

The Internet of Things (IoT)

Concept, Key Components and Features

1 Concept

Meaning

The **Internet of Things (IoT)** connects physical objects equipped with sensors and/or actuators, computing capability and network interfaces. These objects exchange data with other devices or applications to support monitoring, decisions and control.

Core idea: Link the physical world with digital systems. A sensor measures a condition; software interprets the data; a person or an automated system responds.

2 Major / Key Components

These components are grouped by function.

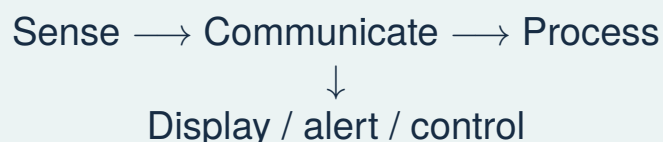
Component	Role in an IoT system
1. Sensors and actuators	Sensors measure conditions such as temperature, light or motion. Actuators produce physical actions, such as switching equipment or moving a motor.
2. Embedded controller	A processor or microcontroller runs software, handles readings and controls communication or actions.
3. Connectivity	Carries data and commands over wired or wireless networks, such as Ethernet, Wi-Fi or cellular networks.
4. Gateway / edge device	Where needed, connects local devices to other networks, translates protocols or processes data nearby.
5. Data processing and storage	Stores and analyses readings using rules or algorithms, on the device, at the edge or in the cloud.
6. Application / user interface	A dashboard or app displays information, provides alerts and allows authorised monitoring or control.

Essential distinction: Gateways and cloud services are not compulsory in every deployment; some functions operate locally.

3 Major Features

1. **Connectivity and data exchange.** Devices exchange readings and commands through networks.
2. **Physical-world interaction.** Sensors capture conditions; actuators enable physical responses. A device need not contain both.
3. **Device identification.** Identifiers associate readings, commands and management actions with the correct device.
4. **Automation and data-driven operation.** Rules or algorithms trigger actions with limited routine human intervention. Artificial intelligence is optional.
5. **Remote monitoring and control.** Authorised users observe device status and, where supported, issue commands from another location.
6. **Timely updates.** Updates may be continuous, periodic or event-triggered. Real-time performance depends on system design.
7. **Heterogeneity and interoperability.** Different devices and software can cooperate through compatible protocols and data formats; compatibility is not automatic.
8. **Scalability and manageability.** Suitable design supports growing device numbers, configuration and updates, within capacity limits.

Basic information flow



In a control system, an actuator changes a physical condition; sensing the result completes a feedback loop.

Security and privacy: requirements throughout

Device authentication, access control, data protection and secure updates must be designed into the system. Personal-data collection and access also need controls; connectivity does not itself provide security.