**SECURITY IN ECOMMERCE**

**E-COMMERCE SECURITY**:  
E-commerce security refers to the protection of electronic transactions and data involved in buying and selling products or services online. It ensures that customers, businesses, and payment systems are safe from fraud, theft, and data breaches.



**Main Aspects of E-Commerce Security**

1. **Confidentiality**
   * Ensures that information is only accessible to authorized parties.
   * Example: Encrypting credit card details during online payment.
2. **Integrity**
   * Ensures that the data sent or received is not altered.
   * Example: Digital signatures validate data authenticity.
3. **Authentication**
   * Verifies the identity of users and systems.
   * Example: Username/password or OTP login systems.
4. **Non-repudiation**
   * Prevents denial of a transaction after it has been completed.
   * Example: E-receipts, email confirmations, and digital signatures.
5. **Availability**
   * Ensures that the website or service is accessible when needed.
   * Example: Protection against DDoS attacks.

**⚠️ Common E-Commerce Security Threats**

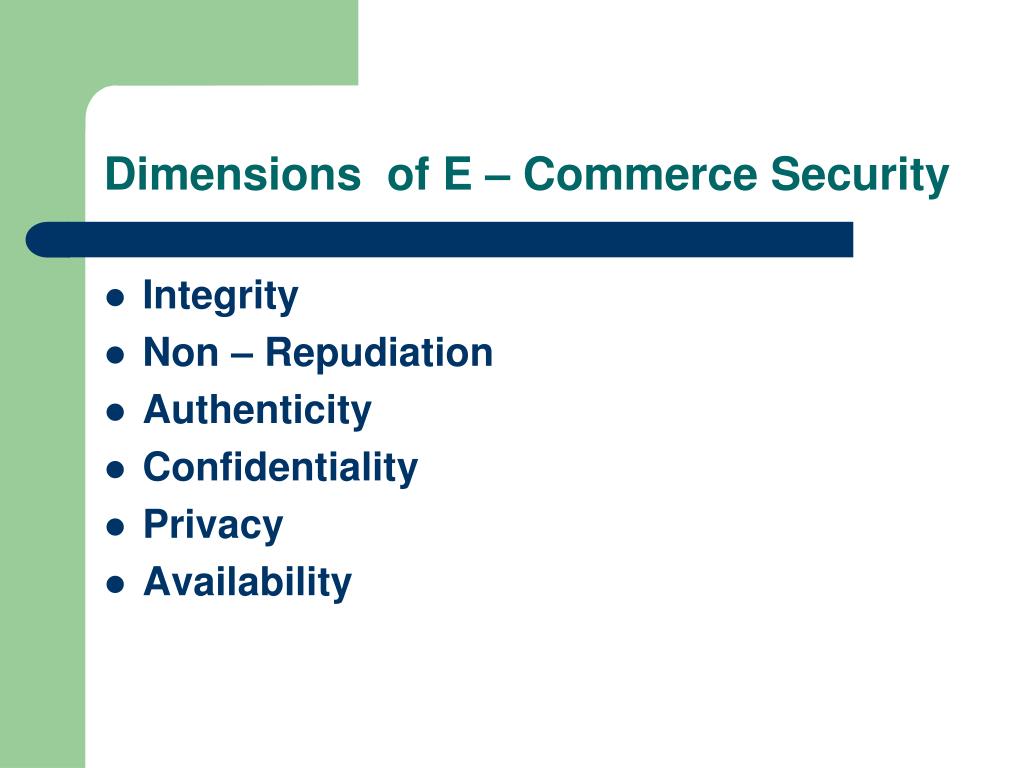
1. **Phishing Attacks** – Fake emails or websites to steal user data.
2. **Malware/Viruses** – Software that can damage or steal data.
3. **Hacking** – Unauthorized access to systems or databases.
4. **Credit Card Fraud** – Use of stolen card details.
5. **Denial of Service (DoS) Attacks** – Making a website crash by overwhelming it with traffic.
6. **Man-in-the-Middle Attacks** – Interception of data between user and website.

**🛡️ Security Measures for E-Commerce**

1. **SSL Certificates (HTTPS)** – Encrypt data between browser and server.
2. **Secure Payment Gateways** – Use trusted platforms like PayPal, Stripe, etc.
3. **Two-Factor Authentication (2FA)** – Extra layer of login security.
4. **Firewall and Antivirus Software** – Protection against malware and unauthorized access.
5. **Data Encryption** – Protects sensitive information in storage and transmission.
6. **Regular Security Audits** – Identifies and fixes vulnerabilities.
7. **Strong Password Policies** – Prevents easy-to-guess passwords.

