# Cyber Security Basics and Attack Surface

Cyber security is all about keeping computers, phones, apps, and other stuff safe from hackers and online attacks. Today people do many things online like banking, shopping, chatting, and social media, so cyber security has become very important. If security is weak, hackers can steal information or mess up systems.

According to IBM,

“Cyber security is the practice of protecting systems, networks, and programs from digital attacks.”

Source: https://www.ibm.com/topics/cybersecurity

# CIA Triad

The CIA Triad is the basic concept in cyber security. It includes Confidentiality, Integrity, and Availability. These three things help keep data and systems safe.

## Confidentiality

Confidentiality means information should be kept private and not shared with the wrong people. If someone accesses data without permission, confidentiality is lost.

Examples:

- Bank account details
- Passwords
- Emails
- Personal photos

As explained by Cloudflare,
“Confidentiality involves preventing unauthorized access to sensitive information.”
Passwords, OTPs, encryption, and biometrics help protect confidentiality.

Source: https://www.cloudflare.com/learning/security/what-is-confidentiality/

## Integrity

Integrity means data should not be changed or modified by hackers. If data is altered, it can cause serious problems.

Examples:

- Changing marks in college database
- Changing bank transaction amount
- Editing official documents

According to Google Cloud,

"Integrity ensures data is accurate and trustworthy over its entire lifecycle."

Source: https://cloud.google.com/learn/what-is-data-integrity

## Availability

Availability means systems and services should be available when users need them. If a website or app is down, users cannot access it.

Examples:

Banking app not working

College website down

Shopping website crashing

Cloudflare explains,

"Availability ensures reliable and timely access to data and services."

Source: https://www.cloudflare.com/learning/ddos/glossary/availability/

# Types of Attackers

There are different kinds of attackers depending on skill and motivation.

- Script Kiddies – beginners using tools downloaded from the internet.
- Insiders – employees or trusted people who misuse access.
- Hacktivists – attackers with political or social motives.
- Organized Cyber Criminals – groups that hack mainly for money.
- Nation-State Hackers – supported by governments and target important systems.
- Ethical Hackers – legal hackers who find problems to improve security.

According to Kaspersky,

“Cybercriminals use different methods depending on their goals, skills, and resources.”

Source: https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

# Attack Surface

Attack surface means all the places where hackers can try to attack a system. More attack points mean more risk.
According to OWASP,

“Attack surface is the sum of all possible paths for data to enter or leave a system.”

Source: https://owasp.org/www-community/Attack_Surface

Common attack surfaces:

- Websites (login pages, forms)
- Mobile apps
- APIs
- Networks
- Cloud systems

# OWASP Top 10

OWASP Top 10 is a list of the most common web application security issues.

Some common OWASP risks are:

- SQL Injection
- Broken Authentication
- Broken Access Control
- Sensitive Data Exposure
- Security Misconfiguration
- Cross-Site Scripting (XSS)

As stated on the OWASP website,

“The OWASP Top 10 represents a broad consensus about the most critical security risks to web applications.”

Source: https://owasp.org/www-project-top-ten/

# Daily Used Applications and Security Risks

- Email
- Phishing emails
- Fake links
- Malware attachments

Google says,

“Phishing is an attempt to steal personal information using deceptive emails.”

Source: https://support.google.com/mail/answer/8253

## WhatsApp

- Scam messages
- Fake links
- Account takeover

## Banking Applications

- Password theft
- Fake banking apps
- Man-in-the-middle attacks

According to RBI,

“Users should never share OTPs or banking credentials with anyone.”

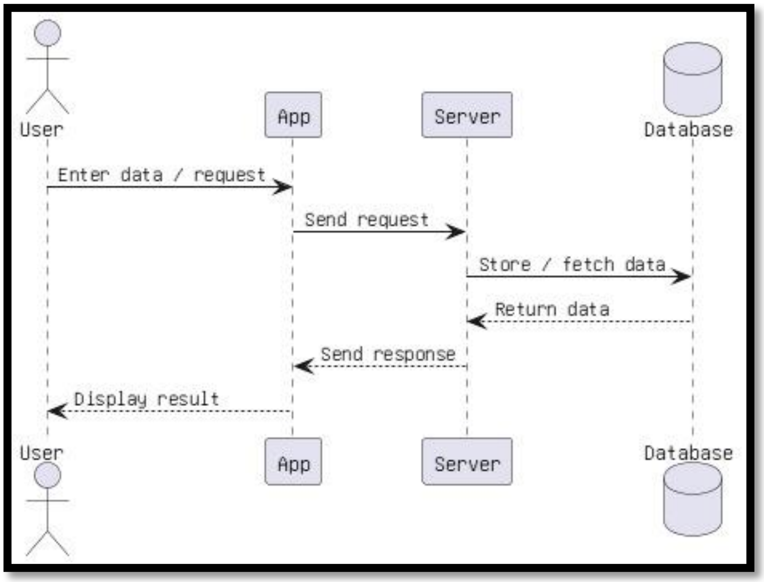
Source: https://www.rbi.org.in

## Social Media

- Fake profiles
- Data leaks
- Account hacking

# Data Flow in an Application

Normal data flow is:



At each stage, attacks can happen:

- User level: phishing and fake links
- App level: poor input checking
- Server level: misconfiguration
- Database level: SQL injection

OWASP explains data flow risks in applications:

Source: https://owasp.org/www-project-webgoat/

# Conclusion

Cyber security is very important in today’s digital world. Knowing basic concepts like CIA triad, attacker types, and attack surfaces helps in understanding how attacks happen. Reading from different websites and learning about real examples improves cyber awareness. Even small precautions can protect our data and systems.