

## **WEEK-5 Project: IAM & Cloud Service Models**

### **Part 1:**

#### **Cloud Service Models:**

1. **IaaS** (Infrastructure as a Service)
2. **PaaS** (Platform as a Service)
3. **SaaS** (Software as a Service)

#### **1.IaaS (Infrastructure as a Service):**

- User manage everything except hardware
- IaaS provides basic computing resources such as virtual machines, storage, and networking. We are responsible for installing and managing operating systems and applications.

#### **Example:** Amazon EC2.

**Explain:** Using Amazon EC2 is like renting a computer online where you decide what software to install and how to use it.

#### **2.PaaS (Platform as a Service)**

- User manage only on application
- PaaS provides a ready-made platform where the infrastructure and operating system are managed by the provider. We only focus on using or running applications.

#### **Example:** AWS Elastic Beanstalk

**Explain:** Elastic Beanstalk allows developers to upload application code while AWS manages servers, scaling, and maintenance automatically. Like If we use Blogspot we just create content and platform is managed by CSP.

#### **3.SaaS (Software as a Service)**

- User just use the software
- SaaS delivers fully functional software applications over the internet. Users simply use the application without worrying about installation or maintenance.

#### **Example:** Amazon WorkDocs.

**Explain:** Amazon WorkDocs allows users to store, share, and collaborate on documents through a web browser without managing servers or software updates. Like Google drive, Gmail allowing users to store and share files using a web browser.

## Difference between IaaS, PaaS and SaaS.

Feature	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
<b>What is provided</b>	Virtual machines, storage, networking	Platform with OS, runtime, tools	Fully ready software
<b>User responsibility</b>	Manage OS, apps, and data	Manage application and data	Only use the software
<b>Provider manages</b>	Hardware, data center, networking	Infrastructure + OS + runtime	Everything
<b>Technical knowledge needed</b>	High	Medium	Low
<b>Flexibility</b>	Very high	Medium	Low
<b>Setup time</b>	Amazon EC2	Quick	Immediate
<b>Common man example</b>	Renting a computer online	Using Blogspot/Wix to create a site	Using Gmail, Netflix
<b>AWS example</b>	Amazon EC2	AWS Elastic Beanstalk	Amazon WorkDocs
<b>Best suited for</b>	System admins, IT teams	Application developers	End users

## Part 2:

### IAM

In this activity, AWS Identity and Access Management (IAM) was used to create and manage users, groups, and permissions. Different access levels were assigned using IAM groups and policies based on user roles. An inline policy was also created to restrict access to specific AWS services and regions. This activity helps in understanding secure access control in AWS.

#### 1. IAM Console showing created users and their assigned groups:

In this activity, IAM users and groups were created to demonstrate access management in AWS. DevUser was assigned to the Developers group with EC2 read-only access, and AdminUser was assigned to the Admins group with full administrative privileges and also an AuditUser was created without adding it to any of the groups.

The screenshot shows the AWS IAM console interface. On the left, there's a navigation sidebar with options like Dashboard, Access management, and Access reports. The main area shows a success message: "User created successfully". Below it, a table lists three IAM users: AdminUser, AuditUser, and DevUser. The AdminUser is in the Admins group, AuditUser is in the Auditors group, and DevUser is in the Developers group. Each user row has a "View user" button and a "Delete" button.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access
AdminUser	/	1	-	-	-	-	-
AuditUser	/	0	-	-	-	-	-
DevUser	/	1	-	-	-	-	-

## 2. IAM Console showing the inline policy attached to AuditUser

An inline IAM policy was created and attached directly to AuditUser to allow access only to Amazon S3 services restricted to the us-east-1 region, following the principle of least privilege.

The screenshot shows the AWS IAM console interface. On the left, there's a navigation sidebar with options like Dashboard, Access management (Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests), and Access reports (Access Analyzer, Resource analysis). The main content area is titled 'AuditUser info' and shows the 'Summary' tab. It includes fields for ARN (arn:aws:iam::370703431304:user/AuditUser), Created (December 14, 2025, 21:41 (UTC+05:30)), Console access (Disabled), and Last console sign-in (-). There's also a section for Access key 1 with a 'Create access key' button. Below this is the 'Permissions' tab, which lists 'Permissions policies (1)'. A single policy named 'AuditS3UsEast1Policy' is shown, categorized as 'Customer inline' and 'Attached via [inline]'. The policy is described as allowing S3 actions in the us-east-1 region. The bottom of the screen shows the standard Windows taskbar with various pinned icons and system status information.