

N|DE
Network Defense Essentials

Module 02

Identification, Authentication, and Authorization

Module Objectives

- Understanding the Terminology, Principles, and Models of Access Control
- Understanding Identity and Access Management (IAM)
- Understanding User Access Management
- Overview of Different Types of Authentication
- Overview of Different Types of Authorization
- Understanding User Accounting

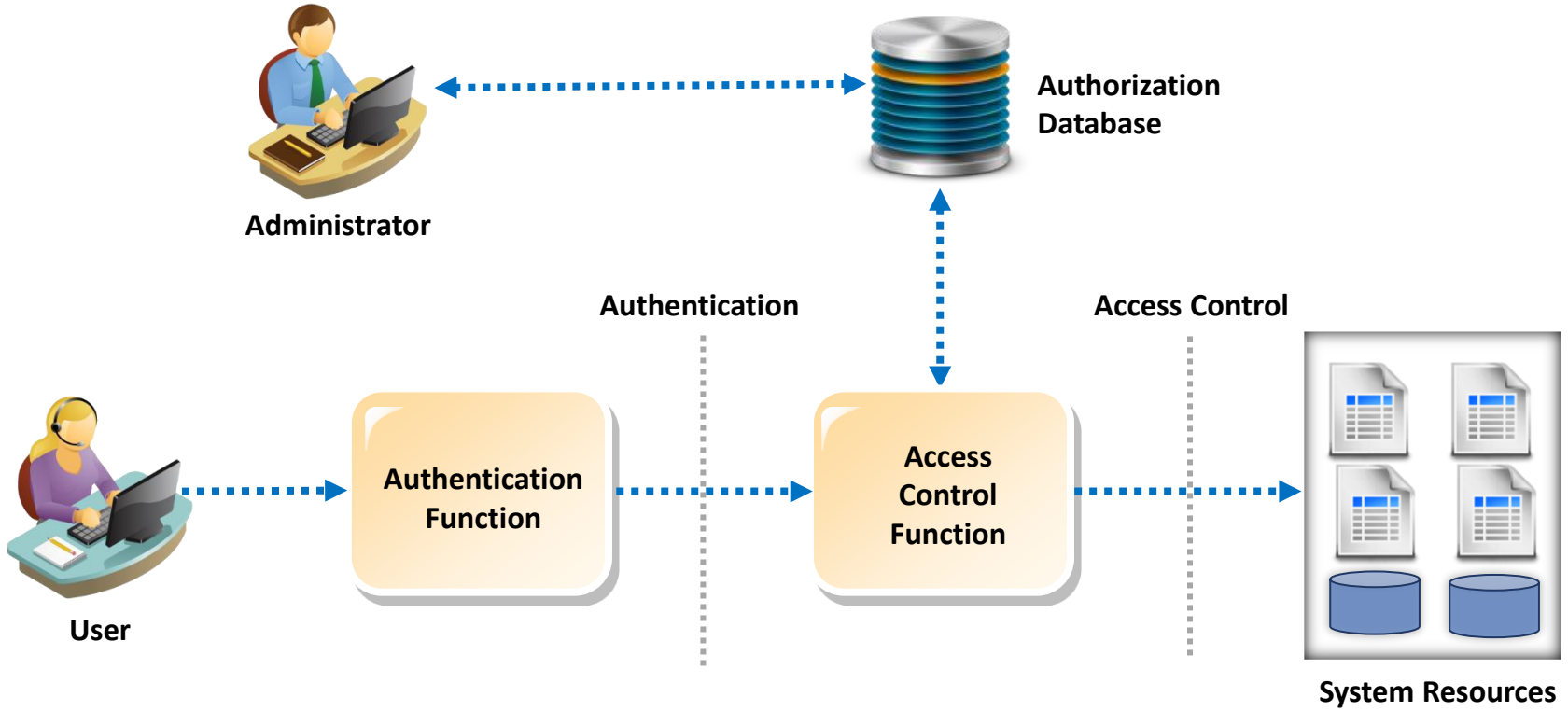


Module Flow

1. **Discuss Access Control Principles, Terminologies, and Models**
2. **Discuss Identity and Access Management (IAM) Concepts**

Access Control

- Access control is the **selective restriction** of access to an asset or a system/network resource
- It **protects the information assets** by determining who can access what
- Access control mechanism uses **user identification**, **authentication**, and **authorization** to restrict or grant access to a specific asset/resource