**Dimensions of E-Commerce Security**

In e-commerce, **security dimensions** refer to key principles or goals that protect digital transactions and data. There are **six main dimensions**:



**1. Confidentiality**

* **Definition**: Ensuring that information is accessible only to those authorized to have access.
* **Example**: Encrypting customer credit card data so hackers cannot read it.

**2. Integrity**

* **Definition**: Ensuring that information is accurate and cannot be changed or tampered with.
* **Example**: Order details should not be modified during transmission between buyer and seller.

**3. Availability**

* **Definition**: Ensuring that e-commerce systems and services are always accessible when needed.
* **Example**: Using backup servers to keep a website online during high traffic or attacks.

**4. Authenticity**

* **Definition**: Ensuring that parties involved in a transaction are who they claim to be.
* **Example**: Login systems, digital certificates, or verified seller badges.

**5. Non-repudiation**

* **Definition**: Ensuring that a party in a transaction cannot deny the authenticity of their signature or the transaction.
* **Example**: Sending a confirmation email or using digital signatures to record proof of transaction.

**6. Privacy**

* **Definition**: Protecting personal and financial data of users from being shared without consent.
* **Example**: Websites should not sell users' information without permission.

**🧾 Summary Table:**

| **Dimension** | **Description** | **Example** |
| --- | --- | --- |
| Confidentiality | Prevent unauthorized access to data | SSL encryption |
| Integrity | Prevent data alteration | Hash functions, checksums |
| Availability | Ensure systems are online and responsive | Backup servers, anti-DDoS systems |
| Authenticity | Verify identity of users and businesses | Login, certificates |
| Non-repudiation | Prevent denial of transaction | Digital receipts, email confirmations |
| Privacy | Protect personal data from misuse | Data protection policies |

**Security Threats in E-Commerce**

E-commerce platforms are often targeted by cybercriminals because they handle sensitive information such as credit card numbers, passwords, and personal details. Below are the **major security threats in e-commerce**:



**1. Phishing Attacks**

* **What it is**: Fake emails or websites trick users into revealing sensitive information.
* **Example**: A fake email that looks like it’s from Amazon asking for login or card details.

**2. Credit Card Fraud**

* **What it is**: Use of stolen or fake credit card details for purchases.
* **Example**: A hacker uses someone else's credit card to buy products online.

**3. Hacking**

* **What it is**: Unauthorized access to e-commerce databases or websites.
* **Example**: Hackers break into a site and steal customer data or manipulate prices.

**4. Malware and Viruses**

* **What it is**: Malicious software that infects systems to steal or destroy data.
* **Example**: A Trojan hidden in a free download that steals admin login info.

**5. Denial of Service (DoS) & Distributed DoS (DDoS) Attacks**

* **What it is**: Overloading a server with traffic so it crashes.
* **Example**: An online store becomes unavailable during a big sale due to a DDoS attack.

**6. Man-in-the-Middle Attacks (MITM)**

* **What it is**: Intercepting data between user and website.
* **Example**: An attacker steals login details by capturing network traffic on public Wi-Fi.

**7. Data Breach**

* **What it is**: Large-scale theft or exposure of sensitive customer data.
* **Example**: A database leak exposes thousands of customer emails and passwords.

**8. E-skimming**

* **What it is**: Inserting malicious code into a website to steal payment info during checkout.
* **Example**: Payment page captures card numbers and sends them to attackers.

**9. Fake Websites (Spoofing)**

* **What it is**: Creating a site that looks like a real e-commerce site to scam users.
* **Example**: A site named “amaz0n.com” pretending to be Amazon.

**10. SQL Injection**

* **What it is**: Inserting malicious SQL code into input fields to gain access to databases.
* **Example**: A hacker extracts usernames and passwords through a search box.

**🛡️ How to Prevent These Threats**

* Use **SSL/TLS encryption**.
* Enable **two-factor authentication** (2FA).
* Use **firewalls and antivirus software**.
* Conduct **regular security audits**.
* Educate users about **phishing and fake sites**.
* Keep platforms and plugins **up to date**.

**vulnerabilities in e-commerce**

**🔐 1. Poor Website Security**

* **Unpatched software/plugins**: Hackers exploit outdated CMS or plugins.
* **Weak authentication**: Weak passwords or lack of multi-factor authentication (MFA).
* **Lack of HTTPS**: No SSL encryption allows data interception (man-in-the-middle attacks).

