

Introduction to Network and Network Security

Prepared by Dr. Sumaya Alkubaisi

FNT625
Cybersecurity Concepts

Lecture 2



Learning Goals

By the end of this lecture, you will be able to:

- Define what a network is and why it matters in fintech.
- Explain OSI and TCP/IP communication models.
- Identify key devices and protocols.
- Recognize common network threats.
- Apply network defenses and best practices.

What is a Computer Network?

- A **computer network** is a group of two or more devices (computers, servers, smartphones, printers, etc.) that are connected to share information and resources.

Why it matters?

Networks are the foundation of modern communication—enabling email, online shopping, streaming, banking, and cloud services. Without networks, devices would work in isolation.

Example:

-At home, your laptop, smart TV, and phone connect to the same Wi-Fi router so you can stream movies, share files, or print documents wirelessly.

Why Networks Matter in Fintech

- Enable payments, trading, and online banking.
- Without secure networks, financial systems are exposed to fraud.

Example:

- Mobile wallets depend on secure internet connectivity.
- Bank ATMs connect to central servers over a secure network to verify balances and approve withdrawals in real time.

Types of Networks

LAN (Local Area Network):

Connects computers within a small area (office, home, or single building).

Example 1: A bank branch network connecting staff computers.

Example 2: Home Wi-Fi router connecting laptop and phone.

Metropolitan Area Network (MAN)

Between LAN and WAN, there is also MAN (Metropolitan Area Network), which covers city-wide networks, such as linking government offices across a city.

❖ It's less common in fintech, but useful to know.

Types of Networks

Wide Area Network (WAN)

A network that connects multiple LANs across large distances, often using public infrastructure like the internet.

Key Features: Covers cities, countries, or even continents; usually slower and more expensive than LANs.

Example:

- A global bank uses a WAN to link its offices in New York, London, and Tokyo for secure data exchange.
- A university connects different campuses in different cities using a WAN.

Types of Networks

Internet

The Internet is the largest network in the world, connecting millions of LANs and WANs together.

- It is the backbone of global communication and the digital economy.
- Without the Internet, e-commerce, global trading, and international payments would not be possible.
- It allows access to information, services, and communication between people and organizations anywhere.

Examples:

- PayPal: Uses the Internet to securely process financial transactions between different countries.
- Video Calls (Zoom, WhatsApp): Connect people from different continents in real time with audio and video.
- E-commerce (Amazon, eBay): Relies on the Internet to display products, receive orders, and process payments.
- E-Government Services: Paying bills or applying for official documents online instead of visiting offices.

Network Topologies

- The physical or logical structure of how devices are arranged in a network.
- Topology affects performance of a network, it influences speed, reliability, cost, and security

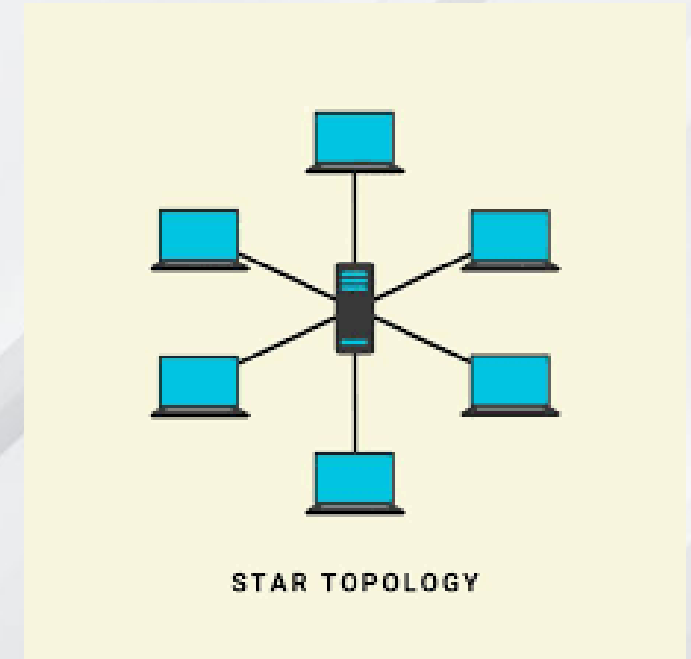
Network Topologies

1. Star Topology

- All devices connect to a central hub or switch.
- Easy to manage, but if the hub fails, the whole network stops.