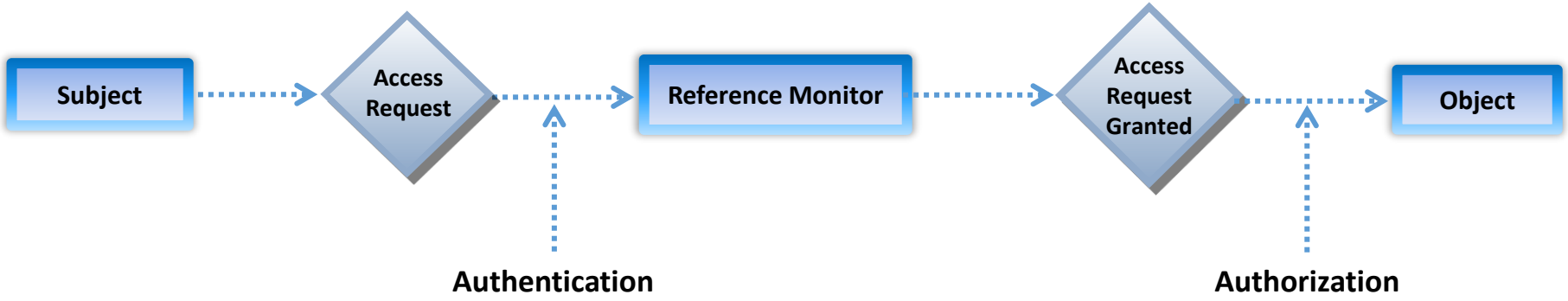
Access Control Terminologies

Subject — This refers to a **particular user** or **process** that wants to access a resource

Object — This refers to a **specific resource** that the user wants to access such as a file or a hardware device

Reference Monitor — It checks the **access control rule** for specific restrictions

Operation — It represents an **action** taken by a subject on an object



Access Control Principles

Separation of Duties (SoD)

- Involves a breakdown of the authorization process into various steps
- Different privileges are assigned at each step to the individual subjects requesting for a resource
- This ensures that no single individual has the authorization rights to perform all functions and simultaneously denies access of all the objects to a single individual

Need-to-know

- Under the need-to-know access control principle, access is provided only to the information that is required for performing a specific task

Principle of Least Privilege (POLP)

- Principle of least privilege extends the need-to-know principle in providing access to a system
- POLP believes in providing employees a need–to-know access, i.e., not more, not less;
- It helps an organization by protecting it from malicious behavior, achieving better system stability, and system security

Access Control Models



- Access control models are the **standards which provide a predefined framework** for implementing the necessary level of access control

Mandatory Access Control (MAC)

- ✓ Only the administrator/system owner has the rights to assign privileges
- ✓ It does not permit the end user to decide who can access the information

Discretionary Access Control (DAC)

- ✓ End user has complete access to the information they own

Role-based Access Control (RBAC)

- ✓ Permission are assigned based on user roles

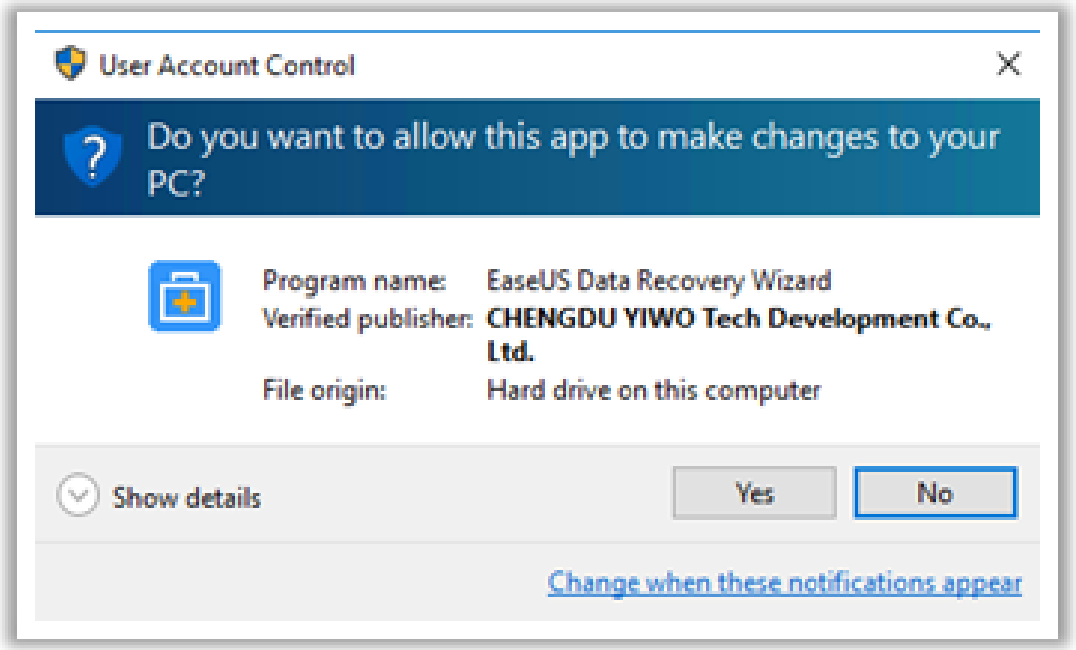
Rule-based Access Control (RB-RBAC)

