Experiment No. 8

Aim: To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud

Objective: Understand the working of Identity and Access Management IAM in cloud computing and to demonstrate the case study based on Identity and Access Management (IAM) on AWS/Azure cloud platform

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.

Steps:

----- Configuring IAM Dashboard -----

1. Go to IAM dashboard
2. Click on create option under Account Alias and give a valid name; save changes
3. (Download Google Authenticator from PlayStore in your Mobile Phone)

----- Configuring IAM Dashboard -----

1. Click on "users" in the left column
2. Click on Add users button
3. Set a custom valid psw (Imc: Qwertyuiop123) and check the Require psw rest box which will make you create a next psw in the next sign in
4. Click on Next: Tags
5. Add a tag if you want to just to keep track of your activities; then click on Next: Review