

Prepared by Dr. Wesam Ahmed

IT402
Internet of Things

Lecture 2



Introduction to the Internet of Things (IoT)-Part2

Lecture 2

IT402

Internet of Things

Prepared by
Dr. Wesam Ahmed

02

Learning Objectives:

- 1.1** Recognize disadvantages in IoT implementation
- 1.2** Define IoT Characteristics
- 1.3** Identify Industrial IoT use case

02

Disadvantages of IoT

- **Network security:** IoT creates an ecosystem of **connected devices communicating over networks** which leave users exposed to various kinds of security attacks. Example : If a hacker breaks into a smart home's connected light bulb, they could potentially access the home's Wi-Fi network and steal personal information.
- **Flexibility:** IoT systems are flexible in integrating easily with each other, which **may cause conflicts between** different vendors or locked systems. Example: A smart fridge from **one company** might not communicate properly with a **smart oven** from another if they use **different communication standards**.

02

Disadvantages of IoT

Complexity: IoT systems are complicated in terms of design, deployment, and maintenance and IoT often uses multiple technologies and a large set of new enabling technologies. Example: In a smart factory, hundreds of sensors and machines must communicate in real-time. Managing updates or diagnosing issues across that network is complex and requires specialized expertise.

Unemployment: The wide-use of IoT will result in a significant loss of mundane jobs and IoT will have a devastating impact on the employment prospects of less-educated workers. Example: A smart warehouse using IoT-enabled robots to track, pick, and ship items might eliminate many human labor roles previously required for these tasks.

02

Disadvantages of IoT

Issue	Description	Example
Network Security	Devices connected to networks increase vulnerability to cyberattacks.	Hacked smart camera exposes private data.
Flexibility	Different systems may not integrate smoothly; vendor lock-in issues.	Smart devices from different brands can't communicate.
Complexity	IoT systems are difficult to design, deploy, and maintain.	Managing hundreds of connected factory sensors.
Unemployment	Automation reduces demand for low-skill labor.	Robots replacing warehouse workers.

02

IoT Basic Characteristics

Considering all **perspectives of modern-day IoT systems**, a few generic and vital characteristics are shown in Figure 2.1.

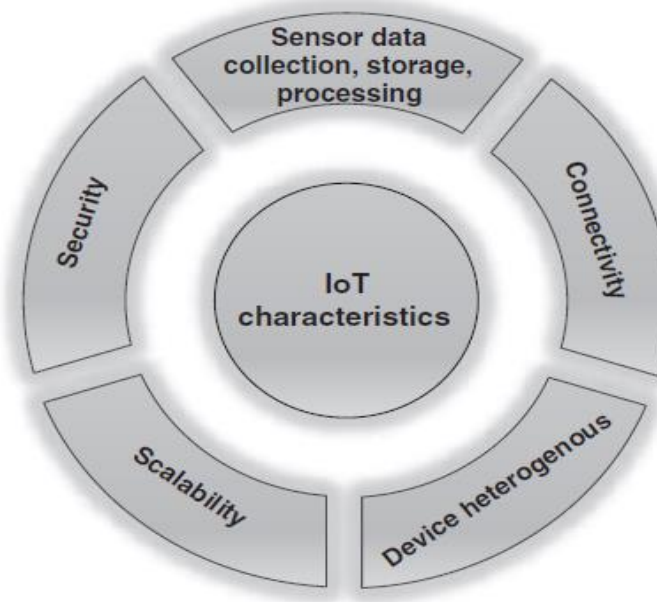


Figure 2.1: Fundamental IoT characteristics

02

IoT Basic Characteristics

- **Sensor Data Acquisition, Storage, Filtering and Analysis** : The plethora of distributed Sensors (or smart things) gather observation of physical environment/entity and direct to Cloud for storage and analytics with an ultimate objective to improve business workflow.
- **Purpose:** The main goal is to transform raw data into meaningful insights that help improve business operations, efficiency, and decision-making.
- **Example** : In a smart agriculture system, soil moisture sensors send data to the cloud, where it's analyzed to determine the best time to irrigate crops — saving water and improving yield.

