Presentation on

Internet of Things

By,

Nand Gondha

160470116012

7th IT D1

Internet of Things(IoT)

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

History of IOT

Kevin Ashton, co-founder of the Auto-ID Center at MIT, first mentioned the internet of things in a presentation he made to Procter & Gamble (P&G) in 1999. Wanting to bring radio frequency ID (RFID) to the attention of P&G's senior management, Ashton called his presentation "Internet of Things" to incorporate the cool new trend of 1999: the internet. MIT professor Neil Gershenfeld's book, When Things Start to Think, also appearing in 1999, didn't use the exact term but provided a clear vision of where IoT was headed.

IoT has evolved from the convergence of wireless technologies, microelectromechanical systems (MEMS), microservices and the internet. The convergence has helped tear down the silos between operational technology (OT) and information technology (IT), enabling unstructured machine-generated data to be analyzed for insights to drive improvements.

Although Ashton's was the first mention of the internet of things, the idea of connected devices has been around since the 1970s, under the monikers embedded internet and pervasive computing.

The first internet appliance, for example, was a Coke machine at Carnegie Mellon University in the early 1980s. Using the web, programmers could check the status of the machine and determine whether there would be a cold drink awaiting them, should they decide to make the trip to the machine.

IoT evolved from machine-to-machine (M2M) communication, i.e., machines connecting to each other via a network without human interaction. M2M refers to connecting a device to the cloud, managing it and collecting data.

Taking M2M to the next level, IoT is a sensor network of billions of smart devices that connect people, systems and other applications to collect and share data. As its foundation, M2M offers the connectivity that enables IoT.

The internet of things is also a natural extension of SCADA (supervisory control and data acquisition), a category of software application program for process control, the gathering of data in real time from remote locations to control equipment and conditions. SCADA systems include hardware and software components. The hardware gathers and feeds data into a computer that has SCADA software installed, where it is then processed and presented it in a timely manner. The evolution of SCADA is such that late-generation SCADA systems developed into first-generation IoT systems.

The concept of the IoT ecosystem, however, didn't really come into its own until the middle of 2010 when, in part, the government of China said it would make IoT a strategic priority in its five-year plan.

How IoT works

An IoT ecosystem consists of web-enabled smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

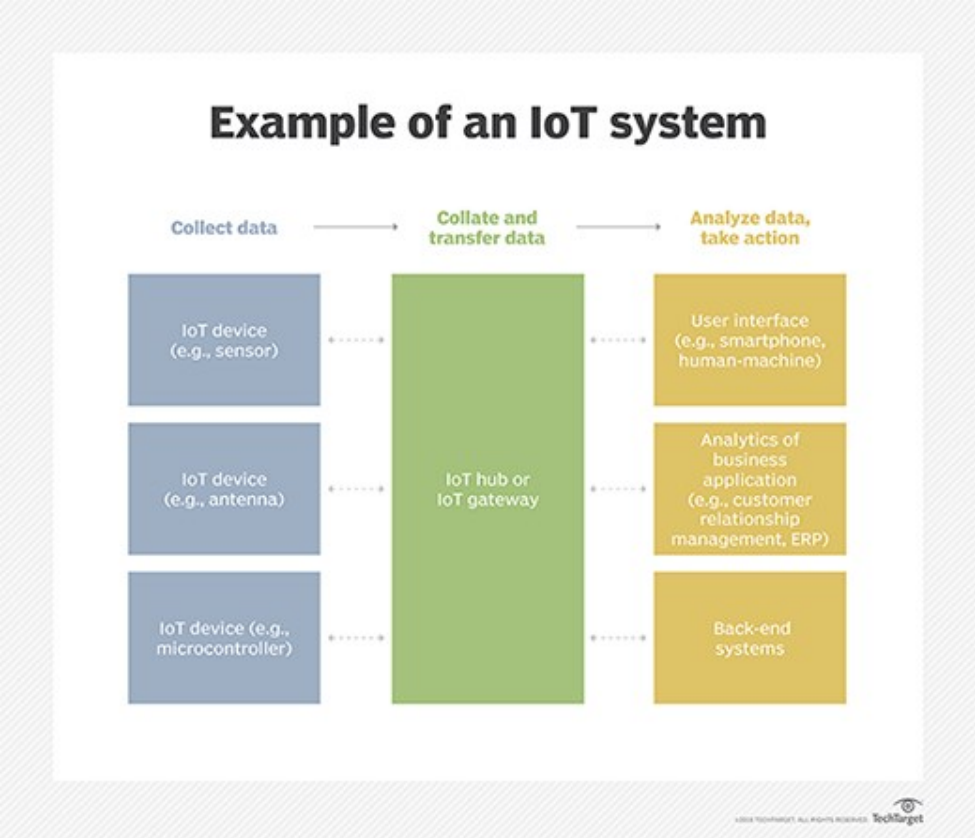
Why IoT is important

The internet of things helps people live and work smarter as well as gain complete control over their lives. In addition to offering smart devices to automate homes, IoT is essential to business. IoT provides businesses with a real-time look into how their companies' systems really work, delivering insights into everything from the performance of machines to supply chain and logistics operations.

IoT enables companies to automate processes and reduce labor costs. It also cuts down on waste and improves service delivery, making it less expensive to manufacture and deliver goods as well as offering transparency into customer transactions.

