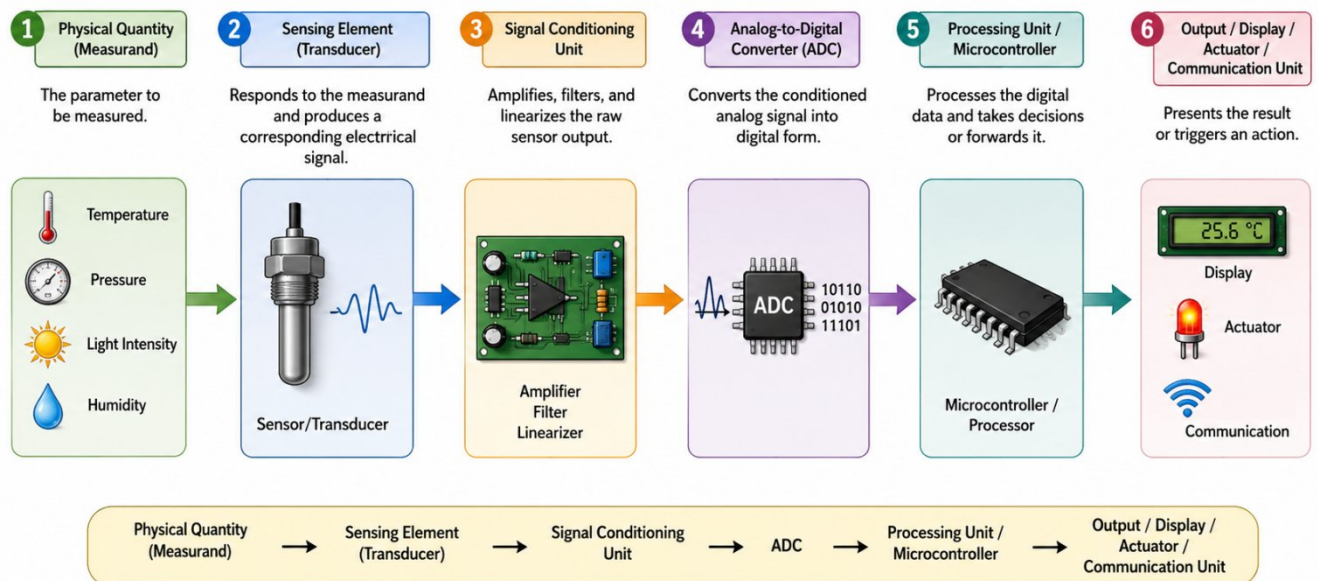


Introduction to Sensors

A sensor is a device that detects and responds to a physical, chemical, or biological stimulus (such as heat, light, pressure, motion, or a chemical concentration) from its environment and converts it into a measurable output signal, usually an electrical signal, that can be read by an observer or by an instrument. A sensor is closely related to a transducer, which is a device that converts energy from one form into another; in practice, a sensor is a special class of transducer that converts a physical quantity into an electrical quantity.

Basic Block Diagram of a Sensing System

A typical sensor-based measurement system converts a physical quantity into useful information.



Basic Block Diagram of a Sensing System

A typical sensor-based measurement system consists of the following stages:

- Physical Quantity (Measurand) – the parameter to be measured, e.g., temperature, pressure, light intensity.
- Sensing Element – the transducer that responds to the measurand and produces a corresponding electrical signal.
- Signal Conditioning Unit – amplifies, filters, and linearizes the raw sensor output.
- Analog-to-Digital Converter (ADC) – converts the conditioned analog signal into digital form.
- Processing Unit / Microcontroller – processes the digital data and takes decisions or forwards it.
- Output / Display / Actuator / Communication Unit – presents the result or triggers an action.

Characteristics / Performance Parameters of Sensors

- Accuracy – closeness of the measured value to the true value.
- Precision – degree of repeatability/consistency of successive measurements.
- Sensitivity – ratio of change in output to change in input (slope of the calibration curve).
- Resolution – smallest change in input that produces a detectable change in output.

- Linearity – how closely the calibration curve approximates a straight line.
- Range/Span – the minimum and maximum values of the measurand that the sensor can measure.
- Response Time – the time taken by the sensor to reach a specified percentage (e.g., 90%) of its final output after a step change in input.
- Hysteresis – difference in output for the same input when approached from increasing and decreasing directions.
- Drift – gradual change in output over time under constant input conditions.
- Repeatability and Reliability – ability to give the same output for repeated identical inputs under the same conditions.