02

IoT Basic Characteristics

- **Connectivity** : IoT has made possible the **interconnectivity of Physical and Virtual things** with the help of the Internet and global communication infrastructure (that is built using wired and wireless technologies).
 - **Purpose**: Connectivity ensures that devices can **communicate, share data, and work together**, regardless of distance.
 - **Example**: A smartwatch connects to a smartphone via **Bluetooth** and syncs data to the cloud through mobile internet, allowing users to view health stats anywhere.
- **Device Heterogeneity and Intelligence**: The interoperability of devices (based on different hardware and network platforms) with the provisioning of ambient intelligence at the hardware/software level supports intelligent interactions. Many IoT systems are designed with **intelligence** (using AI or machine learning) that enables **autonomous interactions**.

02

IoT Basic Characteristics

- **Device Heterogeneity and Intelligence:**
 - **Purpose:** To ensure that devices can **work together intelligently**, even if they're built on different technologies or platforms.
 - **Example:** A **smart home system** where lights, thermostat, and security cameras from different brands coordinate automatically — **turning off lights and locking doors when the user leaves home.**
- **Scalability:** The plethora of IoT devices connectivity shifts human interactions to device interactions Security . IoT systems must be **scalable** — able to handle large increases in connected devices, data, and users without performance issues.
 - **Purpose:** Scalability ensures that IoT networks remain **efficient, reliable, and responsive** even as they expand.
 - **Example:** A **smart city system** must scale from a few hundred traffic sensors to thousands of connected streetlights, cameras, and vehicles **without breakdowns or delays.**

02

IoT Basic Characteristics

- **The security paradigm** : is required to be implemented at the network level as well as the end-devices level to ensure the security of data.
- **Purpose:** To ensure **data confidentiality, integrity, and availability**, preventing unauthorized access or cyberattacks.
- **Example:** Encrypting communication between **a smart door lock and the user's smartphone** prevents hackers from intercepting access codes.

02

IoT Basic Characteristics

Unique Identity: For effective coordination between the “things” in IoT applications, all the “things” are assigned (deployed) with a unique identity . So, a “thing” can be monitored, updated, and controlled remotely due to its unique identity. Identity is the unique characteristic of a person, group, place, or thing. Every identity has a name and an identification number. The combination of the name and number makes up the identity. This is what helps identify people and things on the internet. Identity is a concept that is found in many aspects of IoT. Device identity is the one thing that makes an IoT device unique and identifiable. Identity can be used to distinguish between different devices, give them a name, and allow them to be controlled. For Example, An IP address of a device is a unique identifier that represents a device in a network.

02

IoT Basic Characteristics

Unique Identity:**➤ Real-World Example:**

- Consider a smart home system: Each smart device (e.g., smart bulb, thermostat, door lock) has a unique identity. When a user opens the mobile app to turn off the living room light, the system uses the light's unique ID (like its IP or MAC address) to send the command to the correct device — not to another bulb in the kitchen.

02

IoT Basic Characteristics

Interoperable Communication Protocol: In IoT applications, all the “things” are deployed in the network of communication. Various protocols are available for device to device and device to communication network. IoT interoperability is the capacity for multiple components within an IoT deployment to effectively communicate, share data, and perform together to achieve a shared outcome .Organizations must be able to transmit and understand data throughout all the connections from devices to the cloud. Since the emergence of IoT, **different communities developed different proprietary protocols which may not be interoperable across different devices.** In simple terms, interoperability allows devices to “speak the same language”, even if they come from different vendors or use different hardware and software architectures. These protocols are being standardized so that they **can be used across different devices.** Some of the interoperable or standardized protocols are **Transmission Control Protocol (TCP), User Datagram Protocol (UDP), IEEE 802.15.4, 6LoWPAN, etc.**

02

IoT Basic Characteristics

Dynamic and Self-Adapting: IoT-based applications and devices are made aware of the environment in such a way that changes in parameters of their surroundings change the context and the IoT applications can accommodate such changes based on user's context. Such intelligent systems can be designed and are called self-adapting IoT applications. In the context of the IoT, self-adaptation is a salient property of smart objects. It allows them to be self-configured and adapted to extreme conditions while ensuring the target system objectives such as comfort, automation, security and safety goals . In IoT, the sensors or devices respond to dynamic events and have the ability to adapt to the change in the environment.

