CIA Triad in Real-World Systems

- SWASTHIK C SHETTY
11 August 2025

Introduction

CIA Triad is a fundamental model used to guide security policies and practices. It consists of Confidentiality, Integrity, and Availability three core principles that ensure the security and trustworthiness of information systems. Each element plays a vital role. This report explores the CIA Triad through practical, real-world example.

CIA Triad

1. Confidentiality: Ensuring that data is only accessed by people or systems who are authorized. This is achieved through encryption, authentication, and access controls.
2. Integrity: Maintaining data accuracy, consistency, and trustworthiness by not allowing to change or alter the data.
3. Availability: Making sure systems, applications, and data are accessible to authorized users when they need them, even during failures or attacks

Real-World Examples

Netflix

- Confidentiality: Users accounts are protected by passwords and optional 2Factor Authentication and encrypted streaming links.
- Integrity: Digital rights management to prevent content tampering and data validation for recommendations so that the user can have best experience.
- Availability: Content delivery networks ensure smooth playback to worldwide users.

ATM Network

- Confidentiality: PIN numbers encrypted during transmission and secure chip-based cards.
- Integrity: Transaction validation with bank servers and prevention of double withdrawals.
- Availability: Backup power for ATMs and redundant network links to banking systems.

Gmail (Email Service)

- Confidentiality: Uses TLS encryption for emails in transit, two-factor authentication (2FA) to block unauthorized access.
- Integrity: Employs spam/phishing filters and DKIM signatures to verify email authenticity and prevent tampering.
- Availability: Maintains redundant global data centers with 99.9% uptime guarantees.

Banking App (Mobile Banking)

- Confidentiality: Protects transactions with end-to-end encryption and biometric authentication.
- Integrity: Uses OTP verification for transactions and stores account details using secure hashing algorithms.
- Availability: Cloud-based infrastructure with automatic failover to prevent downtime, supported by 24/7 technical monitoring.

Linux Permissions and CIA

On a Linux operating system:

- Confidentiality: File permissions (chmod) ensure only the right users can read/write certain files.
- Integrity: chattr +i can make a file immutable, preventing unauthorized changes.
- Availability: Scheduled backups ensure data remains accessible even if the original file is lost.

Conclusion

The CIA Triad forms the backbone of cybersecurity. In the real world, companies like ATMs, banks, and Netflix implement all aspects to protect sensitive data and maintain trust. If confidentiality fails, data leaks can occur and if integrity fails, decisions may be made based on incorrect data; and if availability fails, critical services may become inaccessible. Balancing these three components is essential for any secure and reliable system.