Classification of Sensors

(a) Based on Power Requirement

- Active Sensors – require an external power/excitation source to operate (e.g., RFID reader, RADAR, ultrasonic sensor).
- Passive Sensors – generate an output signal directly from the stimulus without external excitation (e.g., PIR sensor, thermocouple, photodiode in photovoltaic mode).

(b) Based on Output Signal

- Analog Sensors – produce a continuous output signal proportional to the measurand (e.g., LM35 temperature sensor).
- Digital Sensors – produce a discrete/binary or digitally coded output (e.g., DHT11 humidity sensor).

(c) Based on Contact

- Contact Sensors – require physical contact with the object being measured (e.g., strain gauge, thermocouple).
- Non-Contact Sensors – measure without physical contact (e.g., infrared thermometer, PIR sensor, ultrasonic sensor).

(d) Based on Quantity Measured

- Physical sensors – temperature, pressure, motion, light, proximity.
- Chemical sensors – gas sensors, pH sensors.
- Biological/Biomedical sensors – ECG, EEG, glucose sensors.

Role of Sensors in IoT and Automation

Sensors form the perception layer of any IoT or automation system. They continuously acquire real-world data, which is then transmitted through communication protocols to gateways and cloud platforms for storage, analytics, visualization, and decision-making. The processed information may subsequently be used to drive actuators, thereby closing the sensor–controller–actuator feedback loop that is fundamental to smart systems such as smart homes, smart healthcare, smart agriculture, smart cities, and Industry 4.0 automation.

Applications

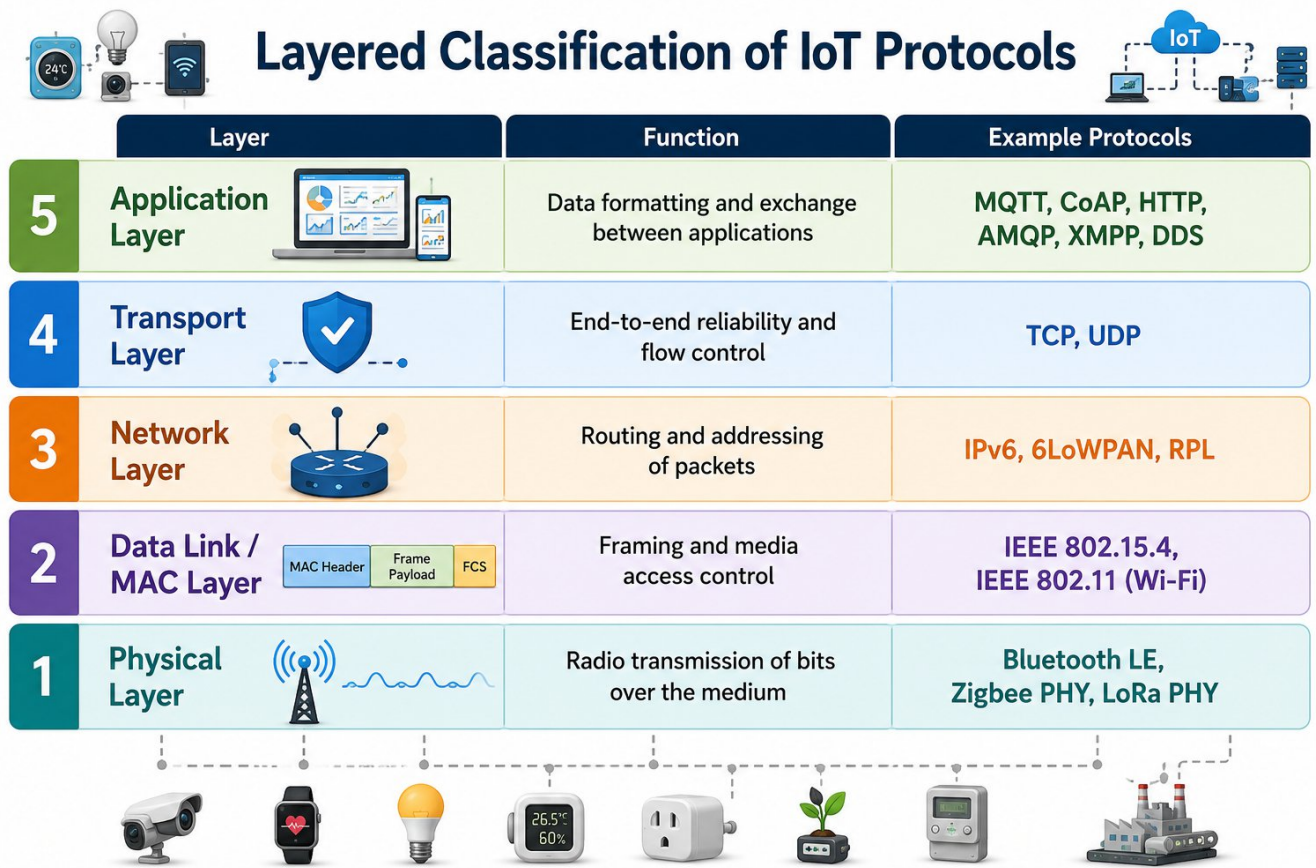
- Industrial process monitoring and control
- Environmental and pollution monitoring
- Healthcare and patient monitoring

