CYBER SECURITY INTERNSHIP

Task 1

Understanding Cyber Security Basics & Attack Surface

JASHMI KS

Cyber Security

Cybersecurity is the practice of protecting digital devices, networks, and sensitive data from threats like hacking, malware, and phishing. Also known as Information Security (INFOSEC), Information Assurance (IA), or System Security.

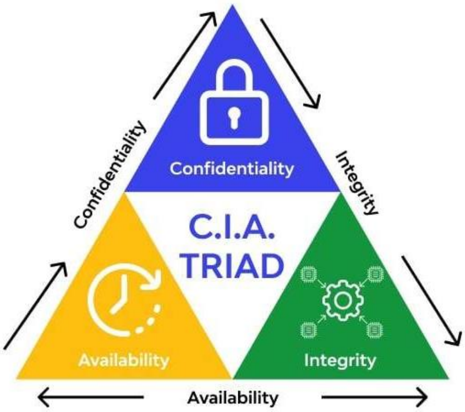
- Protects systems, networks, and personal information
- Uses security tools, policies, and safe online practices
- Prevents data theft, system damage, and unauthorized access

The primary objective of cyber security is to safeguard information assets while ensuring system reliability and trustworthiness.

CIA Triad

The CIA Triad is a core framework in information security that helps organizations protect data and maintain secure, reliable systems.

- Three principles: Confidentiality, Integrity, Availability
- Guides policies for protecting sensitive information
- Ensures data is secure, accurate, and accessible



1. Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized individuals or systems. It prevents unauthorized disclosure of data.

Examples:

- User passwords and personal data in social media platforms
- Financial information in banking systems
- Confidential organizational documents

Mechanisms used to maintain confidentiality include authentication, access control, encryption, and secure communication protocols.

A failure in confidentiality may result in data breaches, identity theft, and privacy violations.

2. Integrity

Integrity refers to the accuracy and completeness of data. It ensures that information is not altered, modified, or deleted in an unauthorized manner.

Examples:

- Accuracy of bank account balances
- Correctness of academic records
- Reliability of transaction logs

Integrity is maintained using hashing algorithms, digital signatures, version control mechanisms, and audit trails.

A compromise in integrity can lead to incorrect information, financial loss, and loss of trust in systems.

3. Availability

Availability ensures that systems, services, and data are accessible to authorized users whenever required.

Examples:

- Availability of online banking services
- Continuous access to email servers
- Reliable operation of business websites

Availability is supported through redundancy, backups, fault tolerance, load balancing, and protection against denial-of-service attacks.

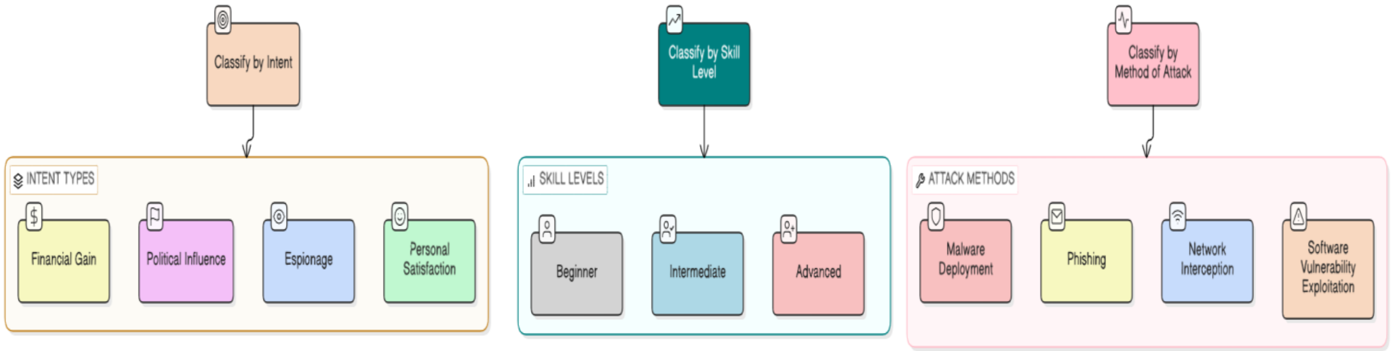
A failure in availability may cause service downtime, operational disruption, and economic losses.

