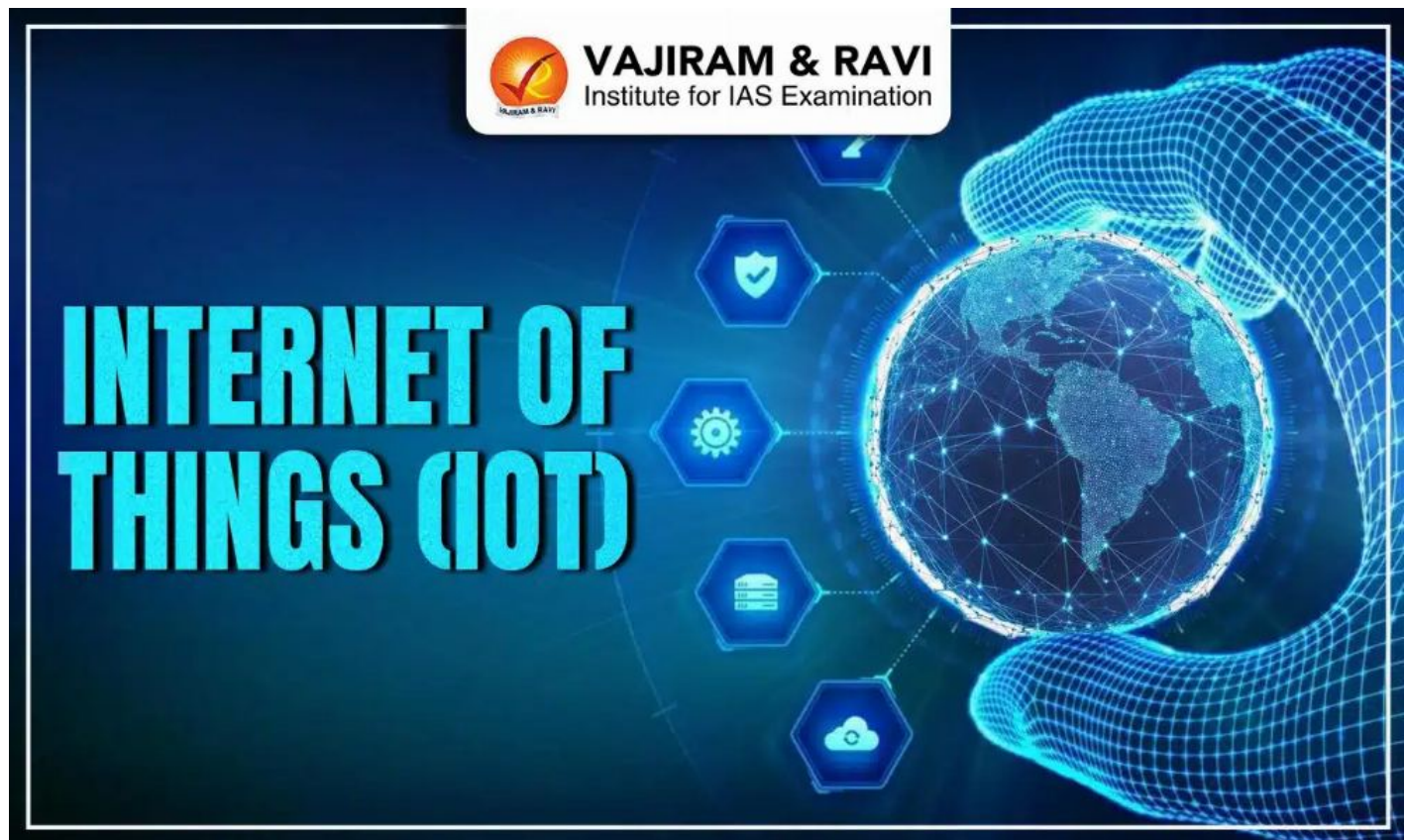


Internet of Things (IoT) - Meaning, Characteristics, Applications

July 10, 2026 • vajiramandravi.com



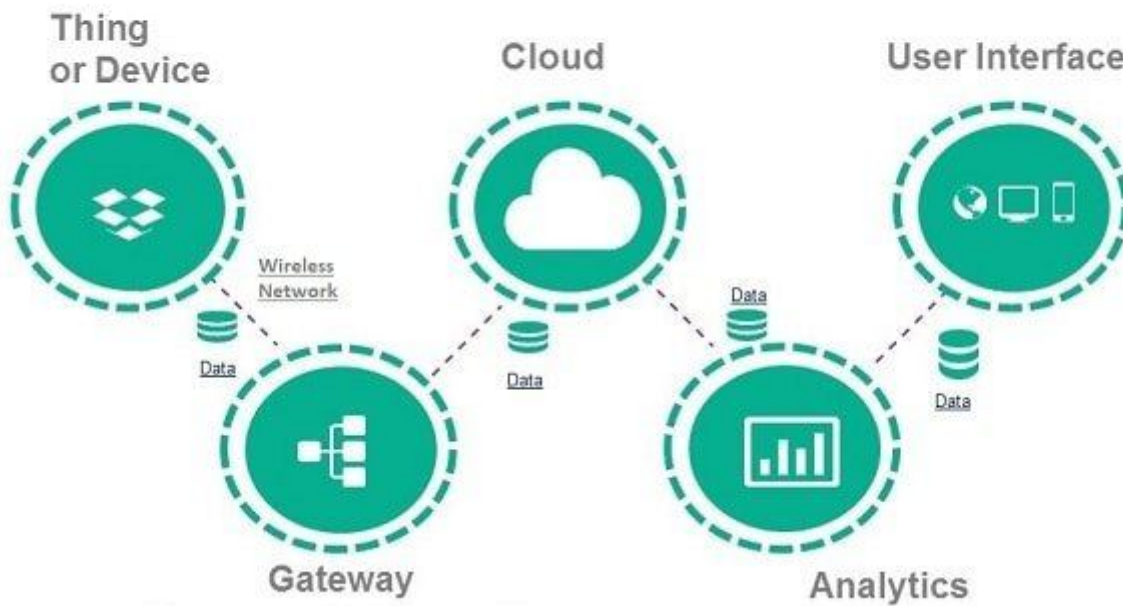
The **Internet of Things (IoT)** refers to an integrated system of **physical objects (things)** embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data within the systems over the “**internet**”. The physical objects used in the IoT range from ordinary household objects to sophisticated industrial tools connected to the internet via embedded devices.

IoT is one of the fastest emerging technologies, providing enormous beneficial opportunities for individuals, society, and governments.

Major Components of Internet of Things

Various components are required to work together in order to facilitate Internet of Things (IoT). These are as follows:

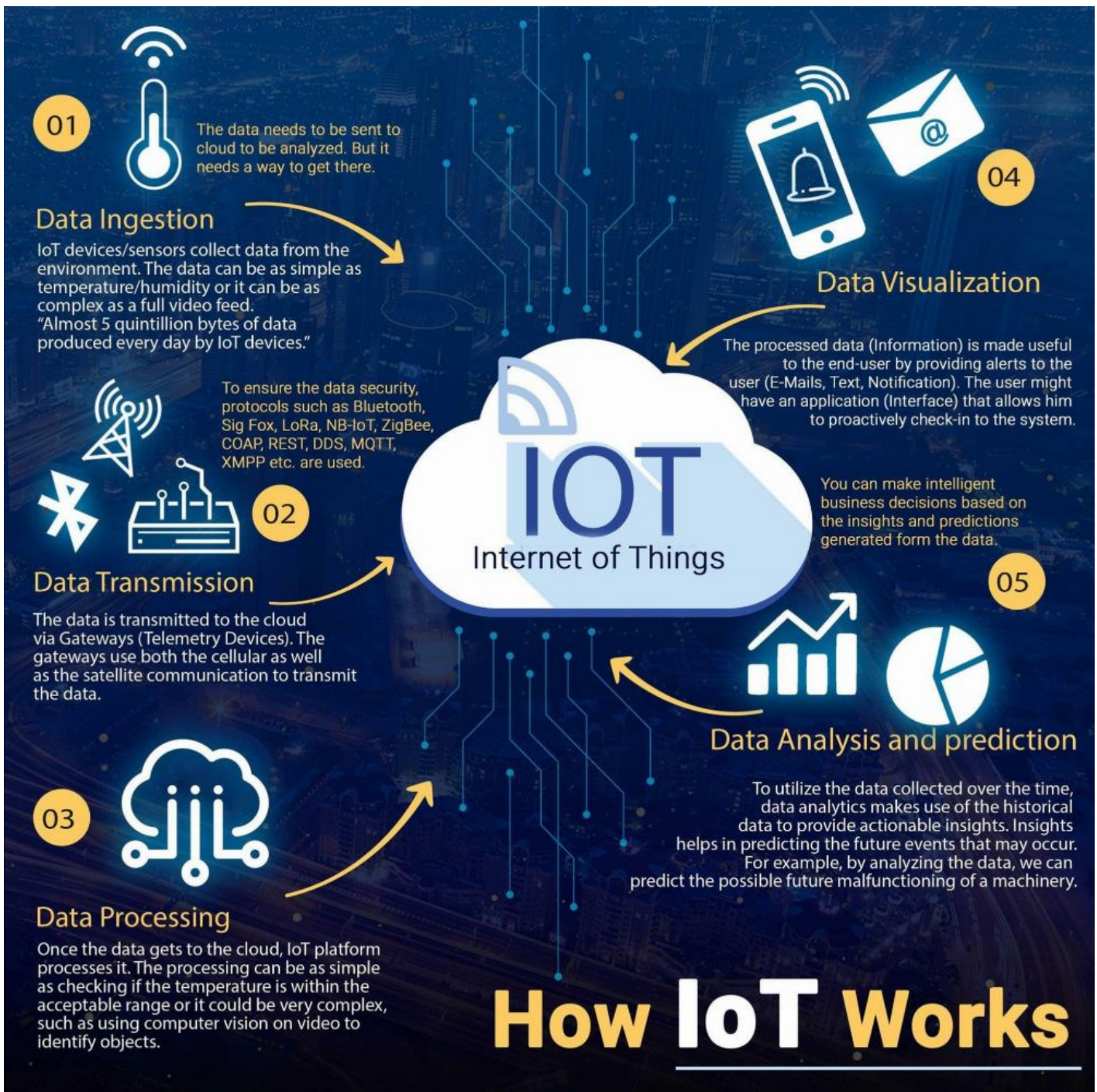
Major Components of IoT



- **Things or devices:** These include smart thermostats, wearable fitness trackers, connected home appliances, industrial machinery that has embedded sensors, processors, and communication hardware to collect and transmit data.
 - IoT devices are connected to the internet network through various means, such as Wi-Fi, cellular networks, Bluetooth, etc.
- **Gateway:** Gateway ensures **interoperability** of the connected devices and sensors.
 - It manages the **bidirectional data traffic** between different networks and protocols.
- **Cloud:** IoT cloud offers tools to collect, process, manage, and store huge amounts of data in real time.