02

IoT Basic Characteristics

Dynamic and Self-Adapting: Dynamic refers to the ability of an IoT system to **respond in real time** to changes in the environment or operating conditions. **Self-adapting** means that the system can **reconfigure or modify its behavior automatically** without the need for manual intervention.

Consider a surveillance system whereby cameras are installed for monitoring a location. Whenever there are no objects in front of the camera, the camera will be in a low power mode. Whenever an object is detected, the camera resumes its activity of monitoring that object. This is the dynamic behavior. The cameras also respond to changes in the environment. If it is night time, the cameras might shift to infrared mode and vice versa during day time. Also, the cameras can adjust their picture clarity based on the environment. Thus, IoT devices can self-adapt to changes in the environment.

02

IoT Basic Characteristics

Self-Configurable: (sometimes referred to as reconfiguration) and **adaptive coordination** (sometimes referred to as **adaptation**) refer to the spectrum of changes that a system makes to itself in response to occurrences in its environment and internally. **Most of the small IoT devices such as sensors, actuators, etc., once deployed have much less direct user interaction. Due to this, many such devices are capable of fetching the latest software updates and setting up basic networking and status checks themselves or with very little user intervention.**

In IoT, self-configurable means that devices (like sensors or actuators) can set themselves up automatically, make changes to their settings, or update their software on their own — without needing a person to do it manually.

02

IoT Basic Characteristics

The IoT sensors or devices have the capability to obtain the instructions from a remote location for installing, updating, or other management-related tasks. These nodes from time to time receive updates or instructions from a remote management server to update the firmware, or remote startup and shutdown. In a weather monitoring system, several sensor nodes or devices will be placed at different locations in a vast area.

- These sensors can automatically connect to the central server when powered on.
- The server can send updates or new instructions: for example, to change how frequently the sensors collect data or to restart them after maintenance.
- All this happens remotely, without a technician physically handling each sensor.

02

IoT Basic Characteristics

Integrated into an Information Network: IoT devices are typically configured in such a way that they can communicate between other devices **in the IoT-based environment to create an information network** . IoT devices can describe themselves using **the unique identity** to other devices or to a network, and are dynamically discovered in the network **by other devices and/or network**. All the sensors or different devices in IoT are connected to the internet or other communication pathway. **The data from sensors is aggregated and pre-processed at the local site or in the cloud. Information can be extracted from the data and appropriate decision can be made.**

02

IoT Basic Characteristics

As an example, consider a fire monitoring system in which different sensors are spread across the trees in a forest. These sensors send the data to a local sink node which is connected to the internet. **This data is analyzed and alerts are generated which are taken care of by the appropriate personnel.**

Being “integrated into an information network” means all IoT devices are **connected, communicating, and cooperating.** They **collect data, share it, and use it** to make smart decisions — creating a system that can think, adapt, and respond automatically. IoT devices are becoming a part of the mainstream electronics culture and people are adopting smart devices into their homes faster than ever. The more data that IoT devices collect, the smarter they will become. The future seems ripe with a host of endless possibilities which only go to show that the evolution of IoT and the growth of IoT technologies have gone past the point of no return.

02

Is IoT The future?

Technology today not only pushes past barricades we once thought insurmountable but also moves us toward a world where equal access to the internet and its resulting technological marvels will be available to everyone. **IoT will continue to evolve in many ways which will amaze and astound us**, ultimately creating a truly limitless potential for everyone. IoT is considered one of the most promising and rapidly evolving technologies of the future. The number of IoT devices is expected to grow exponentially in the Internet of Things coming years, with an **estimated 41.6 billion devices projected to be in use by 2025, according to a report by IDC .**

This growth is being driven by the increasing demand for automation, optimization, and data insights across a range of industries and use cases. IoT has the potential to transform industries such as healthcare, transportation, manufacturing, and agriculture, among others.

02

Is IoT The future?

