

UNIT 1

Introduction to IoT

(8 Hours) — Internet of Things (CACS460)

⚠ Please Note

*These notes were prepared quickly and **may contain errors or omissions**. Please cross-check important definitions, formulas, code and diagrams with your textbook, class notes and the official TU syllabus before relying on them in exams.*

1.1 Definition and Characteristics of IoT

The **Internet of Things (IoT)** is a network of physical objects — “things” — that are embedded with sensors, software, processors and network connectivity so that they can **collect, exchange and act on data** over the Internet with little or no human intervention. A thing can be a temperature sensor, a smart bulb, a tractor, a pacemaker or a delivery truck.

Note: A commonly quoted textbook definition (Arshdeep Bahga & Vijay Madisetti): “A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual ‘things’ have identities, physical attributes and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network.”

Characteristics of IoT

Characteristic	Meaning
Dynamic & self-adapting	Devices adapt to changing context (e.g., a camera switches to night mode when light drops).
Self-configuring	Devices set up themselves and join the network with minimal manual setup (plug-and-play, firmware updates).
Interoperable communication	Devices from different vendors talk using standard protocols (MQTT, CoAP, HTTP, Zigbee).
Unique identity	Every thing has an identifier — IP address, MAC address, RFID tag or URI.
Integrated into the information network	Things share data with other devices and with back-end systems and can be discovered and queried.
Intelligence	Analytics and ML turn raw sensor data into decisions.
Connectivity	Network access and compatibility between heterogeneous devices.
Scalability & heterogeneity	Billions of devices with different hardware, OS and networks must coexist.
Safety & security	Data and physical safety must be protected because IoT devices act in the real world.

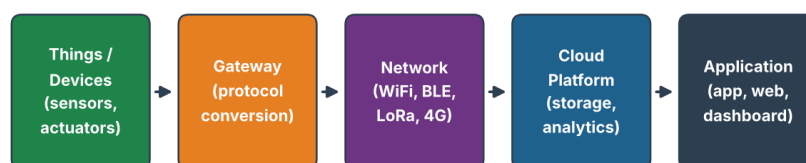
1.2 Physical Design of IoT

The physical design describes the **things (devices)** and the **protocols** used to connect them.

Things in IoT

An IoT device usually has: sensors, actuators, a processor/microcontroller, memory, a power source and a communication interface (WiFi, Bluetooth, Ethernet, Zigbee, LoRa, cellular). Devices may be *monitoring* devices (only sense) or *controlling* devices (sense and actuate). Examples: Arduino, Raspberry Pi, ESP8266/ESP32, smart thermostats, wearables.

Generic IoT System Architecture



Data flows left → right; commands flow back right → left

Figure 1.1 — Generic IoT system architecture

IoT Protocols (Physical Design View)

Layer	Protocols	Purpose
Link layer	802.3 Ethernet, 802.11 WiFi, 802.15.4 (Zigbee, 6LoWPAN), 802.16 WiMAX, 2G/3G/4G/5G	Moves frames between directly connected devices.
Network / Internet layer	IPv4, IPv6, 6LoWPAN	Addressing and routing of packets; 6LoWPAN compresses IPv6 headers for low-power links.
Transport layer	TCP, UDP	TCP: reliable, connection-oriented. UDP: fast, connectionless, low overhead.
Application layer	HTTP, CoAP, WebSocket, MQTT, XMPP, DDS, AMQP	Defines how data/messages are exchanged between applications.

1.3 Logical Design of IoT

Logical design is an **abstract view** of the system — the functional blocks, communication model and APIs — without going into hardware detail.

Functional Blocks of an IoT System

- **Device:** sensing, actuation, monitoring and control functions.
- **Communication:** handles protocols and data transfer between device and network.
- **Services:** device monitoring, control, data publishing and device discovery.
- **Management:** governs the system (configuration, status, diagnostics).
- **Security:** authentication, authorization, message and content integrity, data security.
- **Application:** interface (web/mobile dashboard) through which users view status and control the system.

Communication Models

Model	How it works	Example
Request–Response	Client sends a request; server replies. Stateless; each pair is independent.	HTTP REST calls to read a sensor value.
Publish–Subscribe	Publishers send messages to topics on a broker; subscribers of that topic receive them.	MQTT temperature topic.
Push–Pull	Producers push data into a queue; consumers pull when ready. Decouples speeds.	Sensor data queue consumed by analytics job.
Exclusive Pair	Persistent, full-duplex connection between client and server until closed.	WebSocket, MQTT session.

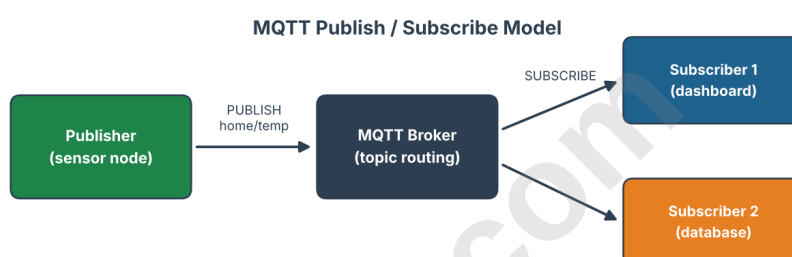


Figure 1.2 — Publish–Subscribe model (MQTT)

Communication APIs

- **REST-based API:** uses HTTP methods (GET, POST, PUT, DELETE) on resources identified by URIs; follows request–response model; stateless.
- **WebSocket-based API:** full-duplex, persistent connection; lower overhead, suited to real-time data.