- ✓ Permissions are assigned to a user role dynamically based on a set of rules defined by the administrator

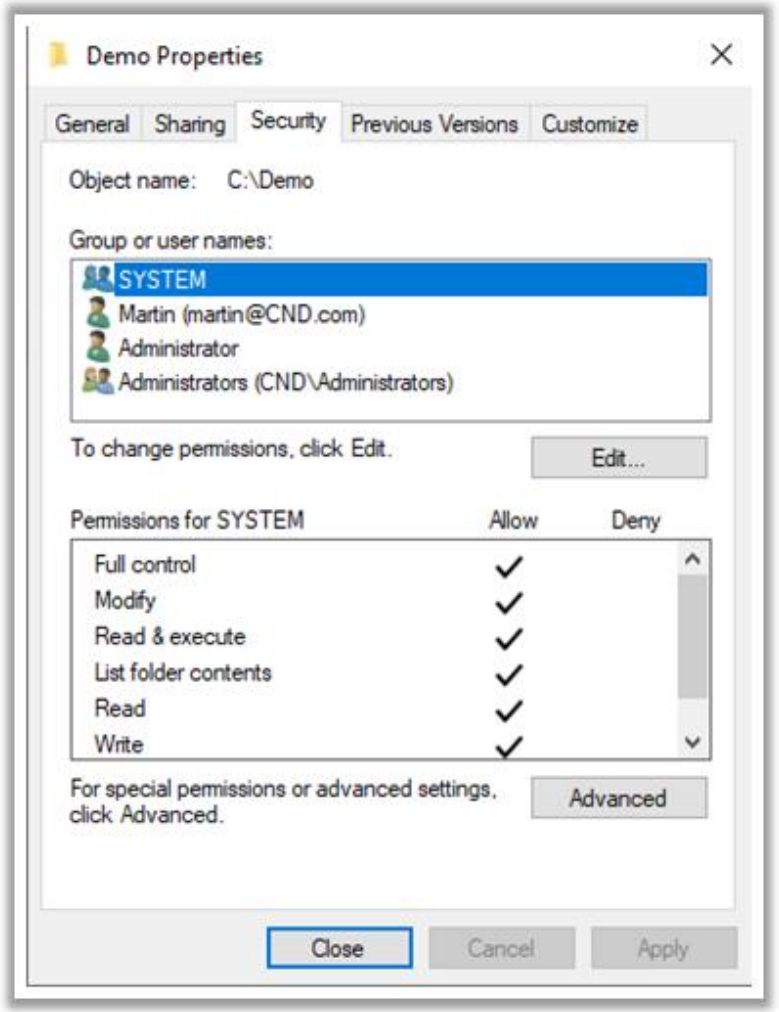
Logical Implementation of DAC, MAC, and RBAC

- Logical implementation of access control is performed using **access control lists (ACLs)**, **group policies**, **passwords**, and **account restrictions**

