MODULE 3 - IOE

RFID (Radio Frequency Identification)

- **Wireless technology** uses radio waves to identify and track objects.
- **Components:**
    - **RFID Tag** → Has Microchip + antenna
    - **RFID Reader** → Sends signals and receives data.
    - **Backend System** → Processes and collects data

RFID supports the **identification layer** of IoT.

Functions: (acronym - DACU)

- **Unique Identification** – Each RFID tag has a unique ID (like a digital fingerprint).
- **Data Collection** – Provides real-time info on location, condition, and movement.
- **Connectivity** – Works with IoT gateways, cloud, and analytics.
- **Automation** – Enables smart environments (factories, logistics, healthcare, homes)

Types of RFID

1. **Passive RFID** – No battery, powered by reader's signal.
    - Uses: inventory, retail, libraries.
2. **Active RFID** – Has its own battery, works at long ranges.
    - Uses: vehicle tracking, supply chain.
3. **Semi-Passive RFID** – Battery powers chip but needs reader for communication.
    - Uses: cold-chain monitoring.

4. Applications of RFID in IoT

❖ **Supply Chain & Logistics:**

- Real-time tracking of goods.
- Automated warehouse management.

❖ **Healthcare:**

- Patient identification and monitoring.
- Tracking medical equipment and medicines.

❖ **Smart Cities:**

- Vehicle identification at toll gates.
- Waste management tracking.

(dont learn applications , add acc to you from above types also)

Advantages of RFID

- **Automation** – Less manual work, fewer errors.
- **Accuracy** – Precise tracking.
- **Security** – Encryption & authentication support.
- **Efficiency** – Hundreds of tags read in seconds.

Disadvantages of RFID

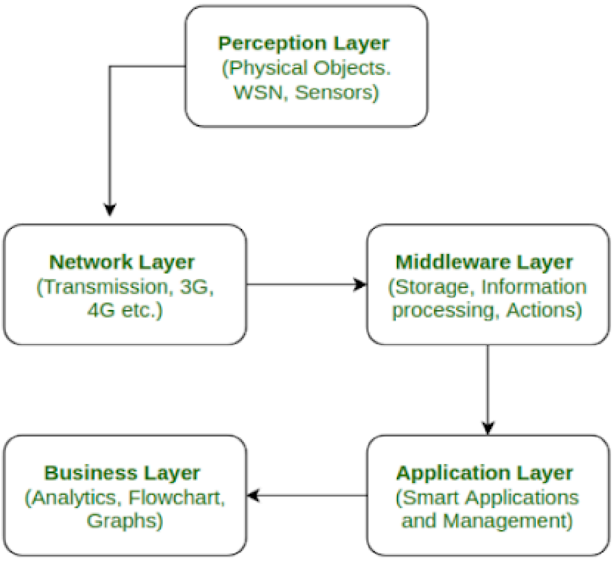
- **Security risk** – Can be intercepted even if encrypted.
- **Privacy concerns** – Data may be misused.
- **High cost** – Active RFID tags are expensive (due to battery).

5 Layer Architecture of IoT with RFID / IOT SYSTEM ARCHITECTURE WITH RFID (exactly same as mod 1 answer)

1. **Perception Layer**
   - First layer of IoT.
   - Uses sensors and actuators to collect information (temperature, moisture, sound, intruder, etc.).
   - Passes collected data to the next layer.
   - **RFID Technologies used:**
     1. RFID systems (tags)
     2. GPS modules
     3. Cameras
     4. Barcodes
2. **Network Layer (Communication Layer)**
   - Acts as a connection between perception and middleware layer.
   - Transfers data using **RFID** technologies like Wi-Fi, 3G, 4G, infrared, etc.
   - Ensures **secure communication** and keeps **data confidential.**
3. **Middleware Layer**
   - Has features like **storage, processing**, and **computation.**
   - Stores data and provides it to the correct device based on address or name.
   - Can take decisions by performing calculations on sensor data.
4. **Application Layer**
   - Manages all application processes based on information obtained from the middleware layer.

- Examples: sending emails, alarms, smartwatches, smart agriculture, smart homes, etc.
- This layer has **two sub-layers**:
    1. **Data Management Sub-layer:** Cleans, restructures, and integrates raw data. Handles redundancy in data.
    2. **Application Service Sub-layer :** Converts processed data into meaningful information

5. **Business Layer**
    - Focuses on how the device and technology is being delivered to its consumers.
    - Includes analysis, flowcharts, graphs, and ways to improve the system.



Virtualization

- Converts **physical hardware resources** into **virtual form.**
- It offers **efficiency, flexibility,** and **scalability.**

1. Types of Virtualization

a) Server Virtualization

- Involves partitioning a single physical server into multiple **virtual servers (VMs)**.
- Each VM runs its own operating system and applications independently.
- Enables better utilization of hardware and reduces the number of physical servers required.

b) Storage Virtualization

- Combines physical storage from multiple devices into a **single, unified storage system**.
- Centrally managed for efficiency.
- Improves storage utilization, flexibility, and data management.

c) Network Virtualization

- Creates **virtual networks** that operate independently of the physical network infrastructure.
- Multiple virtual networks can run on the same hardware.
- Enhances network agility, security, and scalability.