Example:

- A bank branch connects all teller computers to one central server.
- Home Wi-Fi router connects laptops, phones, and smart TVs.



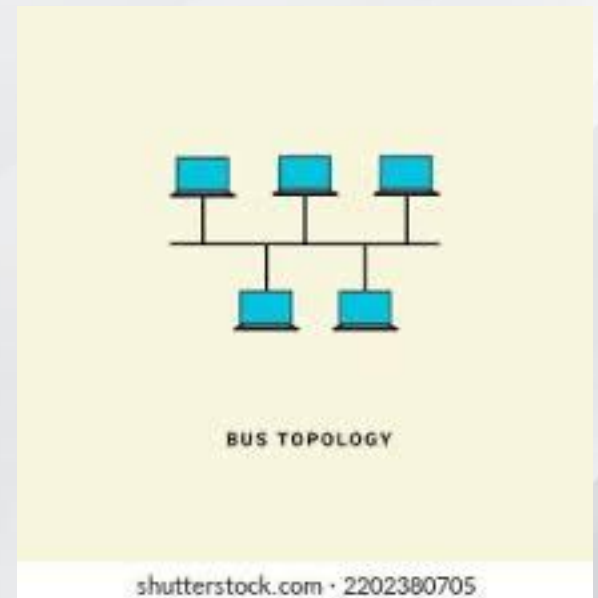
Network Topologies

2. Bus Topology

- All devices share a single communication line (a “backbone”).
- Cheap but vulnerable: if the backbone fails, the network goes down.

Example:

- Rare in banks today, but older branches sometimes used it for cost savings.
- Early home networks with one coaxial cable.



Network Topologies

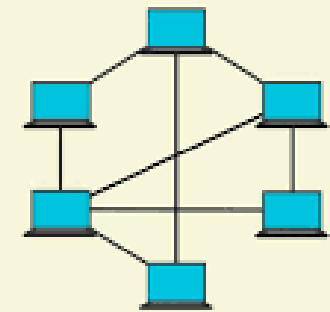
3. Mesh Topology

- Devices are interconnected (many-to-many links).
- Very reliable, but costly to set up.

Example:

-Data centers or stock exchanges use mesh for redundancy.

-Some smart home systems (IoT) use mesh so devices relay signals to each other.