 - Industries and services can easily access this data remotely and make critical decisions when necessary.
- **Analytics:** It is the process of converting analog data from billions of smart devices and sensors into useful insights that can be interpreted and used for detailed analysis.
 - It manages and improves the IoT system.
- **User interface:** User interfaces are the visible and tangible part of the IoT system that users can access, interact with, and feed input and response to.

Working of Internet of Things (IoT)

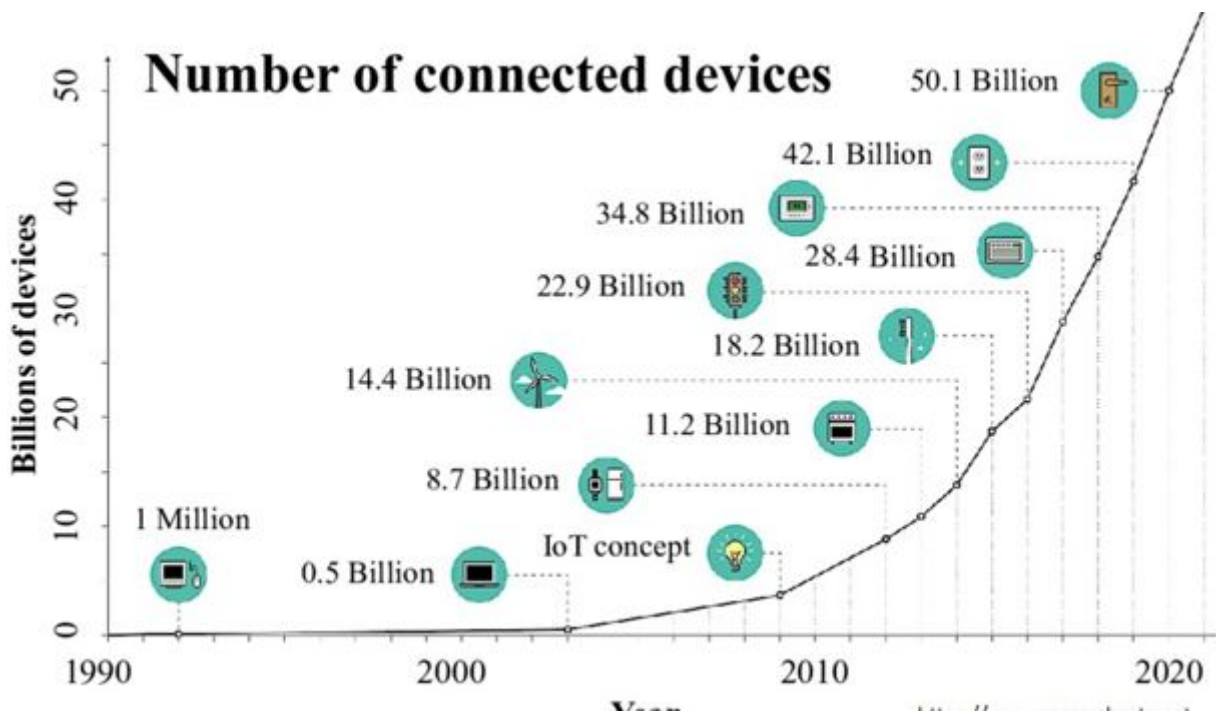
IoT devices usually have some form of built-in intelligence, which allows them to gather data and make decisions without human intervention. Following are the general working principles of IoT.