Benefits of Virtualization

- **Cost Reduction**: Less physical hardware, lower cost, and saves energy.
- **Scalability & Flexibility**: Can scale resources up or down based on demand.
- **Disaster Recovery**: Easy backup and restoration.
- **Simplified Management**: Automation reduces manual intervention and human errors.
- **Security**: Advanced hypervisor-level security features give protection.

IOT ANALYTICS

1. Data Collection

IoT data comes from:

- **Sensors & Actuators** – collect physical data like temperature, pressure, motion, humidity.
- **Edge Devices** – gather raw data from many sensors.
- **Smart Devices** – create logs, updates, and status reports.

Key points while collecting data:

- **Volume & Velocity** – large, continuous and real - time data.
- **Variety** – different types of data: Structured (numbers), Semi-structured (logs), Unstructured (audio, video)

- **Connectivity** – Data transmitted using protocols like HTTP or 5G.
- **Security & Privacy** – use encryption and access control.

2. Data Transmission & Storage

After collection, data must be sent and stored properly.

- **Edge Processing** – preprocessing at the edge[directly on device before sending it to network] (filter, compress) to reduce network usage.
- **Cloud Storage** – store large volumes of data; scalable (eg, write any anyone) AWS IoT, Google Cloud IoT.
- **Data Lakes & Warehouses** – organize raw IoT data for analysis.

3. Data Processing & Analytics

Three levels of IoT analytics:

1. **Descriptive Analytics (What happened?)**
   → Example: sales have been steady in the past year.
2. **Predictive Analytics (What will happen?)**
   → Example: Sales are expected to grow by 15% next quarter.
3. **Prescriptive Analytics (What should be done?)**
   → Example: Launch a targeted marketing campaign next month.

Techniques used:

- **Machine Learning Models** – anomaly detection, forecasting, classification.
- **Big Data Tools** – Hadoop, NoSQL

4. Deployment of IoT Analytics

After building models, they must be used in real IoT systems.

- **Model Deployment** – use ML models with IoT platforms using TensorFlow Lite, Azure ML.
- **Edge Deployment** – models deployed at the edge for fast decisions (e.g., autonomous cars).
- **Scalability** – cloud setups with Kubernetes and Docker.

5. Operationalization (Making It Work Continuously)

To ensure continuous value: **(remember headings, write on your inside ka details)**

- **Monitoring & Feedback** – keep checking system performance and improve it based on feedback.
- **Model Retraining** – keep updating models as new data changes (data drift).
- **Automation** – the devices can respond automatically (e.g., shut down a machine when overheating).
- **Visualization & Dashboards** – insights shown using tools like Power BI, etc

- **Security & Compliance** – continuous encryption and authentication.

6. Challenges in IoT Analytics

1. **Handling massive data** volumes from various sources.
2. **Privacy** and **security risks** - sensitive data leaks and misuse.
3. **Cost management** - can be expensive

DATA CENTERS

- A data centre is a **specialised facility** that provides the necessary **services** and **infrastructure** to **host** the world's largest **computing environments.**
- Its main goal is to ensure **continuous, reliable operation** for businesses that depend on IT services.

Key Factors in Data Center Deployment

1. Location

- Should be in areas with **low natural disaster risk.**
- Must **avoid high-traffic zones** (airports, malls).
- Should not be near **sensitive sites** like refineries or nuclear plants.

2. Security

- Strict **physical access control**.
- **Authorized staff** only; constant monitoring.
- Uses **CCTV, biometrics, and 24/7 surveillance**.

3. Electrical Power

- Needs a **stable** and **continuous power suppl**y.
- Backup systems include **batteries and generators.**

4. Environmental Controls

- Maintains proper **temperature** and **humidity.**
- Uses **HVAC (Heating, Ventilation, Air Conditioning**) systems.
- Has advanced **fire detection systems.**

5. Network Infrastructure

- Requires **redundant, scalable connections.**
- Must ensure **high bandwidth, low latency,** and **fault tolerance.**

Global Data Centers

- There are **over 3,000 data centers** worldwide.
- Many offer **IaaS** (Infrastructure as a Service), providing computing power, storage, and networking.

Big Data Security in Cloud Computing

- Big Data and Cloud Computing are important IT technologies, but the **open nature of the cloud** and **limited user control** make **security and privacy major concerns** as the **data grows**.

How Cloud Ensures Security

- Data is stored and processed on **remote cloud servers**.
- Trust is built through **third-party security services** and **strong protection measures.**
- A **Service Level Agreement (SLA)** defines what security the provider must guarantee. It helps increase trust between customers and cloud providers.
- **Role of SLA:** The SLA is a contract defining:
  - Security responsibilities
  - Protection level
  - Data privacy and availability
  - Scalability and performance

Levels of Data Protection

- **Basic users:** Use logical access control (username/password, permissions).
- **Sensitive data:** Needs stronger protection, like:
  - Encryption
  - Data masking
  - Logging/auditing
  - Intrusion detection systems (IDS)

Security Technologies

- Encryption
- Registry and activity monitoring
- Intrusion detection
- Big data analytics to identify attacks and sophisticated threats

Challenges in Big Data Security

1. Protecting huge datasets from advanced attackers.
2. Guaranteeing secure deletion of massive stored data.

3. Lack of standard rules for auditing and reporting big data.