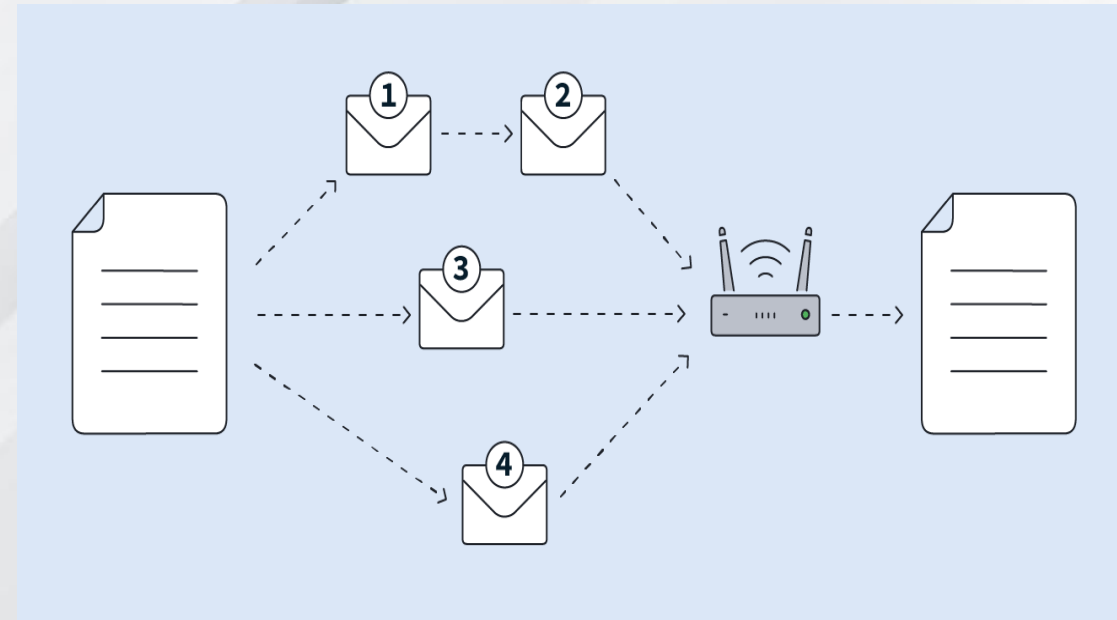
MESH TOPOLOGY

Data in Transit

- Information sent across a network is broken into small units called **packets**.
- Understanding packets helps in analyzing and securing data transfer.

Example:

- A stock order is divided into packets before it reaches the trading server.
- Streaming a movie means thousands of small packets arriving in order.



Key Terms

Bandwidth: Maximum data capacity of a connection.

Latency: Delay in sending/receiving data.

- Low latency and high bandwidth are critical for real-time fintech operations.

Example:

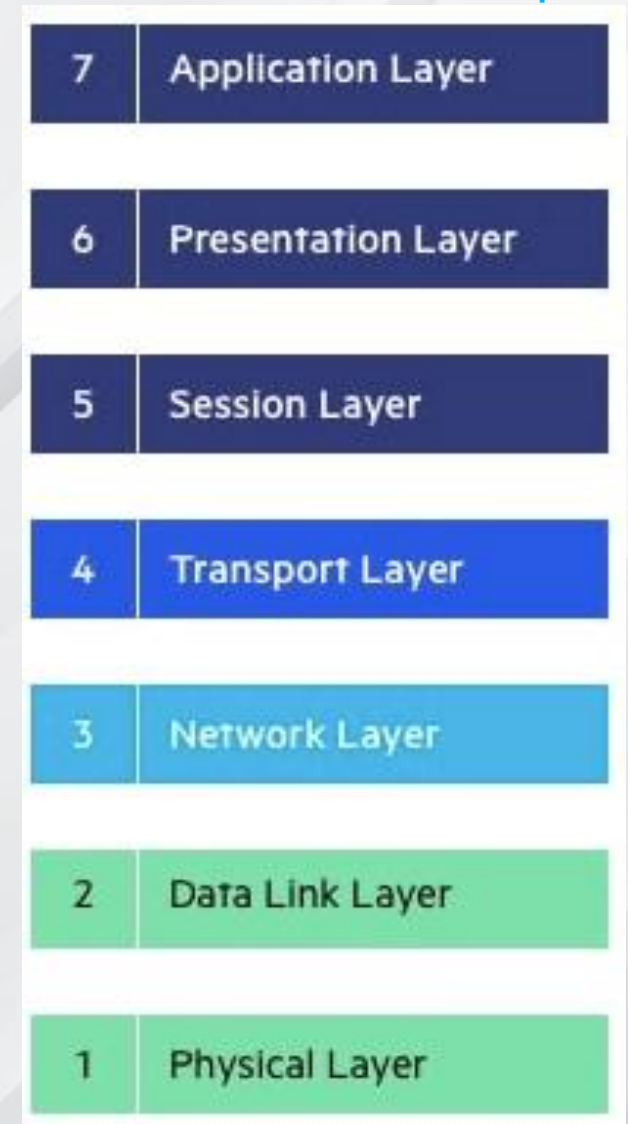
- High-frequency trading firms need ultra-low latency to execute trades.
- Online gaming suffers lag if latency is high.