- **Data Ingestion:** IoT devices or **sensors collect data** from the environment and provide inputs such as temperature and humidity for further processing in clouds.
- **Data transmission:** The data is transmitted to the cloud via Gateway.
 - Gateway uses both cellular and satellite communication to transmit data.
- **Data processing:** Data processed at cloud level generates optimal response.
 - For example, to check the temperature range of an Air Conditioner.
- **Data visualization:** It is about showing information and alerting for proactive response.
- **Data analysis and prediction:** Data analytics make use of collected data over time to provide actionable insight. It helps in predicting future events.
 - For example, by analysing data, future malfunctioning of machines can be predicted.

Characteristics of IoT

The key features of the IoT are being described below.



- **Scalability:** IoT systems can be scaled to accommodate a large number of devices, making it suitable for a wide range of applications, from small-scale home automation to large-scale industrial implementations.
 - As per the projections, 26.4 billion IoT devices will be in service globally by 2026.
- **Connectivity:** Connectivity is the heart of IoT.
 - Devices are interconnected through various communication protocols, including Wi-Fi, cellular networks, etc.
 - This allows devices to communicate and share data over the internet.
- **Remotely Controlled:** IoT devices can be managed and controlled remotely, which allows users to interact with them through various devices including smartphones, via web applications.
- **Customized to user needs:** It provides tailor made solutions to suit specific needs of diverse users.
- **Real-Time Monitoring:** IoT devices provide real-time data, allowing for immediate responses and decision-making based on up-to-date information.
- **Interoperability:** Standardised protocols and communication technologies facilitate the interoperability of different IoT devices and platforms, enabling them to work together seamlessly.
- **Sensor Integration:** IoT devices are equipped with sensors that can collect data about their environment or specific parameters, such as temperature, humidity, pressure, motion, light, and so on.

Applications of Internet of Things

The Internet of Things (IoT) is a **versatile emerging technology** with diverse applications in various key sectors encompassing all quarters of human lives.



- **Smart Homes:** Home automation systems are designed to make everyday routine tasks convenient, such as regulating lights, controlling appliances, adjusting thermostats, etc.
 - It works with the help of **Embedded systems, Home Automation Systems, Energy Management** and **Climate adaptation**.
- **Health and wellbeing (Internet of Medical Things):**
 - **IoT for Patients** - Wearable devices such as fitness bands and other wirelessly connected devices **track and monitor** health parameters such as heartbeats and oxygen saturation in individual patients.
 - **IoT for doctors** - Data collected from IoT devices can help physicians identify the best treatment process for patients by using wearables and other home monitoring equipments, etc.
 - **IoT for Hospitals** - IoT devices tagged with sensors can be used for tracking real time location of medical equipment like wheelchairs, defibrillators, nebulizers, oxygen pumps, and other monitoring equipment.
- **Smart industry:** IoT can boost productivity by enabling industrial **automation** by real-time data analytics and seamless operations with high-quality output.
 - The automation of industrial processes or **Industrial IoT** is integral to **Industry 4.0**.
- **Smart Energy: IoT-enabled smart grid empowers consumers and governments to make better decisions regarding energy usage.**
 - It allows cities to save electricity through sophisticated, seamless connectivity and communications.
- **Smart agriculture:** IoT enables precision farming through data analysis to optimise agricultural operations.
 - It monitors key parameters such as soil moisture, nutrients, etc. and helps the farmer community make better informed decisions.
 - It uses various technologies such as GPS, GIS, sensors, aerial devices, field mapping, etc. to streamline crop management processes, increase production levels, and improve profitability.