1.4 IoT Enabled Technologies

Technology	Role in IoT
Wireless Sensor Networks (WSN)	Distributed sensor nodes that cooperatively monitor environment and relay data to a sink/gateway.
Cloud Computing	Elastic storage, processing and hosting for IoT data and applications (IaaS, PaaS, SaaS).
Big Data Analytics	Processes the huge volume, velocity and variety of sensor data to extract insight.
Communication Protocols	Standards that let devices exchange data reliably and efficiently.
Embedded Systems	Microcontroller/microprocessor-based hardware that runs the device firmware.

1.5 IoT and M2M

Machine-to-Machine (M2M) means direct communication between devices, usually over cellular or wired networks, typically without human involvement. **IoT** extends M2M by connecting devices to the Internet and cloud services and building applications on the collected data.

Basis	IoT	M2M
Communication	Devices communicate via Internet (IP) protocols and cloud	Point-to-point, often non-IP and proprietary
Scope	Broad, many-to-many, application-centric	Narrow, device-to-device or device-to-server
Network	Wi-Fi, BLE, LoRa, cellular, etc.	Mostly cellular, wired, PSTN
Data use	Analytics, big data, cloud services	Mainly remote monitoring and control
Interoperability	Standard open protocols and APIs	Vendor-specific solutions
Software	Rich application layer, web/mobile apps	Limited, device-specific software
Example	Smart home controlled through a phone app	ATM talking to bank server; vending machine telemetry

Note: In M2M, systems are usually vertical silos; IoT aims for horizontal, interoperable platforms. Many books describe M2M as a subset or enabling technology of IoT.

1.6 Domain-Specific IoTs

Home Automation

- **Smart lighting:** bulbs adjust brightness/colour by occupancy, time or ambient light, saving energy.
- **Smart appliances:** washers, fridges and ACs that can be monitored and controlled remotely.
- **Intrusion detection:** door/window sensors, PIR motion sensors and cameras raise alerts on a phone.
- **Smart thermostats and smoke/gas detectors:** automatic climate control and safety alarms.

Cities

- **Smart parking:** sensors detect free slots and guide drivers via apps.

- **Smart lighting:** streetlights dim when roads are empty.
- **Smart roads and traffic:** congestion monitoring, adaptive signals, accident and pothole detection.
- **Surveillance and waste management:** cameras for safety; fill-level sensors in bins optimise collection routes.

Environment

- **Weather monitoring:** temperature, humidity, pressure, rainfall, wind stations.
- **Air and noise pollution:** gas and particulate sensors report AQI in real time.
- **Forest-fire detection:** temperature/smoke sensors in forests for early warning.
- **River-flood detection:** water-level and flow sensors send flood alerts (important in Nepal's river basins).

Energy

- **Smart grids:** two-way flow of power and information; real-time demand-response.
- **Smart meters:** automatic meter reading and time-based billing.
- **Renewable monitoring:** solar panel and micro-hydro performance tracking and prediction.

Retail

- **Inventory management:** RFID/NFC tags track stock on shelves automatically.
- **Smart payments:** contactless and wallet payments.
- **Smart vending machines and shelves:** monitor stock and customer behaviour.

Logistics

- **Route generation and scheduling:** GPS and traffic data pick optimal routes.
- **Fleet tracking:** real-time vehicle location and driver behaviour.
- **Shipment monitoring:** temperature/humidity/shock sensors in cold chain goods.
- **Remote vehicle diagnostics:** predictive maintenance.

Agriculture

- **Smart irrigation:** soil-moisture sensors trigger pumps only when needed.

- **Crop and greenhouse monitoring:** temperature, humidity, light, CO₂ control.
- **Livestock tracking:** wearable tags monitor animal health and location.
- **Drones:** field imaging for crop health and pesticide spraying.

Industry

- **Machine diagnosis and predictive maintenance:** vibration/temperature data predict failures before they occur.
- **Indoor air-quality and safety monitoring:** detects hazardous gas leaks.
- **Industrial IoT (IIoT):** connected production lines for efficiency and quality control.

Health and Lifestyle

- **Wearables:** fitness bands and smartwatches track steps, heart rate, sleep.
- **Remote patient monitoring:** glucose, blood-pressure, ECG sent to doctors.
- **Smart medicine dispensers and elderly care:** reminders, fall detection.

1.7 Tour Colleges (Syllabus Item)

The syllabus lists “Tour Colleges” as an activity item. This is a practical/field activity rather than theory: students visit colleges or labs to observe IoT or embedded-systems setups and usually submit a short visit report. Check with your course teacher for the exact requirement.

Suggested visit-report outline

1. Name and place of institution/lab visited and date.
2. IoT or embedded devices observed (sensors, boards, gateways).
3. Applications or projects demonstrated.
4. What you learned and how it relates to Unit 1–6 topics.
5. Photographs (if permitted) and signatures/endorsement.

Key Takeaways

- ✓ IoT = sensing + connectivity + cloud + analytics + action, with unique identities for things.
- ✓ Physical design = devices and protocols; logical design = functional blocks, communication models and APIs.
- ✓ Four communication models: request–response, publish–subscribe, push–pull, exclusive pair.
- ✓ M2M is direct device communication, IoT is its Internet-scale, cloud-based extension.
- ✓ Know domain examples: home, city, environment, energy, retail, logistics, agriculture, industry, health.

— *End of Unit 1* —

bcalink.com