PES UNIVERSITY

CELEBRATING 50 YEARS

CLOUD SERVICES

S Thenmozhi

Department of Computer Applications

CLOUD SERVICES

Cloud Computing Essentials

S Thenmozhi

Department of Computer Applications

Identity and Access Management

Identity and Access Management (IDAM) for cloud describes the authentication and authorization of users to provide secure access to cloud resources.

Organizations with multiple users can use IDAM services provided by the cloud service provider for management of user identifiers and user permissions.

IDAM services allow organizations to centrally manage users, access permissions, security credentials and access keys.

Identity and Access Management

Organizations can enable role-based access control to cloud resources and applications using the IDAM services.

IDAM services allow creation of user groups where all the users in a group have the same access permissions.

Defining and managing roles and access privileges for individual network users and circumstances to grant privileges

IAM

One digital entity per individual

Once the digital identity is established it should be maintained, modified and monitored through a user’s access life cycle

Administering user access across an entire enterprise and ensure compliance with corporate policies and government regulations.

Password-management tools, provisioning software, security-policy enforcement applications, reporting and monitoring apps and identity repositories

IAM

IAM can be provided by OpenAuth, Role-based Access Control (RBAC), Digital Identities, Security Tokens, Identity Providers, etc.

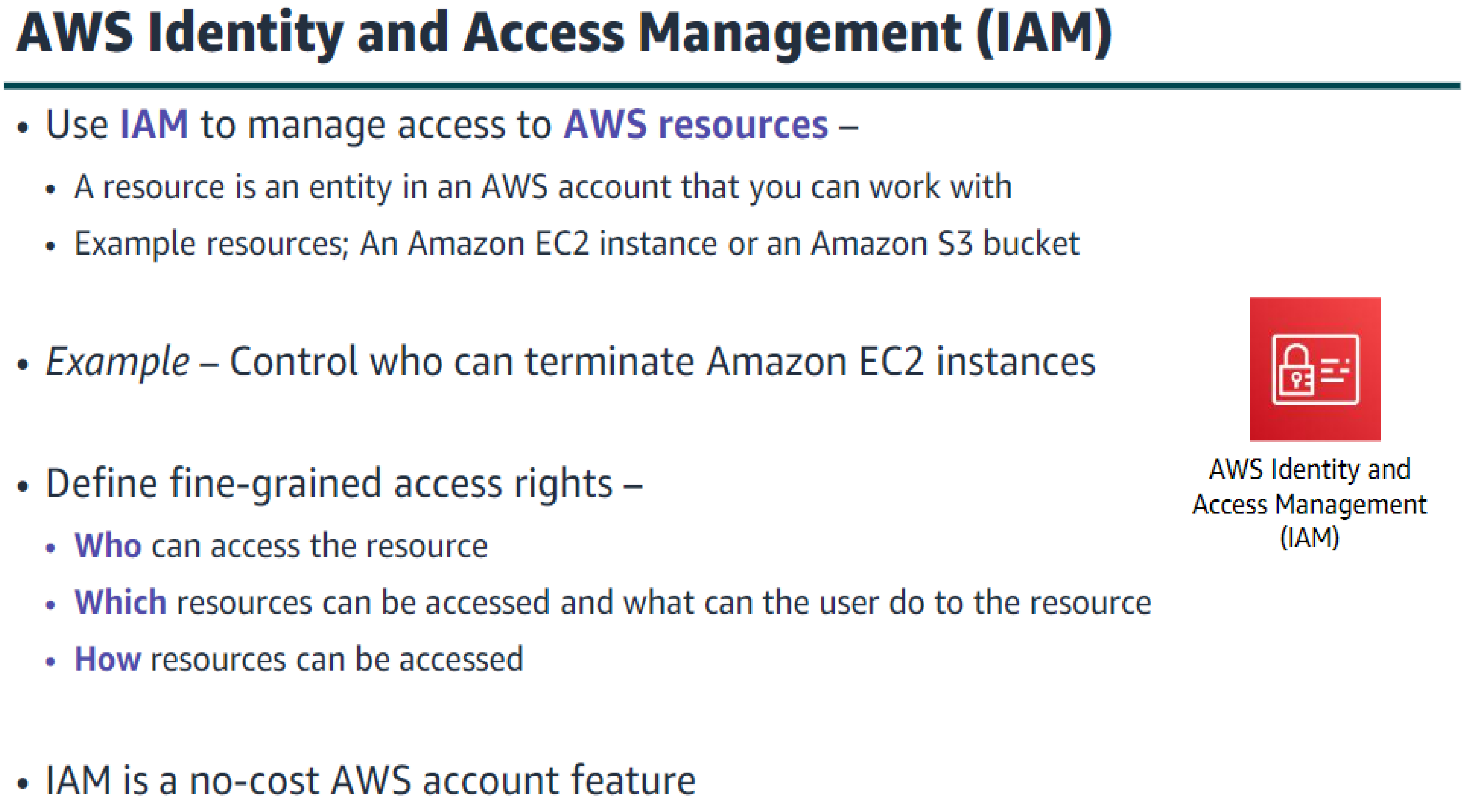
OAuth