OSI Model Overview

- A 7-layer model describing how data moves through a network.
- Provides a standard way to design and troubleshoot networks.

Example:

-An online banking request passes through OSI layers to ensure secure delivery.



1.Application Layer

- The closest layer to the end-user. It provides network services directly to applications (like web browsers, email clients).
- Functions: User interfaces, communication protocols, resource sharing.

Example:

When you open Gmail and send an email, Gmail uses SMTP (protocol at this layer).

Other protocols: HTTP/HTTPS (web), FTP (file transfer), DNS (domain name lookup).

2.Presentation Layer

- Translates, formats, compresses, or encrypts the data so both sender and receiver understand it.
- Functions: Data encoding, encryption/decryption, compression.

Example:

- Email text is encoded in UTF-8 so it looks the same on any device.
- If you send a PDF as an attachment, it might be compressed into a ZIP file.
- For secure emails, data is encrypted using SSL/TLS.

3.Session Layer

- Manages and controls the dialog (session) between two devices. It keeps connections alive and synchronizes communication.
- Functions: Establish, maintain, and terminate sessions.

Example:

- When you log in to Gmail, a session is created between your device and the server.
- If the connection drops, the session layer can re-establish it without you logging in again.
- Video calls (Zoom/Teams) rely on session management to keep streams continuous.

4.Transport & 5.Network Layers

4.Transport Layer: Ensures reliable delivery of data between devices by breaking it into segments and managing error checking.

Example:

- Sending an email: data is split into TCP segments.
- TCP ensures the email arrives complete and in order.

5.Network Layer: Handles logical addressing (IP addresses) and decides the best route for data across networks.

Example:

- Your email data gets an IP address (source = your PC, destination = Gmail server).
- Routers along the way use this address to deliver the packet.
- Protocols: IP, ICMP, OSPF, RIP.

6.Data Link & 7.Physical Layers

6.Data Link: Transfers packets between nearby devices (Ethernet, Wi-Fi).

Example:

- Your laptop's MAC address (like 00:1A:2B:3C:4D:5E) is used to deliver the packet to your Wi-Fi router.
- Protocols: Ethernet, Wi-Fi (802.11), ARP.

7.Physical: The lowest layer — transmits raw bits (0s and 1s) as electrical signals, light pulses, or radio waves over the physical medium (cables, signals, fiber optics).

Example:

- Your email data becomes electrical signals in copper cables, light pulses in fiber optics, or radio signals in Wi-Fi.
- Devices: Cables, switches, hubs.

Example: Sending an Email – OSI Model

Application Layer:

You write your email in Gmail/Outlook. This is the app you see and use.

Presentation Layer:

The email is turned into a format the computer understands (like changing letters into numbers) and may be locked (encrypted) for safety.

Session Layer:

A “conversation” is opened between your computer and the email server so they can keep talking until the email is sent.

Transport Layer:

Your email is cut into smaller pieces (like pages of a book). Each piece is numbered so it arrives in the right order, with checks to make sure nothing is missing.

Network Layer:

Each piece is given an address (your IP and the server’s IP), like writing the sender and receiver addresses on an envelope. Routers use this address to find the path.

Data Link Layer:

The data is packed with a local delivery tag (MAC address) so it can move from your computer to the nearest device (like your Wi-Fi router).

Physical Layer:

Finally, the data becomes tiny signals (electric pulses, light, or radio waves) that travel through cables or Wi-Fi until it reaches the email server.

TCP/IP Model

- The 4-layer the practical networking model used in real-world internet communication.
- Simpler and more practical than OSI (Academic with 7 layers).

The 4 Layers:

- **Application Layer**

- What the user interacts with (websites, apps, email).
- Examples: HTTP/HTTPS, FTP, SMTP, DNS.
- **Finance:** Fintech APIs (like PayPal, Stripe) send/receive data using HTTPS here.

- **Transport Layer**

- Ensures reliable communication between two devices.
- Protocols: **TCP** (reliable, ordered, error-checked) and **UDP** (faster, no guarantees).
- **Example:** YouTube uses TCP so video packets arrive in order.

