



# Vidyavardhini's College of Engineering and Technology

## Department of Artificial Intelligence & Data Science

### Experiment No. 8

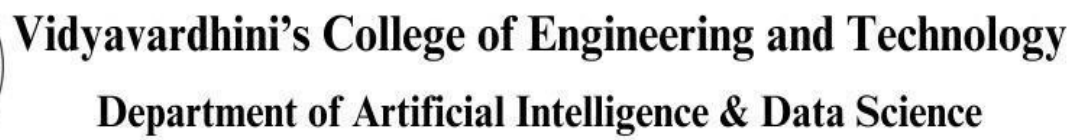
**Aim:** To study and implement Identity and Access Management (IAM) practices on AWS

**Theory:**

- Identity Management is a set of business processes, and a supporting infrastructure, for the creation, maintenance and use of digital identities.
- IAM is an essential function for protecting the privacy of information, enhancing user experience, enabling accountability, and controlling access to an organization's assets.
- IAM is the collection of processes and technology used to manage digital identities and the resource access provided through them.
- Components of access management
  - Establishing unique identities and associated authentication credentials.
  - Authoritative source is maintained as a central repository for storage.
  - Providing capability to identities to request entitlements
  - Assigning roles or entitlements to identities.
  - Managing off boarding and other business work processes by workflows
  - Providing capability to approve, revoke, review or certify entitlements or roles assigned to users.

**Output:**

The screenshot displays the AWS IAM console interface. On the left, a green success message states: "Success. You successfully created the users shown below. You can view and instructions for signing in to the AWS Management Console. This is you can create new credentials at any time. Users with AWS Management Console access can sign-in at: https://". Below this message is a "Download .csv" button and a table with one user named "saurav". On the right, a "Sign in" overlay is visible, featuring radio buttons for "Root user" (selected) and "IAM user". It includes a text input for "Root user email address" with the placeholder "username@example.com", a "Next" button, and a "Create a new AWS account" button at the bottom. The footer of the console shows a feedback link and a language selection notice.



The screenshot shows the AWS Management Console for the Asia Pacific (Tokyo) region. The left sidebar contains navigation links for various services, with 'Instances' selected. The main content area is titled 'Resources' and shows a table of EC2 resources. Each resource has a red error icon and a message. Below the table, there is a section for 'Launch instance' with a yellow highlight on the 'Launch instance' button. To the right, the 'Service health' section shows the AWS Health Dashboard with a green status indicator.

Resource	Status
Instances (running)	API Error
Dedicated Hosts	API Error
Elastic IPs	API Error
Instances	API Error
Key pairs	API Error
Load balancers	API Error
Placement groups	API Error
Security groups	API Error
Snapshots	API Error
Volumes	API Error

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

**Launch instance** **Migrate a server**

**Service health**

Region: Asia Pacific (Tokyo)

Status: **This service is operating normally**



# Vidyavardhini's College of Engineering and Technology

## Department of Artificial Intelligence & Data Science

The screenshot shows the AWS IAM console interface. On the left, there's a navigation menu with options like 'Access management', 'Access reports', and 'Credential report'. The main content area is titled 'Add permissions' and shows a policy named 'AmazonEC2FullAccess' attached directly to the user 'saurav'. The policy summary is displayed in JSON format, showing actions like 'ec2:\*', 'elasticloadbalancing:\*', and 'cloudwatch:\*' with an effect of 'Allow'.

The screenshot shows the AWS IAM console interface. On the left, there's a navigation menu with options like 'Access management', 'Access reports', and 'Credential report'. The main content area is titled 'Users (1) Info' and shows a table with one user, 'saurav'. The table has columns for 'User name', 'Groups', 'Last activity', 'MFA', and 'Password age'. The user 'saurav' is listed with 'None' for groups, '7 minutes ago' for last activity, and no MFA or password age information.

**Conclusion:** In AWS IAM (Identity and Access Management), users are entities that represent individuals or services interacting with AWS resources. Users are granted permissions through IAM policies, which specify what actions they can perform on which AWS resources. IAM allows you to



# Vidyavardhini's College of Engineering and Technology

## Department of Artificial Intelligence & Data Science

---

create, manage, and delete users, enabling you to control access to your AWS environment securely. Users can have unique credentials (such as username and password) or use temporary security credentials for programmatic access. By managing users and their permissions, IAM helps organizations enforce the principle of least privilege, ensuring that users have only the access they need to perform their tasks.