MAC Implementation: The User Account Control (UAC) tool of Windows OS

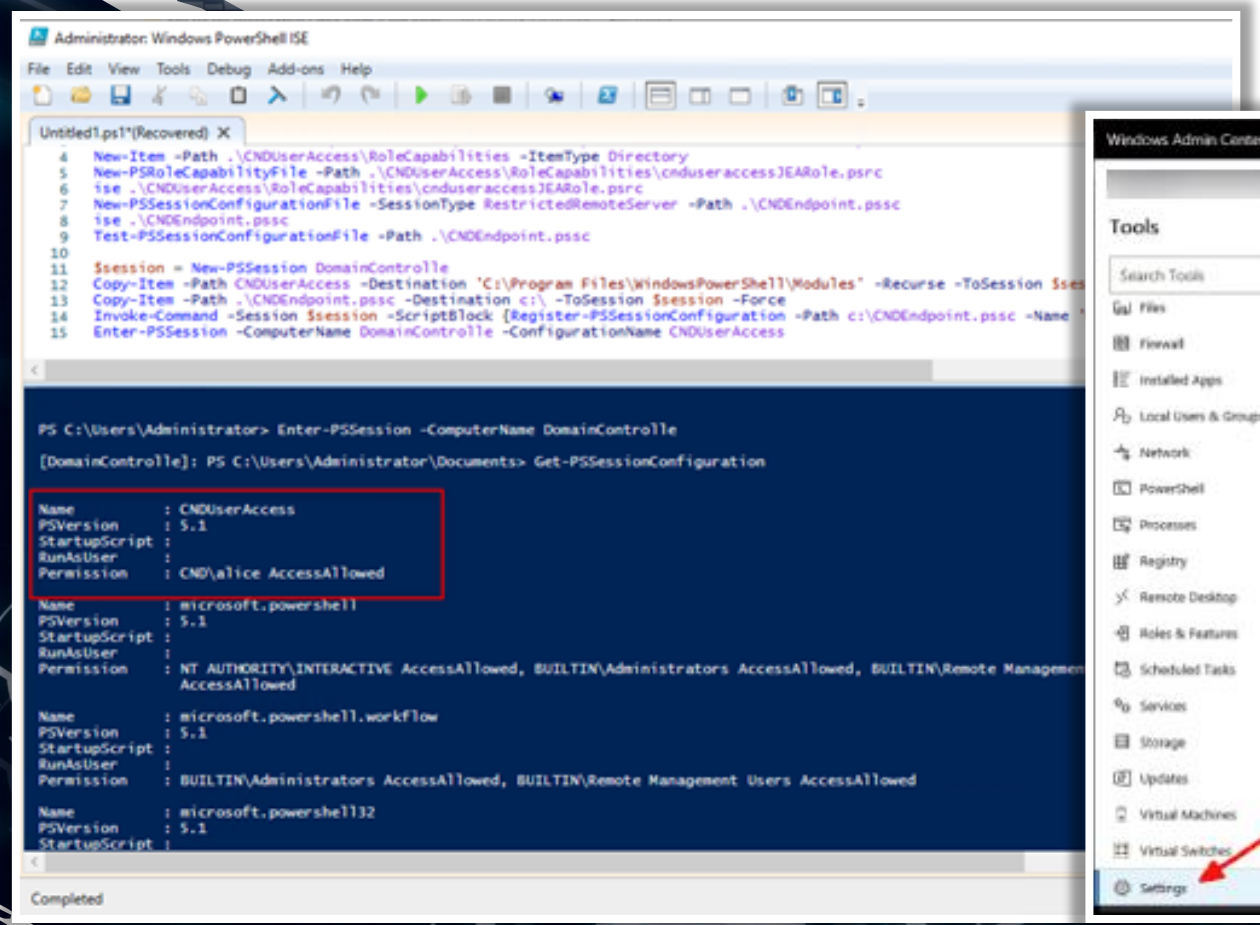


DAC Implementation: Windows File Permissions

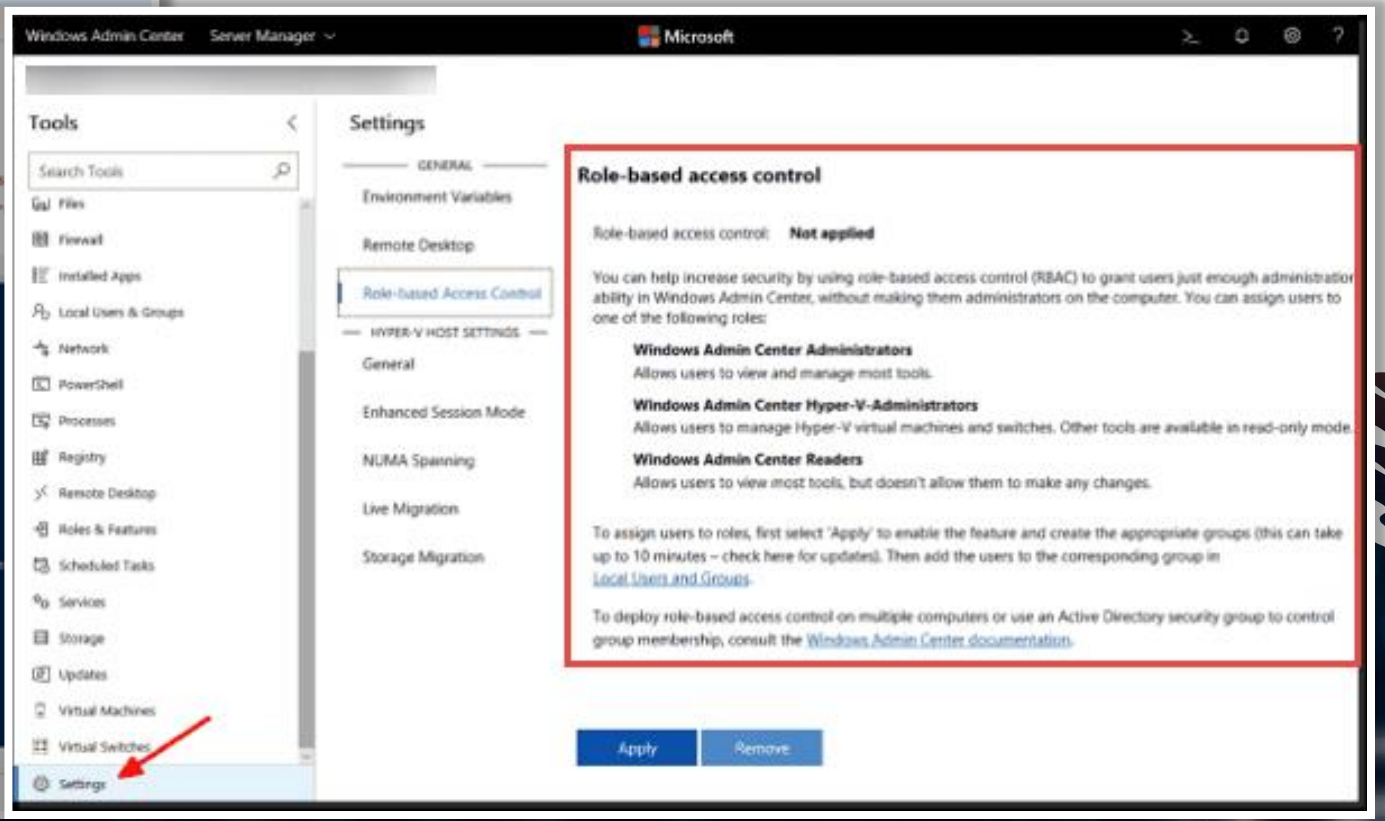


Logical Implementation of DAC, MAC, and RBAC (Cont'd)

RBAC Implementation: Just Enough Administration (JEA)



RBAC Implementation: Windows Admin Center (WAC)