- An application request the access to resources controlled by the resource owner
- The resource owner grants permission to access the resource in the form of token and a matching shared-secret
- Token may be issued with specified scope and lifetime

RBAC

- A user who wants to access the cloud resources sends his/her data to the system administrator

- The administrator assigns permissions and access control policies which are stored in user roles and data access policies



AWS Identity and Access Management (IAM)

- Use **IAM** to manage access to **AWS resources** –
  - A resource is an entity in an AWS account that you can work with
  - Example resources; An Amazon EC2 instance or an Amazon S3 bucket

- *Example* – Control who can terminate Amazon EC2 instances

- Define fine-grained access rights –
  - **Who** can access the resource
  - **Which** resources can be accessed and what can the user do to the resource
  - **How** resources can be accessed

- IAM is a no-cost AWS account feature

AWS Identity and Access Management (IAM)

IAM: Essential components

IAM user

A **person** *or* **application** that can authenticate with an AWS account.

IAM group

A **collection of IAM users** that are granted identical authorization.

IAM policy

The document that defines **which resources can be accessed** and the **level of access** to each resource.

IAM role

Useful mechanism to grant a set of permissions for making AWS service requests.

Authenticate as an IAM user to gain access

When you define an **IAM user**, you select what ***types of access*** the user is permitted to use.

Programmatic access

- Authenticate using:
  - Access key ID
  - Secret access key
- Provides AWS CLI and AWS SDK access