**🕵️ 2. Data Breaches**

* Attackers gain access to sensitive user data like:
  + Credit card info
  + Email addresses
  + Login credentials

**🧑‍💻 3. SQL Injection**

* Malicious SQL code is injected into forms or URLs to access or manipulate databases.

**🌐 4. Cross-Site Scripting (XSS)**

* Attacker injects malicious scripts into websites, often through comment sections or input fields.

**🧬 5. Cross-Site Request Forgery (CSRF)**

* Forces users to perform unwanted actions without their knowledge, like changing passwords or making purchases.

**📩 6. Phishing Attacks**

* Fake emails or websites trick users into sharing credentials or payment info.

**📦 7. Insecure APIs**

* Poorly protected APIs can expose user data or allow unauthorized transactions.

**⚙️ 8. Server Misconfiguration**

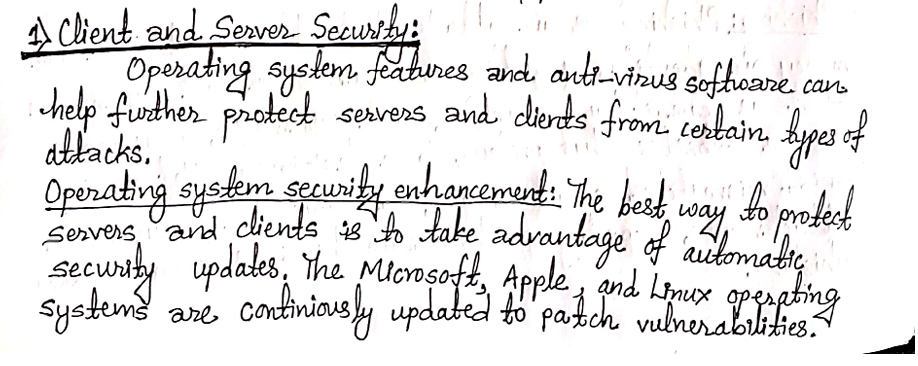
* Open ports, directory listing, or default settings can expose the backend to attackers.

