*"
12        },
13        {
14            "Sid": "AllowManageOwnMFA",
15            "Effect": "Allow",
16            "Action": [
17                "iam:CreateVirtualMFADevice",
18                "iam:DeleteVirtualMFADevice",
19                "iam:ResyncMFADevice"
20            ],
21            "Resource": "*"
22        },
23        {
24            "Sid": "DenyAllMFANoMFA",
25            "Effect": "Deny",
26            "NotAction": [
27                "iam:GetUser",
28                "iam:ListVirtualMFADevices"
29            ]
30        }
31    ]
32 }
```

The right side of the screen shows the 'Edit statement' panel with options like 'AllowMFARead', 'Add actions', and 'Included IAM'. The status bar at the bottom indicates a Windows desktop environment.

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.

A screenshot of a web browser showing the AWS IAM 'Create policy' interface. The URL is 'us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create'. The top navigation bar shows 'Plagiarism Checker | Detect Pl...', 'Meet - vfk-zyze-swp', and 'Create policy | IAM | Global'. The main content area has a green banner at the top that says 'Policy deleted.' Below this, there are two tabs: 'Specify permissions' (selected) and 'Review and create'. The 'Review and create' tab has a sub-section titled 'Policy details' where the 'Policy name' is set to 'MFA_creation'. There is also a 'Description - optional' field which is empty. Below this is a table titled 'Permissions defined in this policy' with the note 'Explicit deny (462 of 462 services)'. The table lists three services: 'Access Analyzer', 'Account', and 'Action Recommendations', each with 'Full access' and the 'Request condition' 'aws:MultiFactorAuthPresent Bool [false]If Exists'. At the bottom of the page, there is a footer with links for 'CloudShell', 'Feedback', 'Console Mobile App', and weather information ('25°C Mostly cloudy'). The status bar shows 'ENG IN 12:12 PM 10-01-2026'.

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.

A screenshot of a web browser showing the AWS IAM 'Create policy' interface, identical to the previous one but with a green banner at the top that says 'Policy created.' The rest of the interface is the same, showing the 'Review and create' step with the 'MFA_creation' policy name and the 'Explicit deny (462 of 462 services)' table.

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.

This screenshot shows the 'MFA_creation' policy details page in the AWS IAM console. The policy was created on January 10, 2026, at 12:10 UTC. It has an ARN: arn:aws:iam::817455142045:policy/MFA_creation. The 'Permissions' tab is selected, showing a table titled 'Explicit deny (462 of 462 services)'. The table lists various AWS services with their access level (Full access), resource (All resources), and request condition (aws:MultiFactorAuthPresent| Bool [false]if Exists). The table includes columns for Service, Access Level, Resource, and Request condition.

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.

This screenshot shows the 'Policies' list page in the AWS IAM console. A search bar at the top is set to 'MFA'. The results table shows one entry: 'MFA_creation' (Policy name, Type: Customer managed, Used as: None). The table includes columns for Policy name, Type, Used as, and Description.

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.