Levels of Security Breach

1. **Low-Level:** Minor unauthorized activity with no data loss (e.g., scanning, failed login attempts).
2. **Moderate-Level:** Partial system access with limited data exposure (e.g., account compromise, website defacement).
3. **High-Level:** Serious compromise involving sensitive data or core systems (e.g., database breach, ransomware).
4. **Critical-Level:** Complete system compromise causing major operational or national impact (e.g., infrastructure attacks).

Types of Cyber Attackers

Cyber attackers can be broadly classified based on intent, skill level, and method of attack. The following are the most basic and commonly recognized attacker types in introductory cyber security studies.



1. Cybercriminals: Cybercriminals are individuals or organized groups that conduct attacks primarily for **financial gain**. They target banking systems, e-commerce platforms, and personal data to steal money or sell information.
Common activities: Credit card fraud, Identity theft, Ransomware attacks, Online scams

2. Malware Attackers
Malware attackers develop and distribute malicious software to damage systems, steal data, or gain unauthorized access.
Common malware types: Viruses, Worms, Trojans
These attackers often rely on **malicious downloads, infected emails, or compromised websites**.

3. Phishers
Phishers use deceptive messages or fake websites to trick users into revealing sensitive information such as passwords or banking details.
Common phishing methods:

- Fake emails
- Fraudulent login pages
- SMS and social media scams

Phishing exploits **human trust rather than technical vulnerabilities**.

4. Password Attackers
Password attackers focus on breaking or stealing login credentials to gain unauthorized access to systems and accounts.
Common techniques:

- Brute-force attacks
- Credential stuffing
- Password guessing

Weak passwords and lack of multi-factor authentication increase risk.

5. Man-in-the-Middle (MITM) Attackers
MITM attackers secretly intercept communication between two parties to steal or modify data.
Common targets:

- Public Wi-Fi networks
- Online banking sessions
- Login communications

These attacks compromise **data confidentiality and integrity**.

6. Insider Threats
Insider attackers are people within an organization who misuse their legitimate access, either intentionally or accidentally.
Types:

- Malicious insiders
- Negligent insiders

Insider threats are dangerous because they bypass many security controls.

Skill-Based Classification of Cyber Attackers

1. Script Kiddies

Script kiddies are individuals with limited technical expertise who use pre-written tools and scripts to exploit known vulnerabilities. Their attacks are usually driven by curiosity or the desire for recognition rather than clear objectives.

2. Insider Threats

Insiders are individuals within an organization who have legitimate access to systems and data. These attackers may intentionally or unintentionally cause harm. Insider attacks are particularly dangerous due to trusted access.

3. Hacktivists

Hacktivists conduct cyber-attacks to promote political, ideological, or social agendas. Their actions may include website defacement, data leaks, or service disruption.

4. Nation-State Actors

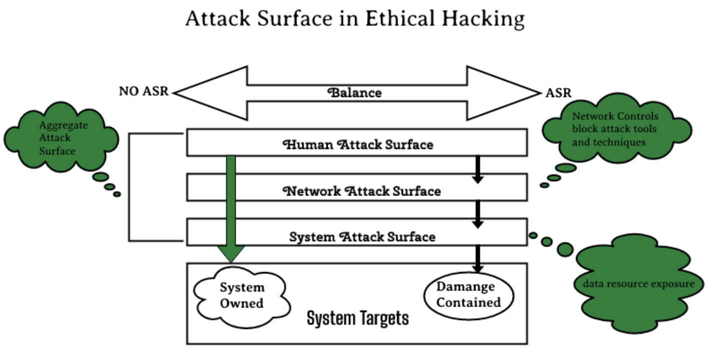
Nation-state attackers are highly skilled and well-funded groups sponsored by governments. Their targets often include critical infrastructure, defence systems, and strategic assets.

5. Attack Surface

An attack surface refers to the collection of all possible points where an unauthorized user can attempt to enter or extract data from a system. The larger the attack surface, the greater the exposure to potential attacks.