- Home and building automation
- Automotive safety systems (airbags, ABS, parking sensors)
- Agriculture (soil moisture, weather monitoring)
- Security and surveillance systems

Protocols in IoT

Need for IoT Protocols

IoT devices are typically resource-constrained in terms of power, memory, processing capability, and bandwidth. Standard internet protocols such as TCP/IP and HTTP were designed for resource-rich devices and are often too heavy for such constrained nodes. IoT protocols are therefore designed to provide lightweight, low-power, reliable, and secure communication between sensors, gateways, and cloud platforms, enabling interoperability between heterogeneous devices.



Layered Classification of IoT Protocols

Layer	Function	Example Protocols
Application Layer	Data formatting and exchange between applications	MQTT, CoAP, HTTP, AMQP, XMPP, DDS
Transport Layer	End-to-end reliability and flow control	TCP, UDP
Network Layer	Routing and addressing of packets	IPv6, 6LoWPAN, RPL
Data Link / MAC Layer	Framing and media access control	IEEE 802.15.4, IEEE 802.11 (Wi-

		Fi)
Physical Layer	Radio transmission of bits over the medium	Bluetooth LE, Zigbee PHY, LoRa PHY

Key Application-Layer Protocols

MQTT (Message Queuing Telemetry Transport)

A lightweight publish–subscribe protocol running over TCP. It uses a central broker to relay messages between publishers and subscribers organized into topics. It supports three Quality of Service (QoS) levels (0 – at most once, 1 – at least once, 2 – exactly once) and is widely used for telemetry data from constrained sensor nodes because of its low bandwidth and power overhead.

CoAP (Constrained Application Protocol)

A lightweight request–response protocol modeled on REST/HTTP but designed to run over UDP for constrained networks. It supports methods such as GET, POST, PUT, and DELETE and includes an observe feature for asynchronous notifications, making it suitable for machine-to-machine (M2M) communication.

HTTP/HTTPS

The standard request–response web protocol; heavier than MQTT/CoAP due to larger header overhead, but widely supported and used when IoT devices communicate directly with web servers or REST APIs.

AMQP (Advanced Message Queuing Protocol)

A message-oriented middleware protocol offering reliable queuing, routing, and transactional messaging; commonly used in enterprise-grade IoT and cloud messaging systems.

Short-Range Communication Protocols

Protocol	Frequency/Range	Data Rate	Power	Typical Use
Bluetooth / BLE	2.4 GHz, ~10-100 m	1-3 Mbps	Low	Wearables, mobile sensors
Zigbee (IEEE 802.15.4)	2.4 GHz, ~10-100 m	250 kbps	Very Low	Home automation, mesh networks
Wi-Fi (IEEE 802.11)	2.4/5 GHz, ~50 m	Up to Gbps	High	Smart home hubs, cameras
Z-Wave	Sub-GHz, ~30 m	9.6-100 kbps	Low	Home automation
NFC	13.56 MHz, <10 cm	424 kbps	Very Low	Payments, access cards
RFID	LF/HF/UHF, cm to 10 m	Varies	Passive/Active	Asset & inventory tracking

Long-Range (LPWAN) Protocols

- LoRaWAN – long range (up to 15 km), very low power, low data rate; used in smart agriculture and utility metering.
- Sigfox – ultra-narrowband, long range, extremely low power, low data rate; used for simple telemetry.

- NB-IoT / LTE-M – cellular-based LPWAN technologies offering wide coverage and moderate power consumption, suitable for smart city and industrial applications.
- 5G – provides high bandwidth, ultra-low latency, and massive device connectivity for advanced IoT applications.