- **Example:** Israel based start-up **FieldIn** employs IoT to manage pests by using pesticides more efficiently and safely.
- **Smart Environment:** IoT allows environmental sensors to connect with devices such as smartphones to enable real time status of environmental factors such as humidity, temperature, pollutants, etc.
 - Moreover, it gives information about CO2 emissions and other greenhouse gases that can be harnessed for climate modeling.
- **IoT in Disaster Management:** IoT can be helpful in quick hazard mapping, Earthquake Early Warning Systems, etc.
 - For example, the **National Advance Seismic System** of the United States delivers real-time information, providing situational awareness for emergency response.
- **Smart Water Monitoring: Ministry of Jal Shakti**, India, has decided to employ “**sensorr-based IoT devices**” in every village under the National Jal jeevan mission to monitor the quality of water.
- **Smart Cities:** Smart cities leverage IoT to facilitate **smart infrastructure** to improve the quality of life for their city residents, optimize resource usage, and increase operational efficiency.
 - **Smart traffic management systems** for example, employ embedded sensors and cameras to regulate traffic flow by taking real time data.
- **Street lighting** offers energy-efficient solutions through adaptive lighting facilitated by embedded systems on the network.
- **Waste Management Systems** optimise collection routes and schedule the fill levels of waste containers by collecting and analysing sensor data.
- **IoT in Defense: The Internet of Military Things (IoMT)** is a class of connected devices employed for warfare.
 - It has wide applications in advanced combat operations and intelligence-oriented warfare.
 - It allows real-time connectivity among devices, such as between unmanned vehicles and a central command station.
 - For example, **Joint All Domain Command and Control** of the United States is based on a similar network of sensors that connect all battlefield devices.

Government Initiatives to Promote IoT

The versatile utility of IoT has prompted the Indian Government to take the following initiatives to boost its adoption in India:

- **Draft IoT Policy, 2015:** Ministry of Electronics and Information Technology launched **India's first** IoT Policy Document in 2014 as a framework for holistic implementation and execution of IoT-related policies.
- **IoT-Centre of Excellence (CoE) by NASSCOM, MeitY, and ERNET:** The CoE is specifically designed to help Indian IoT start-ups create market-leading products.
 - CoE is India's largest deep tech innovation ecosystem.
- **National Digital Communications Policy 2018:** It envisages enhancing internet and digital engagement through IoT.
- **Future Skill PRIME:** It is a joint initiative by **Nasscom & MeitY** aiming to create a reskilling/upskilling ecosystem in ten emerging and futuristic technologies, including **IoT**.

Challenges Associated with IoT

IoT offers many benefits; however, it also poses several risks and challenges. Following are some of the issues.

- **Security and privacy risks:** Any Internet-enabled device is vulnerable to being hacked and misused.
 - In the age of the Internet of Things, there are billions of connected devices that someone can use to access private data, spread malware, or even cause tangible harm.
 - A recent leak of personally identifiable information about 815 million Indians on the dark web highlighted the vulnerability of devices connected to the internet.
 - Data-breach further result in significant financial losses for both individuals and governments.
- **Interoperability issues:** IoT devices from different manufacturers often use distinct standards and protocols, making it incompatible to interact and communicate between machines.
- **Cost and complexity:** Implementing an IoT system requires significant investments in hardware, software, and infrastructure. Moreover, it requires specialized skills and expertise.
- **Regulatory and legal challenges:** Large-scale application and production of IoT devices in various geographies create regulatory and legal challenges.
 - Different regulatory standards across nations create a complex environment for MNCs to comply with data protection, privacy, and cybersecurity laws and regulations.
- **Digital divide:** The operation of IoT depends on Internet facilities, which are lacking in under-developed and developing countries, such as India.

IoT as an emerging technology is still in its evolving phase. Given its vast applications encompassing almost all quarters of human lives, the number of IoT devices is going to increase more rapidly in the future.

Source: <https://vajiramandravi.com/upsc-exam/internet-of-things-iot/>

© Vajiram & Ravi. For personal use only.