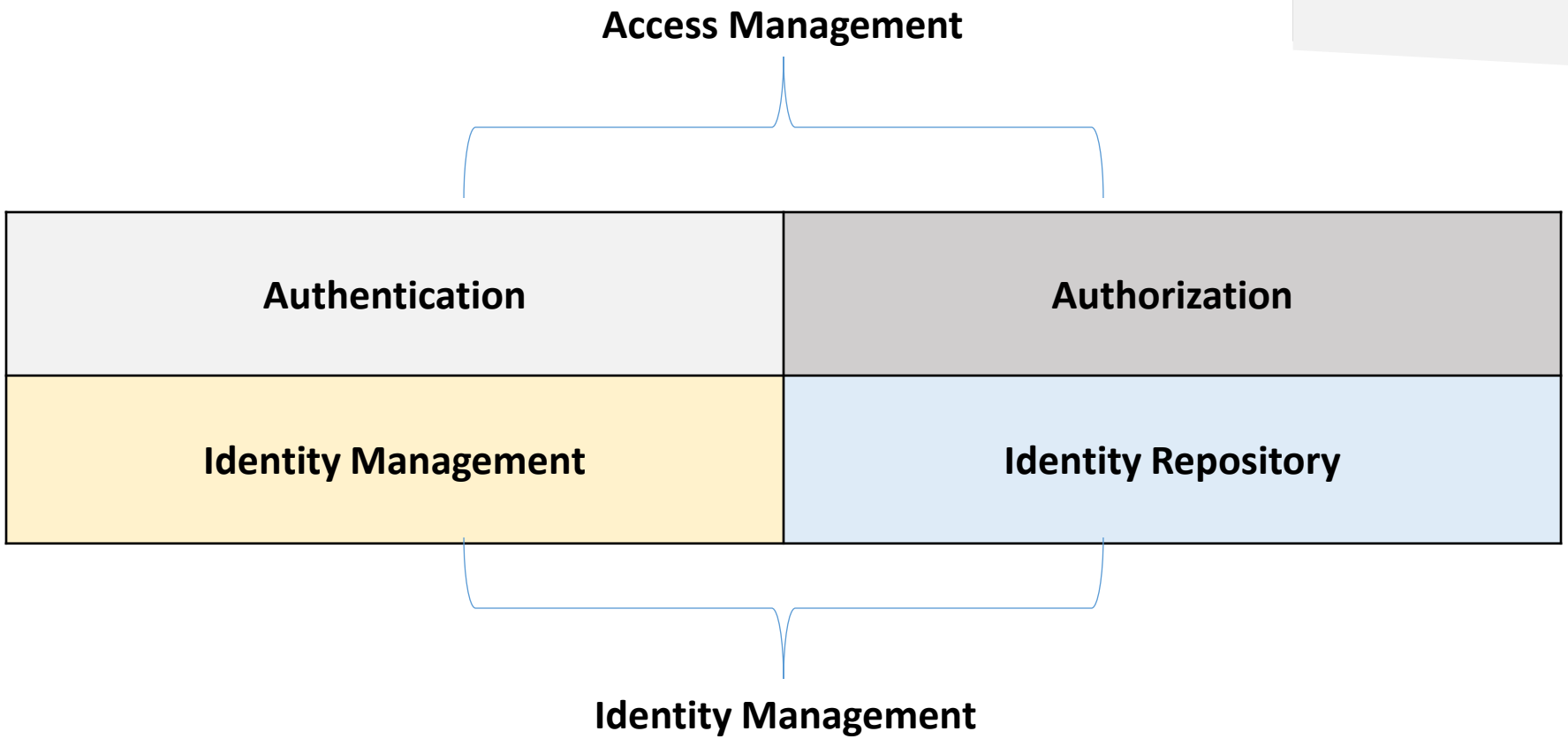


Module Flow

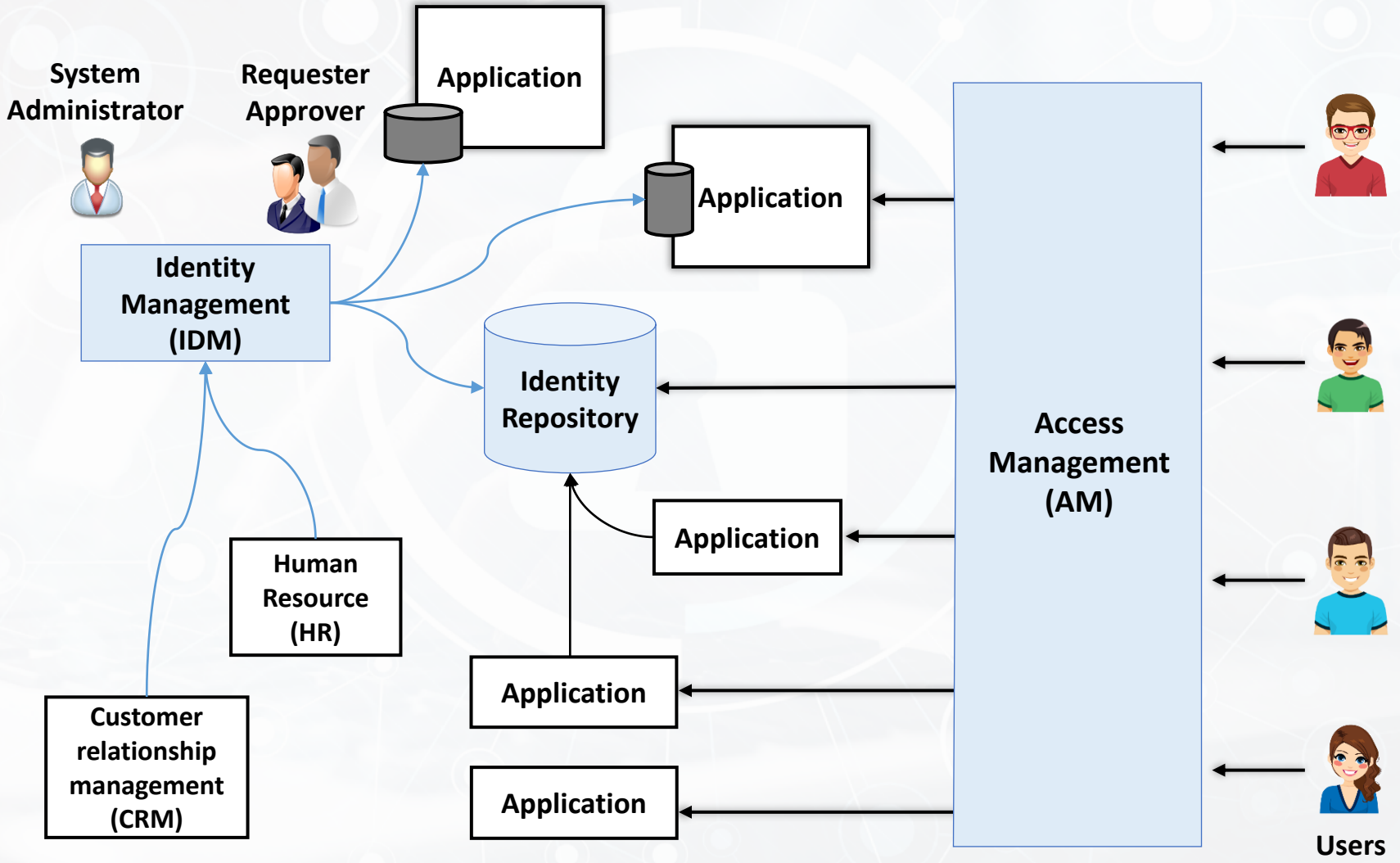
1. Discuss Access Control Principles, Terminologies, and Models
2. Discuss Identity and Access Management (IAM) Concepts