Reducing the attack surface is a key security objective.

Attack Surfaces



An attack surface is the total set of all possible points where a hacker could enter, exploit, or interact with your system. Think of it as every “crack” in your digital, physical, and human environment that attackers could use to break in.

- Bigger systems = larger attack surfaces
- More entry points = more ways to attack
- Most breaches begin with exposed attack surfaces

Common Attack Surfaces

Common attack surfaces in cybersecurity are

- Digital (web apps, cloud, APIs, code),
- Physical (devices, servers, USBs, endpoints), and
- Human/Social Engineering (phishing, insider threats, weak passwords),

representing all potential entry points for attackers to exploit vulnerabilities in software, hardware, networks, or people to gain unauthorized access or leak data

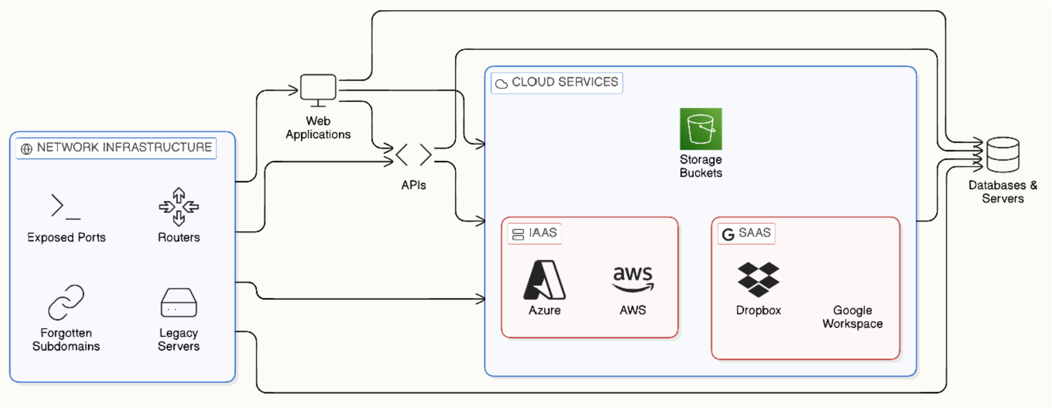
Absolutely! Let’s clearly explain each **common attack surface** in cybersecurity, with examples, in a structured and easy-to-understand way.

Common Attack Surfaces in Cybersecurity

Cybersecurity attack surfaces are the points where attackers can exploit vulnerabilities in software, hardware, networks, or people to gain unauthorized access or leak data. These surfaces can grow with cloud adoption, remote work, and third-party integrations.

1. Digital Attack Surface

All software, applications, and networked systems that can be accessed digitally, both internally and externally.



Examples:

- **Web applications:** Websites with forms, login portals, or e-commerce platforms.
- **APIs (Application Programming Interfaces):** Endpoints that connect services or apps.
- **Cloud services:** SaaS (Google Workspace, Dropbox), IaaS (AWS, Azure), storage buckets.
- **Databases & servers:** Customer databases, application servers, or OS systems.
- **Network infrastructure & forgotten subdomains:** Exposed ports, routers, and legacy servers.

