# CIA Triad

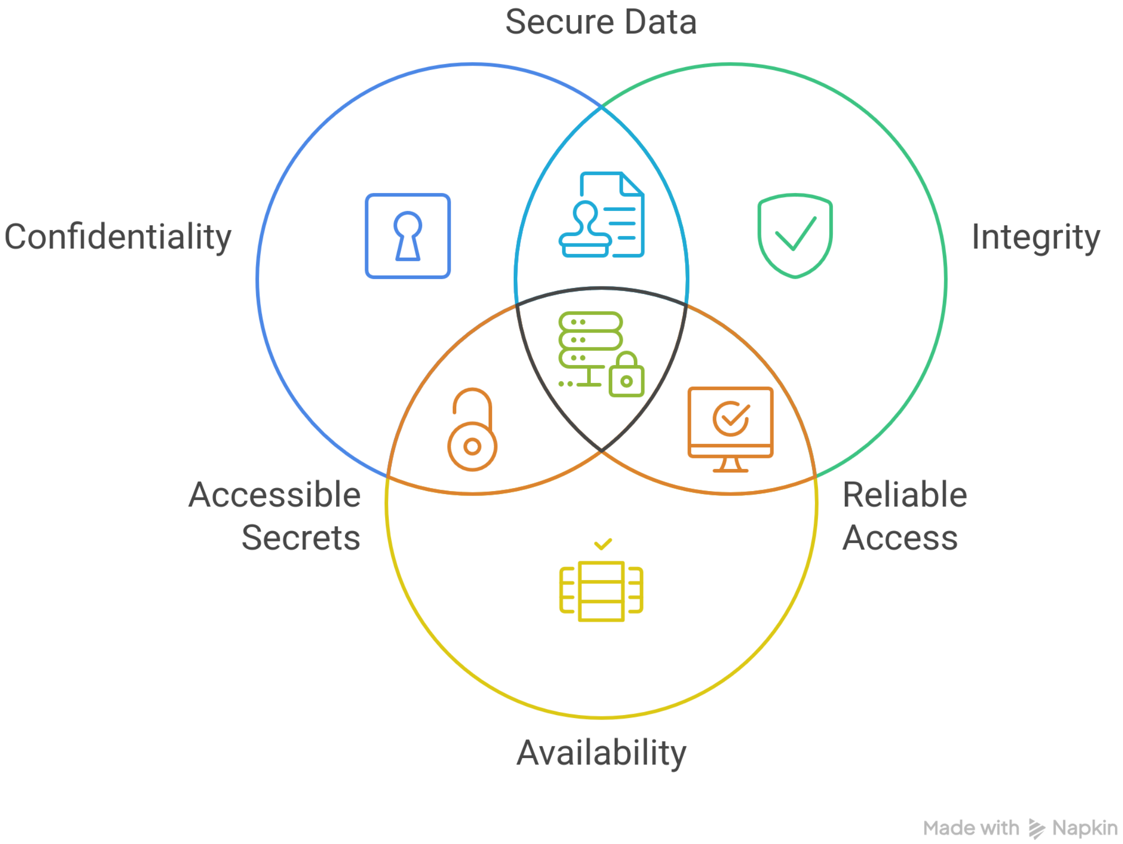
Cybersecurity Internship – Phase 1, Task 1

**Name:**Parmar Rakesh<br>
**Date**:11,AUG,2025<br>
**Internship Program:** Cybersecurity Internship – UJAR TECH

## What is the CIA Triad?

In cybersecurity, it’s not just about keeping your computer safe—it’s also about protecting the data inside it. This is where the **CIA triad** comes in, a simple model to help secure your data. **C** stands for **Confidentiality**, meaning only the **right people can see your data**. **I** stands for **Integrity**, ensuring your data stays **accurate and isn’t tampered** with. **A** stands for **Availability**, making sure your **data is always there when you need** it. If you focus on these three things, your data stays safe and secure.

## What are the Components of the CIA Triad?



1.1Atlas System[1]

# 1.Confidentiality

**Confidentiality** in the CIA triad means keeping your data private so only the intended people can access it. For example, when two people share information digitally, like chatting on WhatsApp, **end-to-end encryption** ensures that no third party can sneak in and steal or read the data. When you see "this chat is end-to-end encrypted" on WhatsApp, it means only you and the person you're chatting with can see the messages—not even a third party or WhatsApp's parent company, Meta, can read them. This is what confidentiality is all about. If confidentiality is weak, your data and information become insecure, leaving them vulnerable to **unauthorized access**.

### Case Study:Adhar data breach(2018)

In early 2018, the Aadhaar database, managed by UIDAI and containing sensitive data like names, bank details, and fingerprints of over **1.1 billion Indians**, faced a massive data leak. Reports revealed that access to the database was being sold on WhatsApp, over 100,000 **former government** employees still had **unauthorized access**[2], Indane's unsecured system exposed Aadhaar details, and over 200 government websites publicly leaked data of 130 million people. Despite UIDAI's denial and legal action against The Tribune for reporting it, many systems were shut down post-exposure, with the World Economic Forum calling it the **world's largest data breach.** This incident underscores the critical role of **Confidentiality** in the CIA triad, as **unauthorized access by former employees** highlights how weak confidentiality measures can lead to significant data breaches.