Identity and Access Management (IAM)

- IAM is responsible for providing the **right individual with right access at the right time**



Identity and Access Management (IAM) (Cont'd)



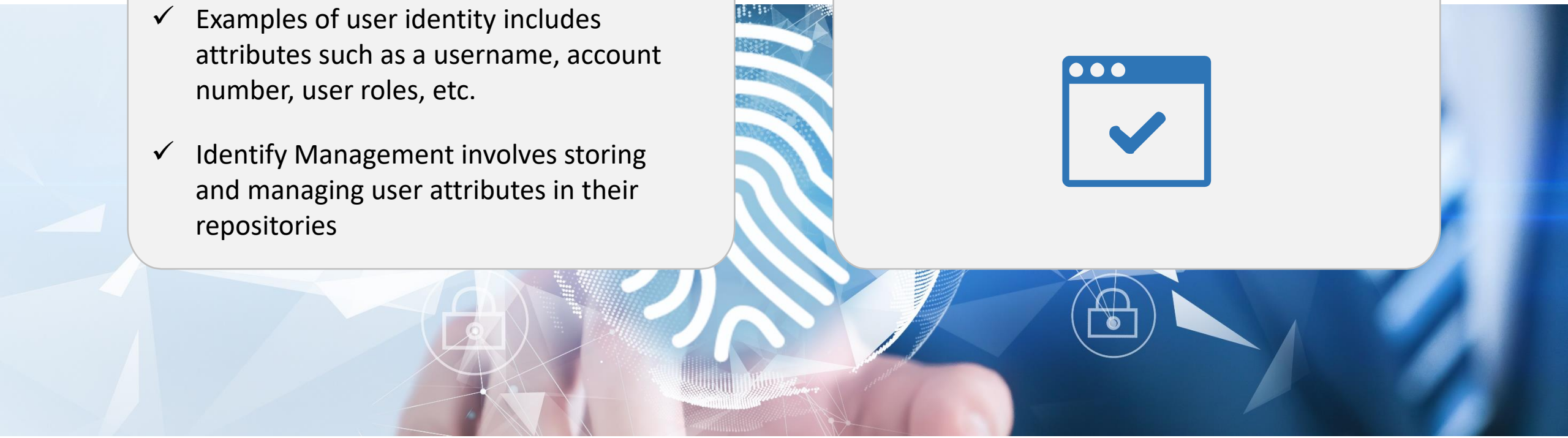
User Identity Management (IDM)

Identity Management

- ✓ User Identification involves a method to ensure that an **individual holds a valid identity**
- ✓ Examples of user identity includes attributes such as a username, account number, user roles, etc.
- ✓ Identify Management involves storing and managing user attributes in their repositories

Identity Repository

- ✓ The user repository is a database where attributes related to the users' identities are stored



User Access Management (AM): Authentication

- Authentication involves validating the **identity of an individual with a system**, **application**, or **network**

Types of Authentication

- **Password Authentication**
- **Smart Card Authentication**
- **Biometric Authentication**
- **Two-factor Authentication**
- **Single Sign-on (SSO) Authentication**

Types of Authentication

Password Authentication

- Password Authentication uses a **combination** of a username and a password to authenticate the network users
- The password is checked against a **database** and the user is given access if it matches
- Password authentication can be vulnerable to **password cracking attacks** such as brute force or dictionary attacks





Types of Authentication (Cont'd)