It can help businesses and organizations to collect valuable data insights, optimize processes, and reduce costs, leading to increased productivity and efficiency. Moreover, IoT technology is evolving at a rapid pace, with advancements being made in areas such as edge computing, AI, and 5G (fifth-generation technology cellular) networks, among others. These advancements are expected to further expand the capabilities and applications of IoT technology, making it even more essential in the future. The future of the IoT is expected to be a major disruptive force in the years to come, transforming the way we live, work, and interact with technology. IoT refers to the interconnected network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and connectivity, allowing these objects to collect and exchange data. The number of IoT devices is projected to continue to grow rapidly in the future. As more devices are connected, there will be an even greater amount of data generated, which can be used to optimize processes and make better decisions .

02

Is IoT The future?

As IoT continues to grow, there will be an increasing focus on integrating AI and machine learning into IoT systems, allowing for even more powerful insights and decision-making. 5G networks promise to deliver higher speeds, lower latency, and greater capacity than previous wireless networks. This will be particularly important for IoT applications, which require reliable and fast connections. The adoption of 5G networks is expected to accelerate the growth of IoT devices and applications. As the number of IoT devices grows, there will be an increasing focus on security and privacy. IoT devices can collect sensitive data, and any security breaches could have serious consequences. Therefore, there will be a greater focus on securing IoT devices and ensuring that user data is protected. In summary, the future of IoT is likely to be characterized by the growth of devices, the integration of AI and machine learning, the development of edge computing, the adoption of 5G networks, and a greater focus on security and privacy.

02

Is IoT The future?

Some of the key trends and advancements expected in the future of IoT include the following :

1. Increased Connectivity: The number of **connected devices is expected to continue to grow**, resulting in a more connected and integrated world. **Example:** In **smart cities**, traffic lights, surveillance cameras, and public transportation systems will all be interconnected, working together to improve traffic flow and public safety.
2. Edge Computing: Edge computing will become increasingly important as **more devices are added to the IoT network, allowing for faster data processing and reducing the need for data to be sent to centralized servers**. Edge computing solves this problem by allowing data to be processed closer to where it is generated — that is, at the “edge” of the network (such as on local gateways or IoT devices themselves).
3. 5G Technology: The rollout of **5G networks** will enable faster and more reliable connectivity, leading to new and improved IoT applications. Example: In healthcare, 5G-enabled IoT devices can transmit patient data instantly to doctors, enabling real-time monitoring and emergency response.

02

Is IoT The future?

4. Artificial Intelligence: The integration of AI into IoT devices will enable more advanced capabilities such as predictive maintenance, enhanced security, and more efficient energy use.
5. Cyber-Security: As the number of connected devices grows, the importance of securing IoT networks will become even more critical, and new technologies and protocols will emerge to address these challenges.
6. Smart Homes and Cities: IoT will play a key role in creating smart homes and cities, with connected devices improving energy efficiency, reducing waste, and making our living spaces more convenient and comfortable.
7. Wearables: The rise of wearable technology will lead to an increased demand for connected devices, such as fitness trackers, smartwatches, and medical devices.

02

History of IoT

The IoT is a term used to describe the interconnected network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to connect and exchange data with each other. The concept of the IoT can be traced back to the late 1990s and early 2000s, when researchers and technology experts first started exploring the idea of connecting everyday devices to the internet . One of the earliest examples of IoT technology was a Coca-Cola machine at Carnegie Mellon University, which was connected to the internet in 1982 and allowed users to check the availability of drinks remotely . Over the next few years, the development of wireless networks, advancements in miniaturization, and the growth of the internet paved the way for the development of the IoT.

02

History of IoT

In 1999, Kevin Ashton, a British technology pioneer, coined the term “IoT” to describe the interconnected network of devices and objects . In the early 2000s, the IoT began to gain momentum, with the introduction of smartphones and the growth of home automation systems. In 2006, Amazon introduced the Amazon Echo, a smart speaker that uses voice commands to control smart home devices and access information from the internet . Since then, the IoT has continued to grow and evolve, with an increasing number of devices being connected to the internet. Today, the IoT is being used in a wide range of applications, from smart homes and cities to industrial systems and healthcare. Figure 1.4 gives insight into the history of the IoT, showing how the term IoT has evolved in the technological world over the period of last three decades.