TCP/IP Model

Internet Layer

- Decides how data packets travel across networks (addressing + routing).
- Protocol: IP (Internet Protocol).
- Example Your request to YouTube is routed using your IP address.

Network Access Layer (Link Layer)

- Physical delivery of data over Wi-Fi, Ethernet, or mobile networks.
- Everyday: Your laptop sends signals through Wi-Fi to the router.

Why It Matters

- Simpler than OSI (4 vs 7 layers).
- Practical: This is the real backbone of the internet.
- Cybersecurity: Attacks can target different layers (e.g., DDoS at transport layer, phishing at application layer).

Network Devices

Routers

- Devices that forward data between networks.
- Directs traffic efficiently and securely.

Example:

- Router connects branch LAN to central banking servers.
- Home router connects your devices to your Internet Service Provider (ISP).

Network Devices

Switches

- Devices that connect multiple computers in the same LAN.
- Reduces traffic and improves efficiency.

Example: -Switch connects all tellers' computers in a branch.
 -Office switch connects employees' PCs and printers.

Firewalls

- Hardware or software that filters traffic based on rules.
- Prevents unauthorized access.

Example: Firewall blocks suspicious logins to online banking.

Network Protocols (Key Protocols)

HTTP/HTTPS (HyperText Transfer Protocol / Secure)

What it does: Web communication; HTTPS encrypts data.

Example:

- Online banking protects passwords & transactions.
- “https://” when shopping online.

DNS (Domain Name System)

What it does: Converts website names into IP addresses.

Example:

- Bank website loads correctly for customers.
- Typing “google.com” opens Google.

Network Protocols (Key Protocols)

SMTP (Simple Mail Transfer Protocol)

What it does: Sends emails between servers.

Example:

- Banks send transaction alerts or statements.
- Sending an email via Gmail or Outlook.

Network Protocols (Secure Protocols)

SFTP (Secure File Transfer Protocol)

What it does: Transfers files securely between computers.

Example:

- Banks use SFTP to send sensitive reports to regulators.
- Uploading files to a secure cloud storage service.

TLS / SSL (Transport Layer Security / Secure Sockets Layer)

What it does: Encrypts data during communication to prevent eavesdropping.

Example:

- Online banking websites encrypt login and transaction data.
- Checkout pages on e-commerce sites use SSL (https://).

CIA Triad (Security Principles)

Confidentiality: Keep data private.

Example:

- Encrypt customer transactions.
- WhatsApp uses end-to-end encryption.

Integrity: Ensure data is not altered or tampered with.

Example:

- Bank balances cannot be changed by attackers.
- Digital signatures verify files are original.

Availability: Keep systems online and accessible.

Example:

- ATMs and online banking must be operational.
- Websites must load reliably for users.

Network Threats

DDoS Attacks (Distributed Denial of Service)

An attack that overwhelms a server, website, or network with a massive number of fake requests from multiple sources, making the service slow or completely unavailable to legitimate users.

Example:

- A stock exchange website is knocked offline during a DDoS attack, preventing trading.
- Online gaming servers crash when targeted by a coordinated flood of traffic.

Network Threats

MITM (Man-in-the-Middle) Attacks

A cyberattack where the attacker secretly intercepts or modifies communication between two parties, allowing them to eavesdrop, steal credentials, or inject malicious content.

Prevention:

- Use secure networks.
- Ensure websites start with HTTPS.
- Avoid entering sensitive information on public networks without a VPN.

Example:

- A hacker sets up a fake Wi-Fi hotspot in a café to steal mobile banking login details.
- Someone intercepts messages sent over an unsecured public Wi-Fi network.

Network Threats

Spoofing

When an attacker pretends to be a trusted entity by faking their IP address, MAC address, email address, or phone number to deceive victims and gain unauthorized access or information.

Example:

- Email spoofing tricks bank customers into providing login credentials or account details.
- Caller ID spoofing makes a scammer appear as a trusted number like a friend or the police.