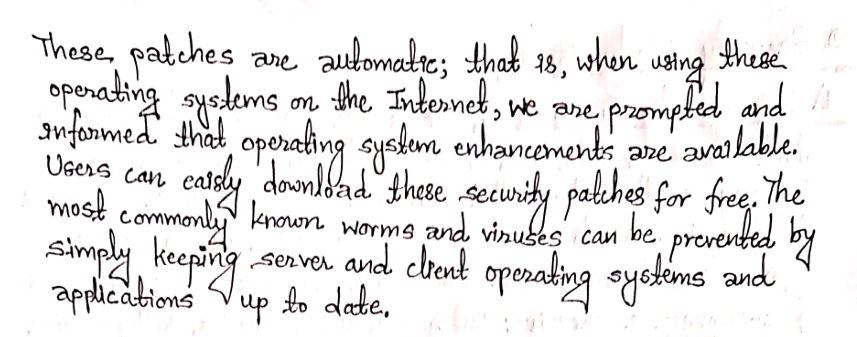
**📲 9. Mobile App Vulnerabilities**

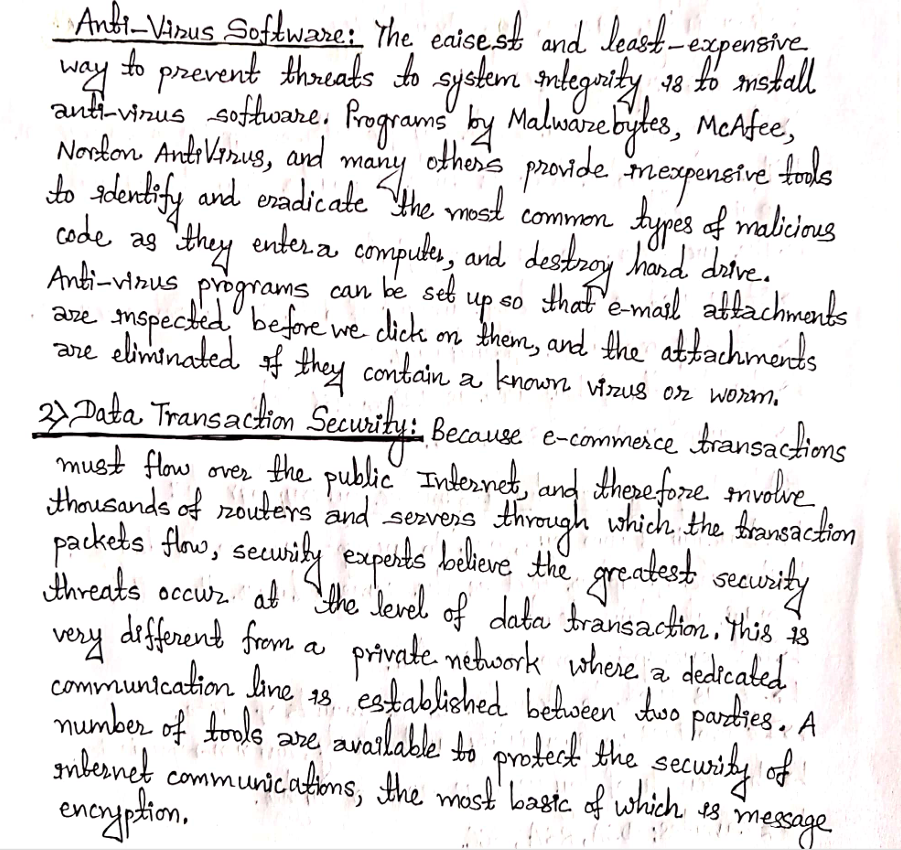
* Insecure mobile e-commerce apps may store sensitive data or use unencrypted connections.

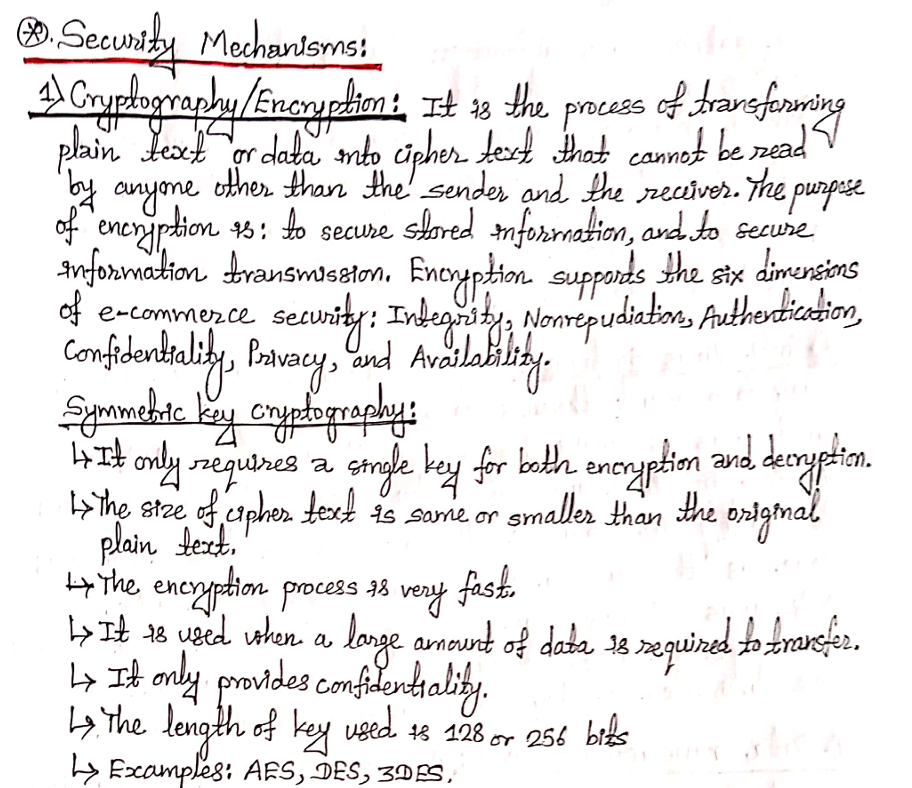
**💳 10. Payment Gateway Exploits**

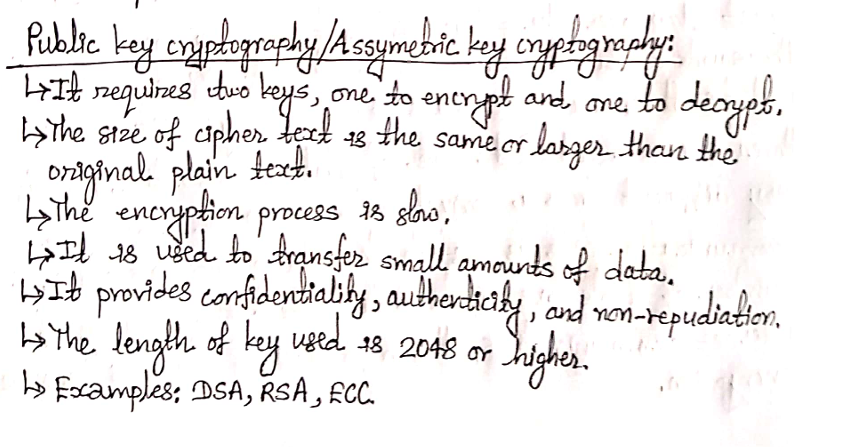
* Weak validation can allow:
  + Fake transactions
  + Payment manipulation
  + Replay attacks