02

History of IoT

LG announced the first smart refrigerator in 2000, the first iPhone was launched in 2007, and by 2008, the number of connected devices exceeded the number of people on the planet .In 2009, Google started testing driverless cars, and in 2011, Google's Nest smart thermostat hit the market, allowing remote control of central heating and cooling. The concept of IoT started to gain some popularity in the summer of 2010. Information leaked that Google's StreetView service had not only made 360-degree pictures but had also stored tons of data of people's Wi-Fi networks .

People were debating whether this was the start of a new Google strategy to not only index the internet but also index the physical world. The same year, the Chinese government announced it would make the IoT a strategic priority in its updated Five-Year Plan.

02

History of IoT

In 2011, Gartner—the market research company that invented the famous “hype-cycle for emerging technologies”—included a new emerging phenomenon on its list: “The Internet of Things” . The next year, the theme of Europe’s biggest internet conference LeWeb was the “Internet of Things.” At the same time, popular tech-focused magazines like *Forbes*, *Fast Company*, and *Wired* starting using IoT as their vocabulary to describe the phenomenon. In October of 2013, IDC published a report stating that the IoT would be a \$8.9 trillion market in 2020 . The term IoT reached mass market awareness when in January 2014, Google announced the purchase of Nest for US\$3.2 billion. At the same time, the Consumer Electronics Show (CES) in Las Vegas was held under the theme of IoT. Despite its tremendous growth, the IoT is still in its early stages and is expected to continue to evolve and grow in the coming years, with the development of new technologies and increasing demand for connected devices.