Network Threats

Sniffing

The process of capturing and analyzing network traffic, especially unencrypted data, to gain sensitive information such as passwords, credit card numbers, or private messages.

Example:

- Hackers capture payment card data transmitted over an unsecured Wi-Fi network at a café.
- Someone uses a packet sniffer to read unprotected messages on a public hotspot.

Network Threats

Insider Threats

Security risks originating from employees, contractors, or trusted individuals who misuse their access privileges, either intentionally or accidentally, to harm the organization.

Example:

- A bank employee leaks sensitive customer information to a competitor or hacker.
- IT staff copying confidential files without permission.

Network Threats

Supply Chain Risks

Security vulnerabilities introduced through third-party vendors, service providers, or software dependencies, which attackers can exploit to infiltrate an organization.

Example:

- Hackers breach a fintech API provider, compromising multiple banks that rely on it.
- Installing a malicious browser extension that steals saved passwords.

Network Threats

Ransomware Spread

Malware that encrypts a victim's files or systems and demands a ransom payment for the decryption key, often spreading across networks to maximize damage.

Example:

- A payment company's shared drives are locked, halting operations until ransom is paid.
- Personal laptop is locked with a ransomware message demanding money to regain access.

Network Threats

Social Engineering Over Networks

Manipulating or deceiving individuals over digital channels (email, messages, calls) to divulge confidential information or perform actions that compromise security.

Example:

- Employees receive a phishing email pretending to be IT support, tricking them into revealing credentials.
- Receiving an SMS saying “Your package is delayed, click here” to steal personal info.

Threat Recap

- Networks face technical threats (DDoS, MITM, sniffing) that target systems and human threats (insider attacks, phishing) that exploit human behavior.
- Effective security requires both protective tools and user awareness, combining technology and training to mitigate risks.

Security Tools

Firewalls

Firewalls are security systems that monitor and control incoming and outgoing network traffic based on rules. They act as a barrier between trusted internal networks and untrusted external networks.

Types :

Packet Filtering, Stateful Inspection, Next-Gen Firewalls (NGFW):

Example:

- A bank's firewall blocks malicious SQL injection attempts targeting customer databases.
- Windows Defender Firewall stops unknown apps or programs from connecting to the internet.

Security Tools

VPNs (Virtual Private Networks)

- A VPN creates a secure, encrypted tunnel over the internet, hiding your data and IP address from attackers or eavesdroppers.
- Employees or users connect to a VPN client, which routes all internet traffic through a secure server.

Example:

- Bank staff working remotely connect via VPN to access internal systems safely.
- Students use VPN to securely access restricted university library resources from home.

Security Tools

IDS & IPS (Intrusion Detection & Prevention Systems)

IDS: Monitors network or system activity to detect suspicious patterns or intrusions.

IPS: Goes further by automatically blocking or preventing detected threats.

- IDS alerts security teams of suspicious activity; IPS can block attacks in real-time.

Example:

- An IPS blocks repeated brute-force login attempts on an online trading platform.
- Home network IDS alerts if someone tries to hack your Wi-Fi.

Security Tools

Network Segmentation

- Dividing a network into separate zones or segments to limit access and contain potential breaches.
- Critical systems (payment servers) are isolated from non-critical systems (HR), reducing risk of lateral movement in attacks.

Example:

- Payment processing servers are separated from human resources and email systems to reduce breach impact.
- Guest Wi-Fi is isolated from the main home network to protect personal devices.

Security Tools

Zero Trust Networking

- Security model based on “never trust, always verify”; every user or device must be authenticated and authorized before accessing resources.
- Continuous authentication, multi-factor verification, and strict access controls are applied to every request.

Example:

- Employees must re-authenticate with MFA to access payment or customer data systems.
- Logging into Gmail requires re-entering password and verification code each session.

Security Tools

Monitoring & Patching

- Continuous monitoring tracks activity for unusual behavior, while patching fixes software vulnerabilities before attackers exploit them.
- Organizations monitor logs, alerts, and traffic, then deploy updates and patches to systems regularly.

