🔑 Authentication & Access Control

1. Authentication

🔷 Definition:
The process of verifying the identity of a user, system, or device before granting access.
👉 It answers: “Who are you?”

🔷 Types of Authentication

1. Single-Factor Authentication (SFA)
   - Just a password or PIN.
2. Two-Factor Authentication (2FA)
   - Password + OTP (something you know + something you have).
3. Multi-Factor Authentication (MFA)
   - Combines 2+ factors (password, OTP, biometric).
4. Biometric Authentication
   - Fingerprint, Face ID, Iris scan.
5. Token / Smart Card Based
   - Hardware or software tokens.

---

2. Access Control

🔷 Definition:
The method of deciding who can access what resources after authentication.
👉 It answers: “What can you do?”

🔷 Types of Access Control

1. Discretionary Access Control (DAC)
   - Owner decides who gets access.
   - Example: File sharing in Windows (user sets permissions).
2. Mandatory Access Control (MAC)

   - Access is based on fixed policies set by the system.
   - Example: Military classifications (Top Secret, Secret, Confidential).

3. Role-Based Access Control (RBAC)
   - Access depends on user’s role.
   - Example: Admin vs Teacher vs Student.
4. Attribute-Based Access Control (ABAC)
   - Access based on attributes (time, location, device, role).
   - Example: Employee can access HR data only during office hours.

---

3. Key Differences

- Authentication ➔ Confirms identity. (Login step)
- Access Control ➔ Grants/denies permissions. (After login)

---

4. Real-Life Examples

- ATM:
  - Authentication ➔ Entering PIN.
  - Access Control ➔ Only your bank account allowed.
- Office Login System:
  - Authentication ➔ Fingerprint scanner.
  - Access Control ➔ Developers can access code repo, HR cannot.