02

History of IoT

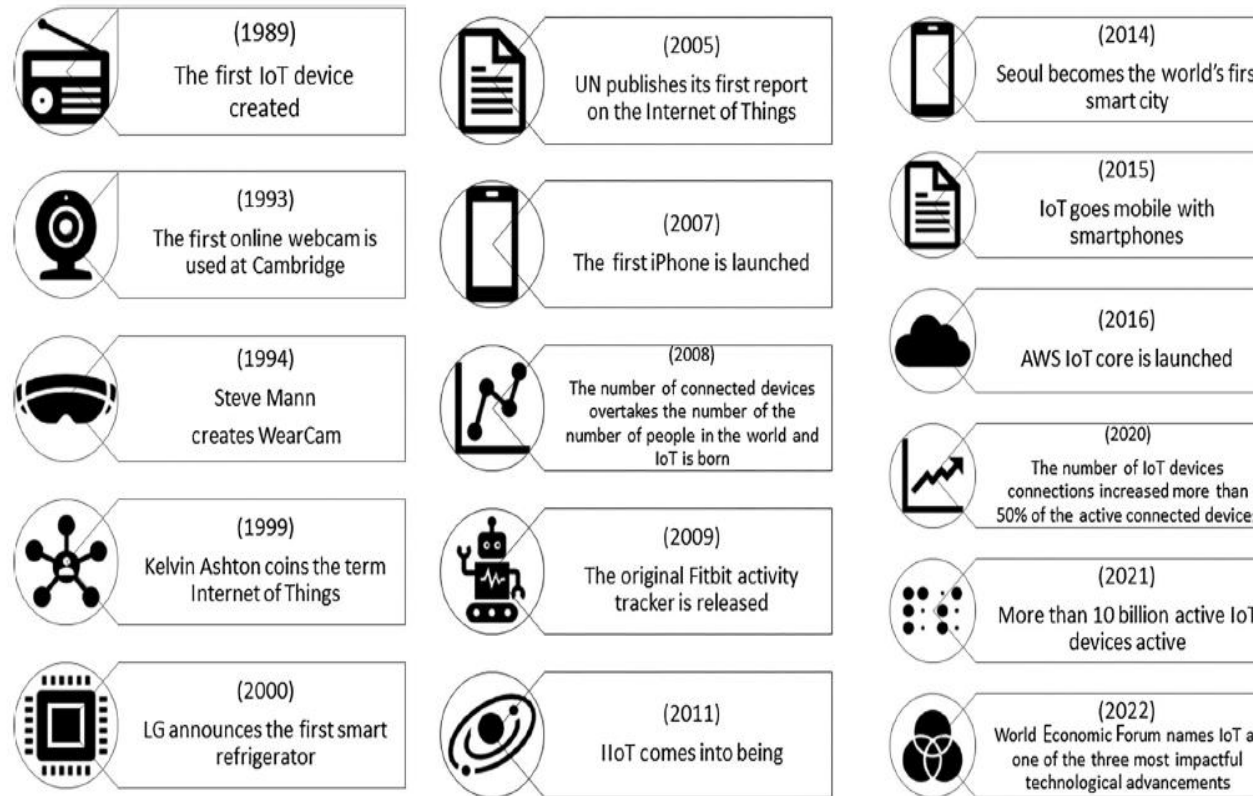


Figure 2.4 The history of the Internet of Things

02

Industrial IoT

Industry 4.0 refers to a new phase in the Industrial Revolution that focuses heavily on interconnectivity, automation, machine learning, and real-time data. Industry 4.0, also sometimes referred to as IIoT(Industrial Internet of Things) or smart manufacturing which provides physical production and operations with smart digital technology, machine learning and big data to create a more holistic and better connected ecosystem for companies that focus on manufacturing and supply chain management. **The Industrial Internet of Things (IIoT)** describes the IoT as used in industries such as manufacturing, logistics, oil and gas, transportation, energy/utilities, mining and metals, aviation and others. These industries represent the majority of gross domestic product among the G20 nations. The IIoT is still at an early stage, similar to where the Internet was in the late 1990s. While the evolution of the consumer Internet over the last two decades provides some important lessons, it is unclear how much of this learning is applicable to the IIoT, given its unique scope and requirements.

Industry 4.0 refers to the use of automation and data exchange in manufacturing. According to the Boston Consulting Group there are nine principal technologies that make up Industry 4.0: Autonomous Robots, Simulation, Horizontal and Vertical System Integration, the Industrial Internet of Things, Cybersecurity, The Cloud, Additive Manufacturing, Data and Analytics, and Augmented Reality. These technologies are used to create a “smart factory” where machines, systems, and humans communicate with each other in order to coordinate and monitor progress along the assembly line.

- Example: A car manufacturing factory uses hundreds of sensors on machines and robots. These sensors send real-time data about temperature, vibration, and energy use to a central system. The system analyzes the data to predict when a machine might fail, allowing maintenance to happen before breakdowns occur.

02

Industrial IoT

Networked devices provide sensor data and are digitally controlled. The net effect is the ability to rapidly design, modify, create, and customize things in the real world, while lowering costs and reacting to changes in consumer preferences, demand, the supply chain and technology. The goal is to enable autonomous decision-making processes, monitor assets and processes in real-time, and enable equally real-time connected value creation networks through early involvement of stakeholders.

For example, **real-time responses are often critical in manufacturing, energy, transportation and healthcare:**

- real time for today's Internet usually means a few seconds ,whereas real time for industrial machines involves **sub-millisecond scales.** Another important consideration is reliability. For example: In a smart factory, production managers can see the exact status of every machine and material in real time. If there's a delay in one stage, the system can automatically adjust other processes or notify workers.

02

Industrial IoT

Suppliers, manufacturers, and distributors can all share data instantly, making the entire supply chain more responsive. This creates a connected ecosystem where every stakeholder — **from suppliers to customers** — is involved early and can react immediately to changes in demand, design, or supply.

➤ Example

- A supplier provides raw materials (like steel, plastic, or microchips).
- IoT sensors on the supplier's inventory system track stock levels, delivery status, and quality in real time.
- This data is automatically uploaded to a shared cloud platform that the manufacturer can access.

02

Industrial IoT

Much attention has been given to the efforts of large companies such as Cisco, GE, and Huawei, and government initiatives such as Industrie 4.0 in Germany.