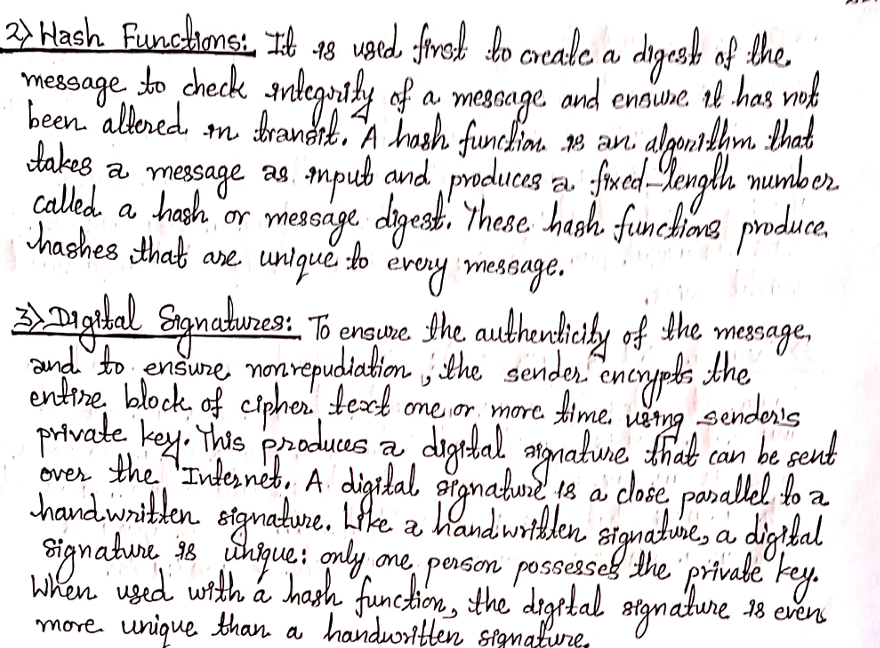




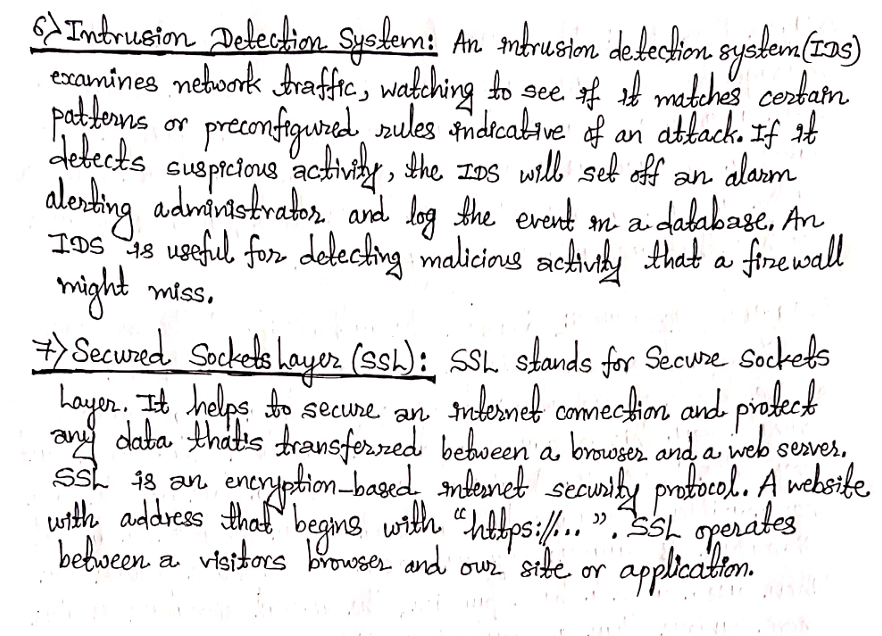






****

****

****

**THANK YOU**