Example:

-Banks update routers, servers, and applications to protect against newly discovered exploits.

-Smartphone or laptop updates install patches that fix security flaws and bugs.

Practice: “How would you protect online payments on public Wi-Fi?” (Individual level)

To protect online payments on public Wi-Fi, you should:

Check the Website Security (HTTPS)

- Before entering payment details, ensure the website uses HTTPS (look for the lock icon in the browser).
- HTTPS encrypts data between your browser and the server.

Use a VPN

- Install a trusted VPN app (e.g., NordVPN, ExpressVPN) on your device.
- Connect to the VPN before accessing the payment site.
- The VPN encrypts all your internet traffic, hiding it from hackers on public Wi-Fi.

Enable Firewall

- Ensure your system firewall is active (Windows Defender Firewall or macOS firewall).
- Configure it to block unknown applications from accessing the internet while performing payments.

Practice: “How would you protect online payments on public Wi-Fi? (Individual level)

Run Antivirus / EDR

- Make sure your antivirus or endpoint security is up-to-date and running.
- Scan your device for malware before entering payment information.

Zero Trust

- Use MFA / one-time passwords (OTP), SMS codes, or authenticator apps to verify your identity for every transaction.
- Avoid Auto-Connect & Unsafe Networks

Disable automatic Wi-Fi connection to public hotspots.

- Only connect manually to trusted networks, preferably with a VPN.

Verify After Payment

- Log out from the payment site after completing the transaction.
- Check account activity to ensure no unauthorized access occurred.

Practice: Protecting Online Payments at a Digital Bank (Organization level)

Deploy Firewalls (NGFW)

- Protect the online banking servers and payment gateways.
- Block malicious traffic (SQL injections, malware, DoS attacks).
- Segment networks: payment processing, customer database, HR, marketing.

Implement VPN for Employees

- Remote staff (support, finance, IT) must connect via a corporate VPN before accessing sensitive systems.
- Encrypts all traffic between employee devices and internal servers.

Deploy IDS/IPS

- Network IPS monitors incoming payment requests for suspicious activity.
- Host-based IPS on critical servers detects and blocks brute-force login attempts or malware in real-time.
- Alerts security team to investigate potential fraud attempts.

Network Segmentation

- Isolate payment processing servers from HR/email servers.
- Use VLANs or zones in data centers to reduce lateral movement in case of a breach.

Practice: Protecting Online Payments at a Digital Bank (Organization level)

Zero Trust / MFA

- Require MFA for employees accessing payment systems or customer data.
- Enforce device compliance (antivirus active, OS updated).
- Employees only access systems necessary for their role (least privilege).

Antivirus / EDR

- Enterprise EDR installed on all servers, workstations, and employee devices.
- Detects malware, ransomware, and suspicious scripts.
- Security team isolates infected devices immediately.

Customer-side Security Advice (Optional for Training)

- Encourage customers to use VPN on public Wi-Fi.
- Ensure transactions use HTTPS.
- Enable MFA/OTP for account verification.

Learning Recap

- Networks = backbone of fintech → enable banking, trading, and global payments.
- Data flow: OSI (7 layers) and TCP/IP (practical model) show how data travels securely.
- Threats: DDoS, MITM, spoofing, sniffing, insider misuse.
- Defenses: Firewalls, VPN, IDS/IPS, segmentation, zero trust.
- Key lesson: Secure networks build trust and keep fintech systems reliable.

References

- Stallings, W. (2014). Foundations of Security: Principles and Practice. Pearson.
- Paar, C., & Pelzl, J. (2010). Understanding Cryptography. Springer.
- Gupta, R. (2022). Cybersecurity Tools. CRC Press.
- Britz, M. T. (2013). Computer Forensics and Cyber Crime. Pearson.
- NIST (2023). Cybersecurity Framework 2.0.
- ENISA (2022). Threat Landscape Report.
- Kaspersky (2023). Financial Cyberthreats Report.