AWS CLI

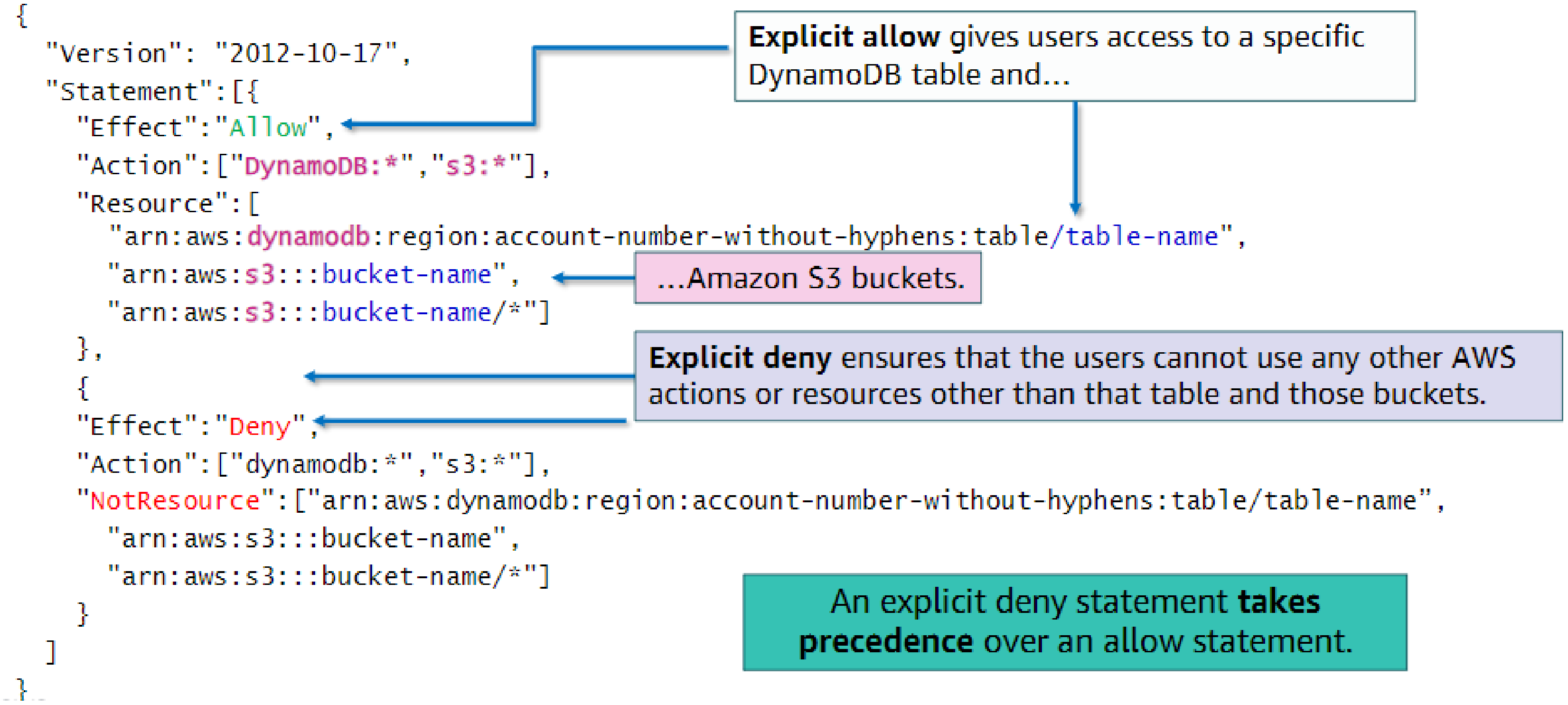
AWS Tools and SDKs

AWS Management Console access

- Authenticate using:
  - 12-digit Account ID *or* alias
  - IAM user name
  - IAM password
- If enabled, **multi-factor authentication (MFA)** prompts for an authentication code.

AWS Management Console

IAM policy example



```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action":["DynamoDB:*","s3:*"],
    "Resource":[
      "arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    },
    {
    "Effect":"Deny",
    "Action":["dynamodb:*","s3:*"],
    "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    }
  ]
}
```

Explicit allow gives users access to a specific DynamoDB table and…

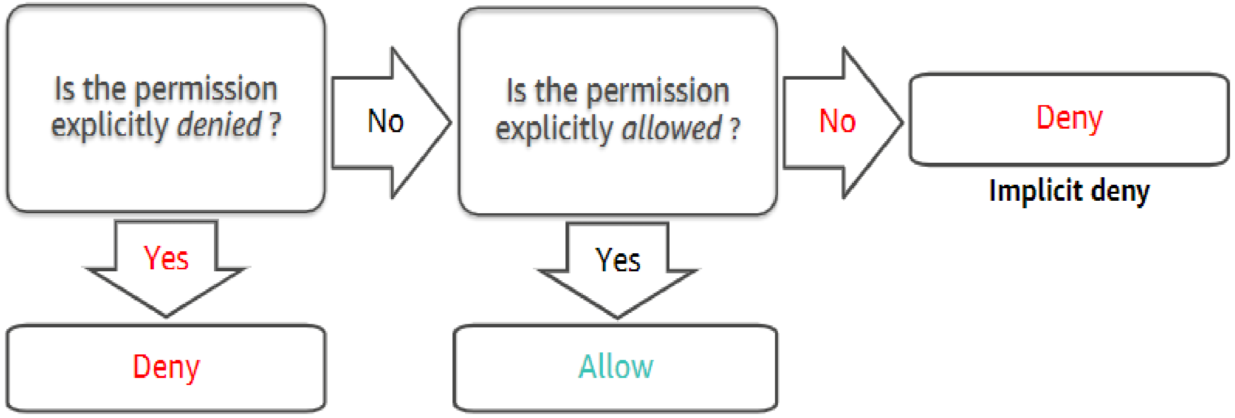
…Amazon S3 buckets.

Explicit deny ensures that the users cannot use any other AWS actions or resources other than that table and those buckets.

An explicit deny statement **takes precedence** over an allow statement.

IAM permissions

How IAM determines permissions:


Is the permission explicitly *denied* ?
No
Is the permission explicitly *allowed* ?
No
Deny
Implicit deny
Yes
Yes
Deny
Allow

PES
UNIVERSITY
CELEBRATING 50 YEARS

THANK YOU

S Thenmozhi
Department of Computer Applications
thenmozhis@pes.edu
+91 80 6666 3333 Extn 393