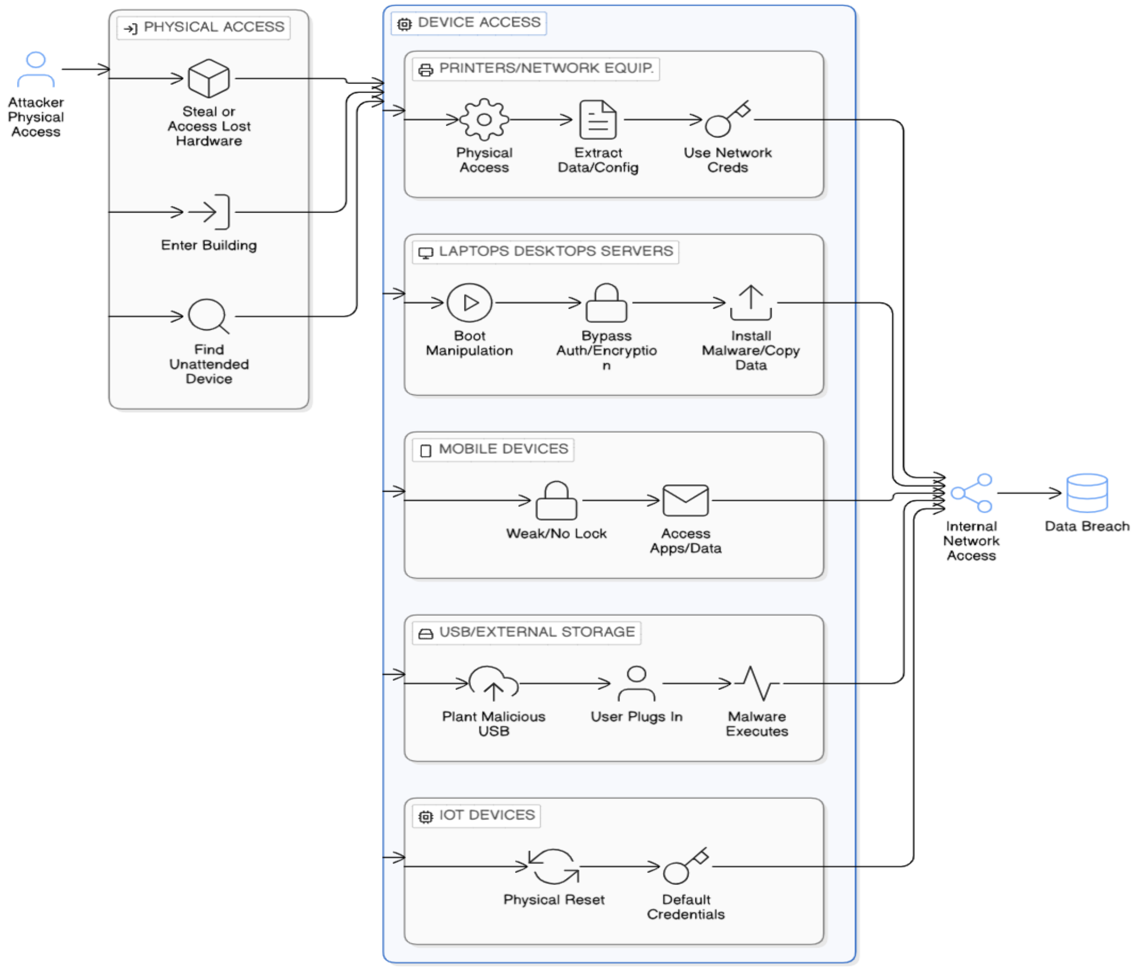
Vulnerabilities:

- Misconfigured cloud storage or firewalls
- Unpatched software or outdated systems
- Insecure code in apps or APIs
- Exposed ports or network devices
- Shadow IT: unauthorized apps or services

Real-world example: A web application login page that doesn’t validate input → attacker performs SQL injection to steal user credentials.

2. Physical Attack Surface

Tangible hardware and devices that can be physically accessed or manipulated.



Examples:

- Laptops, desktops, and servers
- Mobile phones and tablets
- USB drives and external storage devices
- IoT devices (smart cameras, sensors)
- Printers and network hardware

Vulnerabilities:

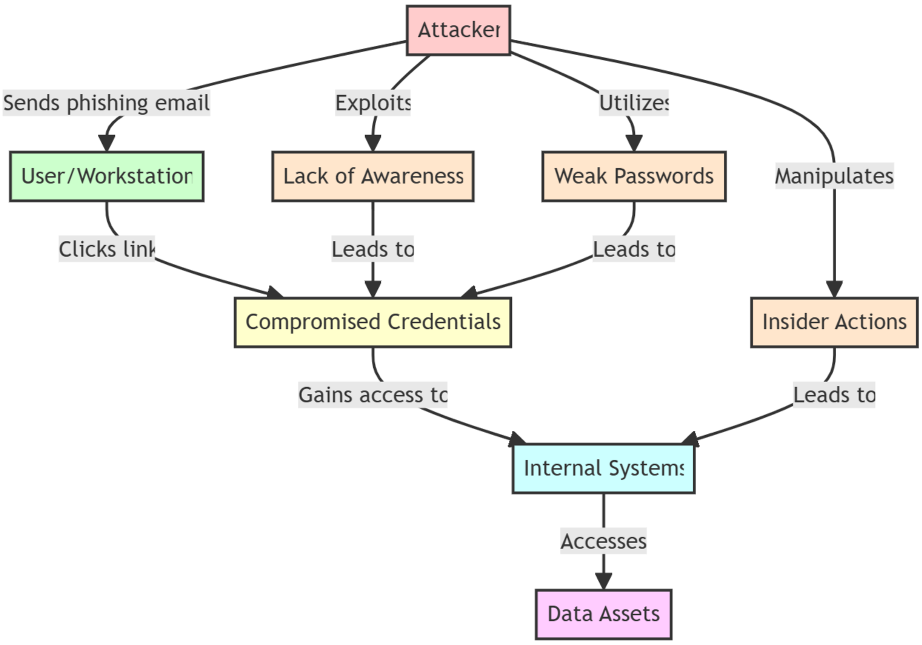
- Lost or stolen devices containing sensitive data
- Unauthorized physical access to offices, server rooms, or network ports
- Carelessly discarded hardware or storage devices

Real-world example:

An employee leaves a company laptop unattended in a cafe → attacker steals it and accesses company files.

3. Human / Social Engineering Attack Surface

Exploiting human behavior, mistakes, or trust to gain unauthorized access



Examples:

- **Phishing emails:** Tricking users to click links or provide credentials.
- **Baiting & pretexting:** Offering something enticing to manipulate users.
- **Insider threats:** Disgruntled or careless employees sharing sensitive info.
- **Weak or reused passwords:** Credentials easily guessed or stolen.
- Lack of security awareness or training

Vulnerabilities:

- Users falling for social engineering attacks
- Poor password practices
- Lack of cybersecurity hygiene

Real-world example:

An attacker sends a fake “IT update” email → employee enters their login info → attacker gains access to internal systems.

OWASP Top 10

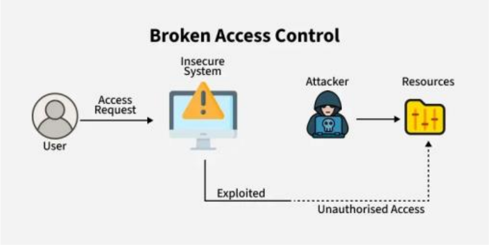
OWASP stands for the Open Web Application Security Project. It is a non-profit global online community consisting of tens of thousands of members and hundreds of chapters that produces articles, documentation, tools, and technologies in the field of web application security.

- OWASP releases the Top 10 Web Application Security Risks every 3-4 years based on real-world vulnerability data.
- The list is created using frequency, severity, and impact of security flaws found in web applications.
- It highlights the most common and most dangerous vulnerabilities that attackers frequently exploit.
- The latest update (2021) helps developers and security professionals build more secure applications.
- It is considered an essential security guide and industry standard for web application security best practices.

OWASP Top 10 risks include:

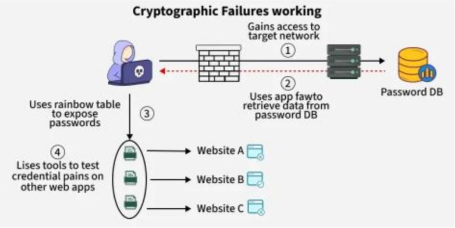
1. Broken Access Control

Occurs when users can access data or functions beyond their permissions due to weak authorization checks.
Attackers exploit this to view or modify other users' data or gain admin privileges.



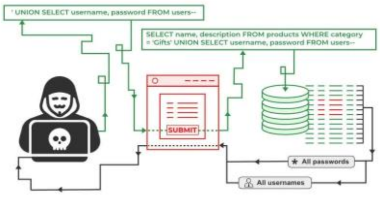
2. Cryptographic Failures

Happens when sensitive data is not properly encrypted during storage or transmission.
Weak algorithms, poor key management, or missing encryption can expose confidential information.


