CIA TRIAD

1. Confidentiality

- **Definition:** Ensuring that information is accessible only to those who have proper authorization.
- **Goal:** Prevent unauthorized access or disclosure of sensitive data.
- **Methods/Examples:**
  - Encryption
  - Access control lists (ACLs)
  - Multi-factor authentication (MFA)
  - Data classification policies

2. Integrity

- **Definition:** Maintaining the accuracy, completeness, and trustworthiness of data over its entire lifecycle.
- **Goal:** Ensure data is not altered or destroyed in an unauthorized way, whether intentionally or accidentally.
- **Methods/Examples:**
  - Checksums and hashing (e.g., SHA-256)
  - Digital signatures
  - Version control
  - Audit logs

3. Availability

- **Definition:** Ensuring that authorized users have timely and reliable access to data, systems, and resources when needed.
- **Goal:** Minimize downtime and ensure continuous operations.
- **Methods/Examples:**
  - Redundant systems and failover mechanisms
  - Regular system maintenance
  - DDoS protection
  - Backup and disaster recovery plans

Use of CIA Triad in Real World Systems

1. Gmail (Email service)

- **Confidentiality:** Uses TLS encryption to protect emails in transit and MFA to prevent unauthorized access.
- **Integrity:** Detects altered or spoofed emails via DKIM and SPF checks.
- **Availability:** Google's distributed servers and uptime monitoring ensure minimal downtime.

2. Banking App

- **Confidentiality:** Encrypts transactions and account details using AES-256 encryption.
- **Integrity:** Verifies transaction data with digital signatures and secure APIs.
- **Availability:** Uses load balancing, failover systems, and scheduled maintenance to stay online.

3. Hospital Electronic Health Record

- **Confidentiality -** Restricts patient record access to authorized medical staff under HIPAA rules.
- **Integrity -** Ensures medical records aren't altered improperly via audit logs and access tracking.
- **Availability:** Has backup servers and disaster recovery plans so doctors can access records even during outages.

How file permissions on a Linux machine support the CIA Triad when configured correctly:

1. **Confidentiality** – Restricting who can read files

   - **How Linux does it:** Each file and directory has **read (r)**, **write (w)**, and **execute (x)** permissions for three categories:
     - **Owner** (user)
     - **Group**
     - **Others** (everyone else)

   - **Example:**
     - `/etc/shadow` stores password hashes.
     - Permissions: `-rw------- 1 root root` → Only the root user can read or write.
     - This prevents unauthorized users from viewing sensitive data.

2. Integrity – Preventing unauthorized modifications

- **How Linux does it:**
  - Write (`w`) permissions are granted only to trusted users or processes.
  - Use **immutable attribute** (`chattr +i file`) to lock critical files from changes.

- **Example:**
  - System configuration files like `/etc/passwd` or `/etc/fstab` have restricted write access to prevent tampering.
  - If an unauthorized user tries to modify them, permission is denied.

3. Availability – Ensuring needed files remain accessible

- **How Linux does it:**
  - Execute (`x`) permission allows running programs.
  - Proper group assignments ensure teams can access shared files without bottlenecks.
  - Backups and correct ownership prevent accidental deletion or lockouts.

- **Example:**
  - A script in `/usr/local/bin` might have `-rwxr-xr-x` so all users can run it but only admins can modify it, keeping it available and functional.