Smart Card Authentication

- Smart card is a small **computer chip device** that holds a users' personal information required to authenticate them
- Users have to insert their smart cards into the card reader machines and enter their **personal identification number** (PIN) to authenticate themselves
- Smart card authentication is a **cryptography-based authentication** and provides stronger security than password authentication

Types of Authentication (Cont'd)

Biometric Authentication

Biometrics refers to the **identification of individuals** based on their physical characteristics

Biometric Identification Techniques

Fingerprint Scanning

Compares two fingerprints for verification and identification on the basis of the patterns on the finger

Retinal Scanning

Analyzes the layer of blood vessels at the back of their eyes to identify a person

Iris Scanning

Analyzes the colored part of the eye suspended behind the cornea

Vein Structure Recognition

Analyzes thickness and location of veins to identify a person

Face Recognition

Uses facial features to identify or verify a person

Voice Recognition

Uses voice patterns to identify or verify a person

Types of Authentication (Cont'd)

Two-factor Authentication

1. Two-factor authentication involves using two different authentication factors out of three (something you know, something your have, and something you are) to verify the **identity of an individual** in order to enhance the **security in authentication systems**

2. **Combinations of two-factor authentication:** password and smart card/token, password and biometrics, password and one-time password (OTP), smart card/token and biometrics, etc.

3. "Something you are" is the best companion of two-factor authentication as it is considered as the **hardest to forge** or **spoof**



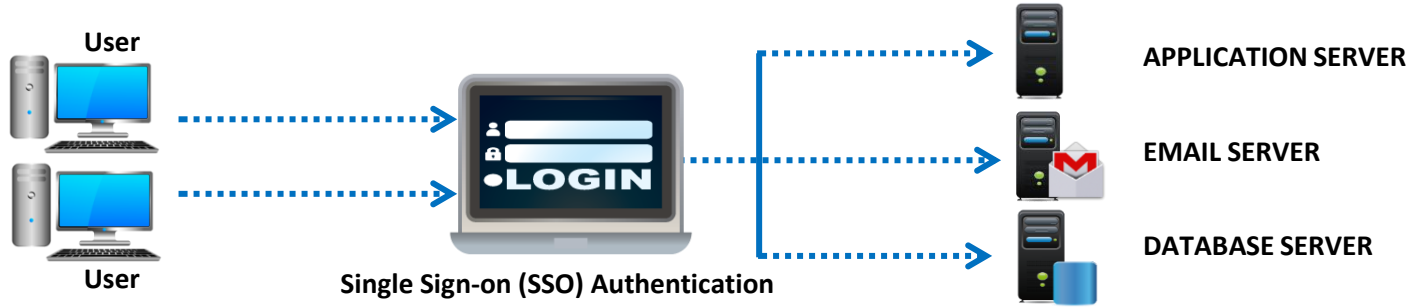
Types of Authentication (Cont'd)

Single Sign-on (SSO) Authentication

- It allows a user to authenticate themselves to **multiple servers** on a network with a **single password** without re-entering it every time

Advantages

01. No need to remember passwords of multiple applications or systems
02. Reduces the time for entering a username and password
03. Reduces the network traffic to the **centralized server**
04. Users need to enter credentials only once for multiple applications





User Access Management (AM): Authorization

- Authorization involves **controlling the access** of information for an individual (E.g.: A user can only read a file, but not write in it or delete it)

Types of Authorization Systems

Centralized Authorization

- ✓ Authorization for network access is done using a **single centralized** authorization unit
- ✓ It maintains a **single database** for authorizing all the network resources or applications
- ✓ It is an **easy and inexpensive** authorization approach

Decentralized Authorization

- ✓ Each network resource maintains its **authorization unit** and performs authorization locally
- ✓ It maintains its **own database** for authorization



Implicit Authorization

- ✓ Users can access the requested resource **on behalf** of others
- ✓ The access request goes through a **primary resource** to access the requested resource

Explicit Authorization

- ✓ Unlike implicit authorization, explicit authorization requires **separate authorization** for each requested resource
- ✓ It explicitly maintains authorization for each **requested object**

User Access Management (AM): Accounting

- Accounting is a method of keeping **track** of **user actions** on the network. It keeps track of who, when, and how the users access the network.
- It helps in identifying authorized and unauthorized actions
- The account data can be used for trend analysis, data breach detection, forensics investigations, etc.



Module Summary

- This module has discussed the access control principles, terminologies, and models
- It has discussed identity and access management concepts
- It also discussed different methods used for user access management
- It has discussed different types of authentication and authorization techniques
- Finally, this module ended with an overview of user accounting and accountability
- In the next module, we will discuss in detail on network security controls - administrative controls