Cryptographic Failures working
Gains access to target network
①
②
Uses app fawto retrieve data from password DB
Password DB
Uses rainbow table to expose passwords
③
④
Lises tools to test credential pains on other web apps
Website A
Website B
Website C

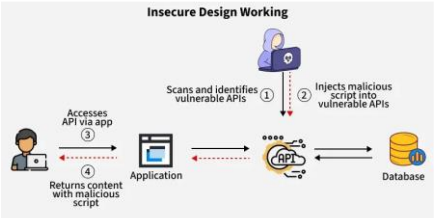
3. Injection

Occurs when untrusted input is inserted into commands or queries and executed by the system.
This allows attackers to manipulate databases, execute commands, or bypass authentication.


' UNION SELECT username, password FROM users--
SELECT name, description FROM products WHERE category = 'Gifts' UNION SELECT username, password FROM users--
SUBMIT
All passwords
All usernames

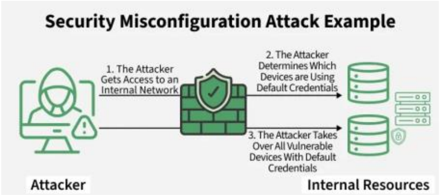
4. Insecure Design

Results from security flaws introduced during the system design phase. Even correctly implemented code remains vulnerable if security requirements are not planned early.


Insecure Design Working
Scans and identifies vulnerable APIs
①
②
Injects malicious script into vulnerable APIs
Accesses API via app
③
④
Returns content with malicious script
Application
API
Database

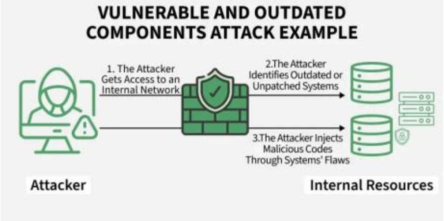
5. Security Misconfiguration

Caused by improper or default security settings in applications, servers, or cloud services.
Attackers exploit exposed services, default credentials, or unnecessary features.


Security Misconfiguration Attack Example
1. The Attacker Gets Access to an Internal Network
2. The Attacker Determines Which Devices are Using Default Credentials
3. The Attacker Takes Over All Vulnerable Devices With Default Credentials
Attacker
Internal Resources

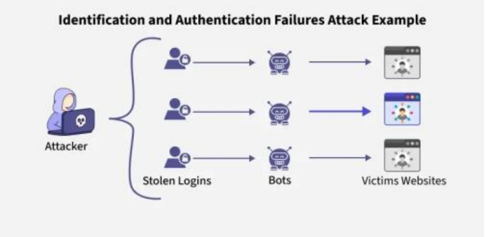
6. Vulnerable and Outdated Components

Occurs when applications use libraries or software with known vulnerabilities.
Attackers exploit these outdated components to gain access or execute malicious code.


VULNERABLE AND OUTDATED COMPONENTS ATTACK EXAMPLE
1. The Attacker Gets Access to an Internal Network
2.The Attacker Identifies Outdated or Unpatched Systems
3.The Attacker Injects Malicious Codes Through Systems' Flaws
Attacker
Internal Resources

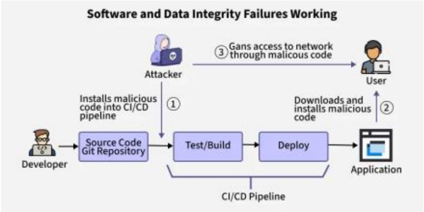
7. Identification and Authentication Failures

Happens when authentication mechanisms are weak or improperlyimplemented.
Attackers can brute-force, steal credentials, or impersonate legitimate users.



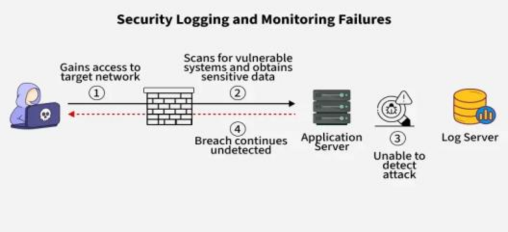
8. Software and Data Integrity Failures

Occurs when software updates, plugins, or data are not verified for authenticity and integrity.


