TASK 1: Exploring the CIA Triad in Real-World Scenarios

# CIA TRIAD

# What is CIA Triad?

The CIA Triad stands for:

1. Confidentiality
2. Integrity
3. Availability

It is a core concept in cybersecurity that guides how organizations protect information and systems.  
The goal is to ensure data is kept secret, accurate, and accessible.

Three main goals of CIA Triad :

CONFIDENTIALITY – KEEPS DATA SECRET

INTEGRITY – KEEPS DATA ACCURATE

AVAILABILITY – KEEPS DATA ACCESSIBLE

1.Confidentiality **– "Only the right people should see it."**  
Confidentiality means protecting sensitive information from being accessed by unauthorized people.

If attackers get access to confidential data, they can misuse it for fraud, identity theft.

**How confidentiality is achieved:**

* **Access control** – Only give permissions to authorized people.
* **Encryption** – Make data unreadable without the key.
* **Authentication** – Verify identity using passwords, biometrics, MFA etc.
* **Data classification** – Mark data as Public, Internal, Confidential, or Restricted.

2. Integrity **– "The data must remain correct."**  
Integrity ensures information is accurate, complete, and unaltered.

**How integrity is achieved:**

* **Hashing –** Generate a digital fingerprint of data to detect changes.
* **Digital signatures –** Verify the sender and ensure the content hasn’t been changed.
* **Version control systems –** Keep track of changes.
* **Checksums –** Validate data in files or transmissions.

3. Availability **– "The data and systems should be there when needed."**  
Availability means ensuring that authorized users can access the systems and data when they need it.

Even if data is confidential and accurate, it’s useless if you can’t access it on time.

**How it’s achieved:**

* **Disaster recovery plans** – Quickly restore services after outages.
* **Regular maintenance** – Apply updates and patch vulnerabilities.
* **DDoS protection** – Prevent attackers from overwhelming the system.

## Real-World Applications of the CIA Triad

## Gmail

**Confidentiality** – Gmail keeps your emails private using:

* Encryption so only you and the recipient can read them.
* Passwords and 2-step verification to stop unauthorized logins.

**Integrity** – Gmail makes sure emails are not changed by:

* Checking that the message is the same as when it was sent.
* Blocking spam and fake emails.

**Availability** – Gmail is almost always online by:

* Using many servers worldwide.
* Backups to keep your emails safe even if one server fails.

## WhatsApp

**Confidentiality** – Keeps chats private with:

* End-to-end encryption only you and the person you chat with can read messages.
* Lock or fingerprint to open the app.

**Integrity** – Makes sure messages are not changed by:

* Verifying they are sent exactly as typed.
* Blocking altered or fake messages.

**Availability** – Always ready to use by:

* Having many servers around the world.
* Working even on slow internet and reconnecting if the signal drops.

## Banking App

**Confidentiality** – Keeps your account private with:

* Passwords, OTP, and fingerprint login.
* Encryption so hackers can’t read your banking data.

**Integrity** – Makes sure your money and details are correct by:

* Confirming transactions with OTP or PIN.
* Recording and checking every change in your account.

**Availability** – Lets you use banking anytime by:

* Running 24/7 with backup servers.
* Protecting against crashes and cyberattacks.

## Linux file permissions support CIA

In Linux, every file and folder has permissions for:

Read (r) – view the file content.

Write (w) – modify the file.

Execute (x) – run the file as a program or script.

Permissions are assigned to:

**Owner** (user who owns the file) , **Group** (users in the same group) , **Others** (everyone else)

**Confidentiality :** Restrict read permissions so that only authorized users can view sensitive files.

Example: Password file /etc/shadow → Only root can read it.

**Integrity :** Restrict write permissions so unauthorized users cannot change or corrupt files.

Example: System file /etc/hosts → Only root can edit it, so no one can tamper with it.

**Availability :** Correct execute permissions ensure programs and scripts run when needed.

Proper permissions prevent accidental deletion or disabling of important system files, keeping services available.

Example: /bin/ls → Has execute permission for everyone so the ls command works for all users.

## Here’s a clear list of Linux commands you can use in a practical way to show how file permissions support the CIA Triad.

1.ls -l : Lists files with their permissions, owner, and group.

2.chmod [permissions] filename : Change Permissions

examples:

chmod 600 secret.txt # Owner can read/write, no access for others (Confidentiality)

chmod 644 file.txt # Owner read/write, others read only (Integrity)

chmod 755 script.sh # Owner read/write/execute, others read/execute (Availability)

3.chown user:group filename : change file owner

4.chgrp groupname filename : change file group name

5. stat filename : Shows file size , owner & group , permissions , last access/change time

## Conclusion

The CIA Triad is the foundation of all cybersecurity practices, and understanding how it applies in real-world systems is essential for protecting data and maintaining trust. Confidentiality ensures that sensitive information is only accessible to authorized individuals, Integrity maintains the accuracy and trustworthiness of data, and Availability guarantees that information and systems are accessible when needed. In this task, we explored practical examples like Gmail, banking applications, and whatsapp systems to see how each principle is applied using technologies such as encryption, access control, backup systems, and redundancy. We also learned how Linux file permissions directly support the CIA Triad by controlling who can read, write, or execute files, thereby protecting data privacy, preventing unauthorized changes, and ensuring essential services run without interruption. These concepts are not just theoretical but are actively implemented in every secure system we use today.