For example:

- **GE announced** that it realized more than \$1 billion in incremental revenues in 2014 by helping customers improve asset performance and business operations through IIoT capabilities and services.
- The German government is sponsoring “Industrie 4.0”, a multi-year strategic initiative that brings together leaders from the public and private sectors as well as from academia to create a comprehensive vision and action plan for applying digital technologies to the German industrial sector.

02

Industrial IoT

The IIoT's potential payoff is enormous. **Operational efficiency is one of its key attractions**, and early adopters are focused on these benefits. By introducing automation and more flexible production techniques.

➤ For example, in manufacturing, by using IIoT:

- Machines can self-monitor for signs of wear or failure.
- Production lines can adjust automatically to demand changes.
- Workers receive real-time alerts about performance issues.

As a result, factories can increase productivity by up to 30%, while reducing downtime, maintenance costs, and energy consumption.

02

Industrial IoT

In this context, three IIoT capabilities must be mastered:

1. **sensor-driven computing:** converting sensed data into insights that operators and systems can act on.

➤ **Example:** In a chemical plant, sensors monitor the pressure and temperature inside a reactor.

If readings exceed safe limits, the system automatically:

- Adjusts the input valves, or
- Sends an alert to engineers to **take corrective action**.

2. **industrial analytics:** turning data from sensors and other sources into **actionable insights**.

➤ **Example:** In a car manufacturing plant, industrial analytics can:

- Predict when a robotic arm is about to fail based on its vibration and movement data.
- Suggest preventive maintenance before it breaks down.
- Optimize production speed by identifying slow points in the assembly line.

02

Industrial IoT

In this context, three IIoT capabilities must be mastered:

3. intelligent machine applications: integrating sensing devices and **intelligent components into machines.**

➤ **Example:** In a **smart factory**, a production robot:

- Detects a problem in one part of the assembly line.
- Automatically slows its speed.
- Sends a signal to other machines to adjust their timing to avoid defects.

02

Industrial IoT

How These Three Capabilities Work Together

Capability	Function	Outcome
Sensor-Driven Computing	Collects and converts physical data into digital signals.	Real-time awareness of equipment and environment.
Industrial Analytics	Processes data to find patterns and make predictions.	Smarter decisions and proactive maintenance.
Intelligent Machine Applications	Machines act autonomously using sensor data and analytics.	Automation, flexibility, and self-optimization.

02

Industrial IoT

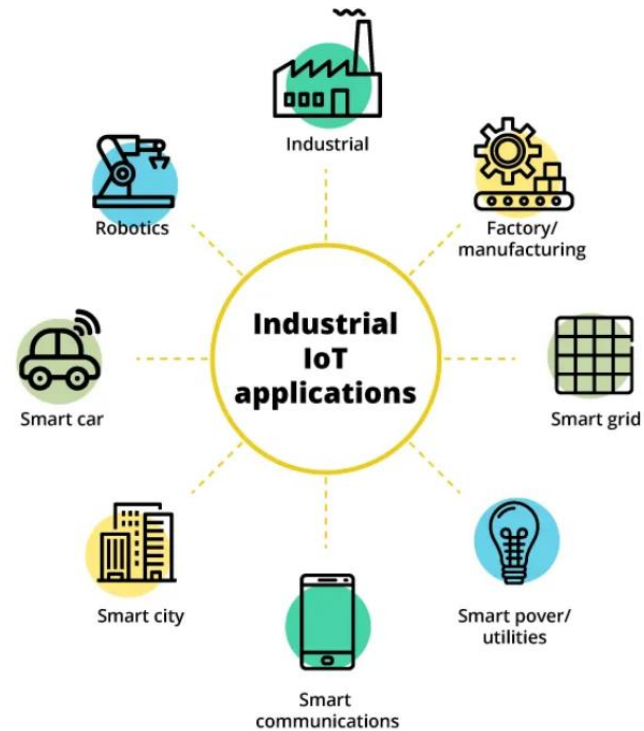


Figure 2.5
The applications of IIoT

02

Summary

1. Disadvantages of IoT
2. Characteristics of IoT
3. History of IoT
4. Industrial IoT



Thank You