Software and Data Integrity Failures Working
Attacker
③ Gans access to network through malicous code
User
Installs malicious code into CI/CD pipeline
①
Downloads and installs malicious code
②
Developer
Source Code Git Repository
Test/Build
Deploy
Application
CI/CD Pipeline

9. Security Logging and Monitoring Failures

Happens when security events are not properly logged or monitored.
This allows attackers to operate undetected and delays incident response.


Security Logging and Monitoring Failures
Gains access to target network
①
Scans for vulnerable systems and obtains sensitive data
②
④
Breach continues undetected
Application Server
③
Unable to detect attack
Log Server

10. Server-Side Request Forgery (SSRF)

Occurs when a server fetches user-supplied URLs without validation.
Attackers force the server to access internal or restricted resources, leaking sensitive data.

Mapping Daily Applications to Attack Surfaces

1. Email Systems

Attack surfaces include login pages, mail servers, databases, and network connections. Common threats are phishing, credential theft, malware delivery, and unauthorized access.

2. Banking Applications

Attack surfaces include mobile apps, APIs, backend servers, and databases. Common threats include man-in-the-middle attacks, data manipulation, and fraudulent transactions.

3. Social Media Platforms

Attack surfaces include web apps, APIs, user accounts, and third-party integrations. Common threats include account takeover, data scraping, and privacy breaches.

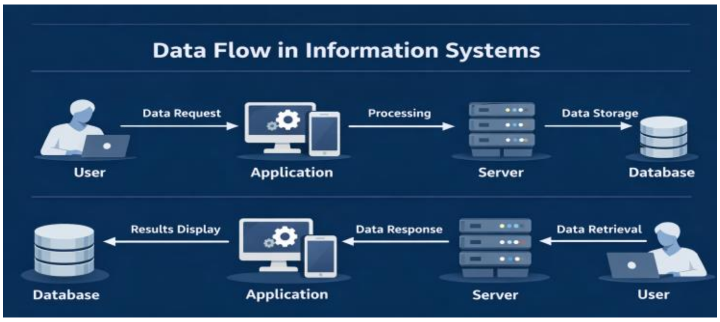
4. E-Commerce Applications

Attack surfaces include payment gateways, web applications, databases, and APIs. Common threats include card skimming, SQL injection, and fake transactions.

5. Cloud Storage Services

Attack surfaces include cloud consoles, APIs, access keys, and network configurations. Common threats include misconfigurations, data leaks, and unauthorized access.

Data Flow in Information Systems



A typical application follows a structured flow of data between components to process user requests securely and efficiently.

1. **User → Application**
   The user initiates a request (login, search, transaction) through a web or mobile application.
   Potential attack point: Input manipulation, malicious data entry, phishing.

2. **Application → Server**
   The application sends the request to the backend server for processing and business logic execution.
   Potential attack point: Insecure APIs, session hijacking, man-in-the-middle attacks.
3. **Server → Database**
   The server queries or updates the database to fetch or store required data.
   Potential attack point: SQL injection, unauthorized database access.
4. **Database → Server**
   The database returns the requested data to the server after processing the query.
   Potential attack point: Data leakage, improper access control.
5. **Server → Application**
   The server sends processed results back to the application.
   Potential attack point: Data tampering, insecure data transmission.
6. **Application → User**
   The application displays the final output to the user.
   Potential attack point: Cross-site scripting (XSS), information exposure.

Potential Attack Points in Data Flow

- User level: phishing attacks and weak credentials
- Application level: input validation failures and malicious scripts
- Server level: unauthorized access and configuration flaws
- Database level: data theft and tampering
- Network level: interception and traffic manipulation

From this study, I understood that cybersecurity is mainly about keeping our data, systems, and online services safe from hackers and attacks. Attacks usually happen through weak points like insecure apps, devices, networks, or even human mistakes such as clicking phishing links. By knowing about attack surfaces, attacker types, and how data flows in a system, we can understand where problems may occur and how to protect systems better.