1
Edge Layer

2
Gateway/Network Layer

3
Cloud Layer

4
Application Layer

5
Security Layer

INDUSTRIAL IOT ARCHITECTURE

The 5 Basic layers

EDGE LAYER

Part of the network where data processing and analysis happens close to the data source

Key Components

- Edge Devices: Physical hardware of IoT devices, e.g. sensors, actuators, and other peripherals.
- Embedded Operating System: Manages the processes on the edge device.
- Device Firmware: Software and instructions programmed onto the IoT devices.
- Edge Gateways: Devices that connect IoT devices to edge infrastructure.
- Local Edge Servers: Provide additional processing power and storage capabilities at the edge.

Benefits

- Low Latency: Reduces the time it takes for data to be processed and acted upon, crucial for applications like smart manufacturing or autonomous vehicles.
- Reduced Bandwidth Usage: Less data needs to be transmitted to the cloud, saving bandwidth and potentially costs.
- Enhanced Security: Can improve security by reducing the amount of sensitive information transmitted over the network.
- Improved Reliability: In cases where internet connectivity is unreliable, edge processing can ensure that devices continue to function.

Use Cases

- Smart Manufacturing: Edge devices can be used to monitor production lines, detect defects, and optimize processes.
- Healthcare Monitoring: Wearable devices can collect real-time health data, which can be processed at the edge to provide early warnings or enable timely intervention.
- Autonomous Vehicles: Edge computing can be used to process sensor data and control vehicle actions in real-time.
- Smart Cities: Edge devices can be used to monitor traffic flow, manage energy consumption, and improve public safety.

NETWORK LAYER

Part of the network responsible for routing data between devices and systems

Key Components

- Routers: Direct data packets between networks based on their addresses.
- Switches: Connect devices within a local area network (LAN) to enable communication.
- Firewalls: Monitor and control incoming and outgoing network traffic.
- Network Interfaces: Allow devices to connect to the network physically or wirelessly.
- Protocols (e.g., IP, TCP): Define rules for data transmission and reception.

Benefits

- Efficient Routing: Ensures data packets take the optimal path to reach their destination.
- Traffic Management: Balances data flow to prevent congestion and improve performance.
- Security Controls: Filters traffic to protect the network from malicious activities.
- Reliable Communication: Maintains connectivity between devices even under heavy loads.

Use Cases

- Internet Communication: Enables seamless connectivity for browsing, streaming, and file transfers.
- Enterprise Networks: Supports data flow within office environments, connecting computers and servers.
- Remote Access: Facilitates VPN connections for secure remote work.
- Data Centers: Manages high-volume data traffic efficiently and securely.

CLOUD LAYER

Part of the network where data storage, processing, and services are hosted remotely

Key Components

- Virtual Machines: Simulate physical computers, running applications and services.
- Storage Systems: Store large amounts of data, accessible from anywhere.
- APIs and Microservices: Enable flexible, modular application development.
- Load Balancers: Distribute workload across multiple servers.
- Data Analytics Tools: Process and analyze data for insights.

Benefits

- Scalability: Resources can be adjusted according to demand.
- Cost Efficiency: Reduces hardware maintenance and operational costs.
- Data Backup and Recovery: Ensures data is securely stored and can be recovered if needed.
- Global Accessibility: Access data and applications from any internet-connected device.

Use Cases

- Web Hosting: Deploy websites and web applications on cloud servers.
- Data Analysis: Perform large-scale computations and analytics on cloud platforms.
- Collaboration Tools: Enable teamwork through shared documents and data.
- Disaster Recovery: Securely back up data and ensure business continuity.

APPLICATION LAYER

Part of the network that interacts directly with end-users through software and interfaces

Key Components

- User Interfaces (UIs): The visual elements that users interact with.
- API Gateways: Allow communication between client applications and backend services.
- Web Servers: Host websites and deliver content to users.
- Data Processing Applications: Handle tasks such as data entry, analysis, and reporting.
- Authentication Services: Verify user identity and control access.

Benefits

- User-Friendliness: Makes complex tasks accessible through intuitive interfaces.
- Customization: Tailors applications to meet specific user or business needs.
- Seamless Integration: Connects with other systems and databases effortlessly.
- Enhanced Accessibility: Allows remote and mobile access to applications.

Use Cases

- E-commerce Platforms: Facilitate online shopping and payment processing.
- Social Media Applications: Enable communication and content sharing.
- Productivity Software: Supports tasks like document creation and project management.
- Business Intelligence: Visualize data and generate insights.

SECURITY LAYER

Part of the network dedicated to protecting data, applications, and systems from threats

Key Components

- Encryption Protocols: Protect data during transmission and storage.
- Authentication Mechanisms: Verify user identities to prevent unauthorized access.
- Intrusion Detection Systems (IDS): Monitor for suspicious activities.
- Firewalls and Anti-malware: Block malicious traffic and software.
- Access Control Systems: Manage user permissions and data access.

Benefits

- Data Integrity: Ensures that data is not altered or corrupted.
- Confidentiality: Protects sensitive information from unauthorized access.
- Availability: Keeps systems running and accessible even during attacks.
- Threat Mitigation: Detects and responds to security breaches quickly.

Use Cases

- Financial Transactions: Secure online payments and banking.
- Healthcare Systems: Protect patient data and maintain compliance.
- Enterprise IT Security: Safeguard corporate networks and databases.
- Personal Device Protection: Guard against malware and phishing attacks.

GRAPHICAL REPRESENTATION