Authentication Mechanisms

What is Authentication?

Authentication is the process of **verifying the identity of a user, device, or system** to check whether they are really who they claim to be.

In simple words → It makes sure that the person trying to access a system is genuine, not an attacker.

Examples:

- When you enter your **password** in Gmail, the system checks if it matches the one stored → if yes, you are authenticated.
- Unlocking your phone with a **fingerprint** → confirms your identity.
- Showing an **ID card** at an exam hall → proves you are the right student.

Purpose of Authentication:

- To ensure that only **authorized users** can access information.
- To prevent **unauthorized access** and protect sensitive data.

Authentication Mechanisms in Detail

1. Password-Based Authentication

How it works:

- The user enters a **username** and a **password**.
- The system checks if the password matches the one stored in its database (usually stored in **encrypted/hashed** form).
- If it matches → access is granted.

Example: Logging into Facebook, Gmail, or a Windows computer.

Advantages:

- Simple and widely used.
- Does not need extra hardware.

Disadvantages:

- Passwords can be guessed or stolen (phishing).
- People often use weak or repeated passwords.

---

2. Biometric Authentication

How it works:

- Uses **unique physical or behavioral characteristics** of a person.
- Types include:
    - **Fingerprint recognition**
    - **Face recognition**
    - **Iris or retina scanning**
    - **Voice recognition**

- System compares the captured biometric sample with the stored one.

Example: Unlocking phones with fingerprint/Face ID, using iris scan at airports.

Advantages:

- Hard to copy or steal.
- No need to remember passwords.

Disadvantages:

- Needs special devices (scanners, cameras).
- Sometimes false negatives (system doesn't recognize you if finger is wet, face in low light).
- Privacy concerns if biometric data is stolen.

---

3. Token-Based Authentication

How it works:

- A **token** (physical device or app) generates a temporary code.
- You enter this code along with your password.
- Tokens can be:
    - **Hardware token**: small device generating numbers.
    - **SMS/Email OTP**: one-time password sent to your phone/email.

Example: Online banking login with password + OTP, Paytm or UPI OTPs.

Advantages:

- More secure than just password.
- OTP changes each time, so harder to steal.

Disadvantages:

- Token/phone can be lost.
- If network is down (no SMS), you may not receive OTP.

---

4. Certificate-Based Authentication

How it works:

- Uses **digital certificates** issued by a trusted authority (like an electronic ID card).
- The certificate contains your identity info + a cryptographic key.
- When you log in, system checks your certificate for validity.

Example:

- SSL/TLS certificates in websites (the 🔒 lock in the browser).
- Employees using digital certificates to access company VPN.

Advantages:

- Very strong security.
- Hard to fake certificates.

Disadvantages:

- Needs a **Public Key Infrastructure (PKI)** to manage certificates.
- Complex and expensive to implement.

---

5. Multi-Factor Authentication (MFA)

How it works:

- Combines **two or more** methods of authentication:
    1. Something you **know** (password, PIN)
    2. Something you **have** (OTP, token, smart card)
    3. Something you **are** (fingerprint, face)
- User must pass at least two checks.

Example: Gmail → password + OTP from phone.
Bank ATM → card (have) + PIN (know).

Advantages:

- Much harder for hackers to break.
- Even if password is stolen, account is safe.

Disadvantages:

- Slower and less convenient.
- Requires extra devices or steps.

---

6. Single Sign-On (SSO)

How it works:

- User logs in once → system creates a **session/token**.
- This token allows access to multiple applications without re-entering credentials.

Example:

- Google account → once logged in, you can access Gmail, Drive, YouTube, etc.
- Office 365 → one login for Word, Excel, Outlook.

Advantages:

- Convenient, no need to remember many passwords.
- Saves time.

Disadvantages:

- If main account is hacked → all services are exposed.
- Complex setup in organizations.

---

7. Smart Card Authentication

How it works:

- Smart cards have a **chip** that stores credentials.
- User inserts card into reader and enters PIN/password.

- System checks the information from the card.

Example:

- ATM cards with chip.
- Office ID cards to access restricted areas.

Advantages:

- Secure and portable.
- Hard to duplicate.

Disadvantages:

- Requires card readers.
- Card can be lost or damaged.

---

8. Knowledge-Based Authentication (KBA)

How it works:

- User answers **personal questions** as proof of identity.
- Two types:
    - **Static KBA**: Fixed questions like “mother’s name”.
    - **Dynamic KBA**: Questions generated from user’s history (e.g., “Which bank did you take a loan from in 2018?”).

Example:

- Resetting password in older email services.

- Some banks use KBA as extra verification.

Advantages:

- Easy to use, no extra device needed.
- Can be used as backup if you forget password.

Disadvantages:

- Easy to guess or find answers on social media.
- Not very secure in modern times.