Routing and Network Layer Protocols

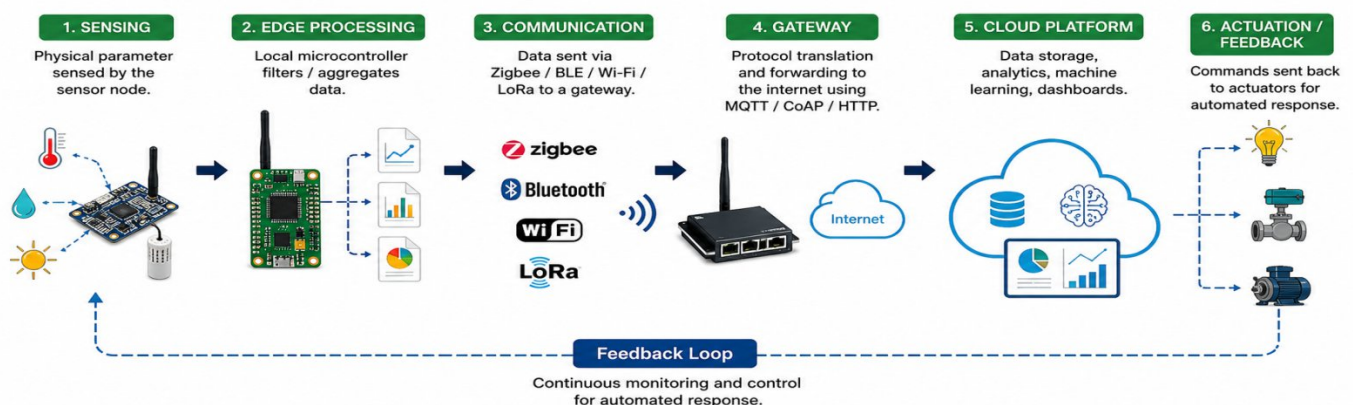
- 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) – enables IPv6 packet transmission over low-power, low-bandwidth networks such as IEEE 802.15.4.
- RPL (Routing Protocol for Low-Power and Lossy Networks) – a distance-vector routing protocol designed for constrained networks, forming a Destination-Oriented Directed Acyclic Graph (DODAG).

Sensors in IoT

Role of Sensors in the IoT Architecture

In a typical IoT architecture, sensors reside at the Perception/Edge Layer. They acquire raw physical data, which is pre-processed at the edge, transmitted via the Network Layer (using protocols discussed above) to gateways, and finally delivered to the Cloud/Application Layer for storage, analytics, and visualization. Insights generated may trigger actuators to complete the control loop.

Typical IoT Sensor Data Pipeline



Typical IoT Sensor Data Pipeline

- Sensing – physical parameter sensed by the sensor node.
- Edge Processing – local microcontroller filters/aggregates data.
- Communication – data sent via Zigbee/BLE/Wi-Fi/LoRa to a gateway.
- Gateway – protocol translation and forwarding to the internet using MQTT/CoAP/HTTP.
- Cloud Platform – data storage, analytics, machine learning, dashboards.
- Actuation/Feedback – commands sent back to actuators for automated response.

Common Categories of Sensors Used in IoT Systems

Category	Examples	Typical IoT Application
Temperature/Humidity	LM35, DHT11/22, thermocouple	HVAC, smart agriculture, cold-chain

		monitoring
Proximity/Distance	Ultrasonic (HC-SR04), IR sensor	Robotics, parking assist, level sensing
Pressure	Piezoresistive, capacitive pressure sensor	Industrial process control, tyre pressure monitoring
Light	LDR, photodiode	Smart lighting, ambient monitoring
Gas/Chemical	MQ series, electrochemical sensors	Air quality, leak detection, safety monitoring
Motion/Position	Accelerometer, gyroscope, PIR	Wearables, security, gesture control
Level	Float switch, ultrasonic level sensor	Water tank monitoring, industrial silos
Biometric/Medical	ECG, SpO2, glucose sensor	Remote patient monitoring, wearable health

IoT Application Domains Driven by Sensors

- Smart Home – occupancy, temperature, smoke, and door/window sensors for automation and security.
- Smart Agriculture – soil moisture, humidity, and weather sensors for precision irrigation.
- Smart City – traffic, parking, waste-level, and streetlight sensors for urban management.
- Industrial IoT (IIoT) – vibration, temperature, and pressure sensors for predictive maintenance.
- Healthcare IoT (IoMT) – wearable biomedical sensors for continuous remote monitoring.
- Smart Grid – current, voltage, and energy sensors for load and fault monitoring.

Challenges in IoT Sensor Deployment

- Power constraints and limited battery life of sensor nodes
- Scalability of large sensor networks
- Interoperability among heterogeneous sensors and protocols
- Data security and privacy
- Sensor calibration, drift, and maintenance
- Latency and bandwidth limitations in real-time applications