# 2.Integrity

**Integrity** in the CIA triad means ensuring that the information sent by the sender remains **unchanged** and reaches the receiver **exactly as it was** sent. A great example of integrity is your bank account. Suppose you have ₹6,378 in your XYZ bank account. If the bank's integrity is weak, a hacker could **tamper with the data and change it to show ₹1,000,000 or even ₹0**. The same applies to social media or messaging apps like WhatsApp or Telegram. For instance, if you send a message to a friend saying, "**Hi, how are you?**" and the app's integrity is weak, a hacker could intercept and alter it to something like, "**Bro, I need money urgently, send it to this account**," or even, "**I've hacked your account, now do what I say**." Integrity is a crucial part of the CIA triad for keeping data secure, and if it's weak, it creates a big opportunity for hackers to cause trouble.

### Case Study: Stuxnet Worm(2010)

**Stuxnet**, a 500-kilobyte computer worm discovered in 2010, was a sophisticated cyberweapon targeting Iran's industrial systems, particularly the Natanz nuclear facility. It operated in three steps: infiltrating Windows systems and replicating itself, exploiting Siemens Step7 software used in industrial control systems, and gaining control over machines like **programmable logic controllers to manipulate sensitive data**. Spread via infected USB drives, Stuxnet damaged 984 centrifuges at Natanz, reducing uranium enrichment efficiency by 30%[3], as confirmed by Belarusian experts who identified the worm in Iran's systems. This attack, likely initiated through a worker's USB, highlights the critical role of **Integrity** in the CIA triad, as weak integrity allowed Stuxnet to infiltrate and alter critical data, demonstrating how vital maintaining data accuracy is to prevent such devastating cyber attacks.

## 3. Availability

The term "availability" refers to the ability to access digitally stored information or services at any time when needed. For example, consider a scenario where an accident occurs, and nearby people try to call an ambulance, but all ambulances at the hospital are busy. This means the required resource (the ambulance) is not available when needed. Similarly, in a digital context, suppose I get kidnapped and manage to steal the kidnapper's phone to send a message or call for help. I try calling someone, but no one picks up for various reasons. Then, I attempt to send a message on WhatsApp or Telegram, saying, "Here's my live location, I've been kidnapped, please help." This is where availability comes into play. If the servers of Google Maps, WhatsApp, or Telegram are down, I won't be able to share my live location or contact anyone. In this way, the "A" in CIA (Confidentiality, Integrity, Availability) stands for availability, highlighting its critical importance.

### Case Study:Microsoft Outage Due to CrowdStrike(2024)

On July 19, 2024, a faulty software update (channel file 291) from CrowdStrike's[4] Falcon platform, caused by a logic error and inadequate testing, led to the largest IT outage in history, crashing 8.5 million Windows systems worldwide with the **"Blue Screen of Death"** (BSOD), costing US Fortune 500 companies $5.4 billion. The error in the update, meant to enhance Windows' named pipe execution, affected critical systems like airlines (causing thousands of flight cancellations), public transit, healthcare (disrupting hospital appointments and 911 services), financial platforms, and media, but spared macOS and Linux due to their less integrated Falcon setup. Recovery required manual intervention, slowed by BitLocker encryption, with 99% of systems restored by July 29, though full recovery for some took longer. Hackers exploited the chaos with fake support scams, while legal battles ensued, including a shareholder lawsuit and Delta Airlines' $500 million claim against CrowdStrike, who countered with their own suit. CrowdStrike introduced rigorous update testing, phased rollouts, and customer control options to prevent future issues, highlighting the critical need for robust testing, manual workarounds, and disaster recovery plans in our tech-dependent world.

## How it ensure Confidentiality,protect Integrity and maintain Availability?

The CIA triad Confidentiality, Integrity, and Availability is maintained through various measures. **Confidentiality** is ensured by implementing access control methods such as login IDs, passwords, biometrics, and OTPs, along with encrypting data at rest and in transit using technologies like **AES, TLS, and HTTPS**, and securing networks with firewalls, VPNs, and protocols like SSH e.g., Gmail uses TLS encryption and 2FA to ensure only the owner can read emails. **Integrity** is protected through hashing algorithms **(SHA256, MD5)** to detect changes, digital signatures to verify trusted sources, and version control or audit logs to track and detect **unauthorized modifications** e.g., banking systems store transaction hashes to trigger alerts if data is tampered with. **Availability** is maintained using redundancy through multiple servers and backups, load balancing to distribute traffic evenly, and disaster recovery plans to quickly restore services after failures e.g., Netflix operates multiple data centers to keep services running even if one fails

## Linux machines and how file permissions support CIA.

In Linux, file permissions help uphold the CIA triad—Confidentiality, Integrity, and Availability. **Confidentiality** is supported by restricting access to sensitive files using commands like **chmod 600 secrets.txt**, which allows only the owner to read and write the file, keeping it hidden from unauthorized users. **Integrity** is maintained by controlling write permissions, for example, **chmod 644 config.cfg** lets only the owner modify the file while others can only read it, preventing accidental or malicious changes. **Availability** is ensured by granting appropriate execute and read permissions, such as **chmod 755 script.sh**, which gives the owner full rights and others read and execute access, allowing necessary programs or scripts to run when needed.

.