IoT touches every industry, including healthcare, finance, retail and manufacturing. Smart cities help citizens reduce waste and energy consumption and connected sensors are even used in farming to help monitor crop and cattle yields and predict growth patterns.

As such, IoT is one of the most important technologies of everyday life and it will continue to pick up steam as more businesses realize the potential of connected devices to keep them competitive.



Benefits of IoT

The internet of things offers a number of benefits to organizations, enabling them to:

- Monitor their overall business processes;
- Improve the customer experience;
- Save time and money;
- Enhance employee productivity;
- Integrate and adapt business models;
- Make better business decisions; and
- Generate more revenue.

IoT encourages companies to rethink the ways they approach their businesses, industries and markets and gives them the tools to improve their business strategies.

Pros and cons of IoT

Some of the advantages of IoT include:

- Ability to access information from anywhere at any time on any device;

- Improved communication between connected electronic devices;
- Transferring data packets over a connected network saves time and money;
- Automating tasks helps improve the quality of a business' services and reduces the need for human intervention.

Some disadvantages of IoT include:

- As the number of connected devices increases and more information is shared between devices, the potential that a hacker could steal confidential information also increases;
- Enterprises may eventually have to deal with massive numbers -- maybe even millions -- of IoT devices and collecting and managing the data from all those devices will be challenging.
- If there's a bug in the system, it's likely that every connected device will become corrupted;
- Since there's no international standard of compatibility for IoT, it's difficult for devices from different manufacturers to communicate with each other.

IoT standards and frameworks

There are several emerging IoT standards, including:

- 6LoWPAN (IPv6 over Low -Power Wireless Personal Area Networks), an open standard defined by the Internet Engineering Task Force (IETF). The 6LoWPAN standard enables any low-power radio to communicate to the internet, including 804.15.4, Bluetooth Low Energy and Z-Wave (for home automation).
- ZigBee0, a low-power, low data-rate wireless network used mainly in industrial settings. ZigBee is based on based the IEEE 802.15.4 standard. The ZigBee Alliance created Dotdot, the universal language for IoT that enables smart objects to work securely on any network and understand each other.
- LiteOS, a Unix-like operating system for wireless sensor networks. LiteOS supports smartphones, wearables, intelligent manufacturing applications, smart homes and Internet of Vehicles (IoV). The operating system also serves as a smart device development platform.
- OneM2M, a machine-to-machine service layer that can be embedded in software and hardware to connect devices. The global standardization

body, OneM2M, was created to develop reusable standards to enable IoT applications across different verticals to communicate.

- DDS (Data Distribution Service) was developed by the Object Management Group (OMG) and is an IoT standard for real-time, scalable and high-performance machine-to-machine communication.
- AMQP (Advanced Message Queuing Protocol), an open source published standard for asynchronous messaging by wire. AMQP enables encrypted and interoperable messaging between organizations and applications. The protocol is used in client/servermessaging and in IoT device management.
- CoAP (Constrained Application Protocol), a protocol designed by the IETF that specifies how low-power compute-constrained devices can operate in the internet of things.
- LoRaWAN (Long Range Wide Area Network), a protocol for wide area networks, it's designed to support huge networks, such as smart cities, with millions of low-power devices.

IoT frameworks include:

- AWS IoT, a cloud platform for IoT released by Amazon. This framework is designed to enable smart devices to easily connect and securely interact with the AWS cloud and other connected devices.
- ARM Mbed IoT, a platform to develop apps for the IoT based on ARM microcontrollers. The goal of the ARM Mbed IoT platform is to provide a scalable, connected and secure environment for IoT devices by integrating Mbed tools and services.
- Microsoft's Azure IoT Suite, a platform that consists of a set of services that enables users to interact with and receive data from their IoT devices as well as perform various operations over data, such as multidimensional analysis, transformation and aggregation, and visualize those operations in a way that's suitable for business.
- Google's Brillo/Weave, a platform for the rapid implementation of IoT applications. The platform consists of two main backbones: Brillo, an android-based operating system for the development of embedded low power devices; and Weave, IoT-oriented communication protocol that serves as the communication language between the device and the cloud.
- Calvin, an open source IoT platform released by Ericsson designed for building and managing distributed applications that enable devices talk to each other. Calvin includes a development framework for application developers as well as a runtime environment for handling the running application.

Consumer and enterprise IoT applications

There are numerous real-world applications of the internet of things, ranging from consumer IoT and enterprise IoT to manufacturing and industrial IoT (IIoT). IoT applications span numerous verticals, including automotive, telecom and energy.

In the consumer segment, for example, smart homes that are equipped with smart thermostats, smart appliances and connected heating, lighting and electronic devices can be controlled remotely via computers and smartphones.

Wearable devices with sensors and software can collect and analyze user data, sending messages to other technologies about the users with the aim of making users' lives easier and more comfortable. Wearable devices are also used for public safety -- for example, improving first responders' response times during emergencies by providing optimized routes to a location or by tracking construction workers' or firefighters' vital signs at life-threatening sites.

In healthcare, IoT offers many benefits, including the ability to monitor patients more closely to use the data that's generated and analyze it. Hospitals often use IoT systems to complete tasks such as inventory management, for both pharmaceuticals and medical instruments.

Smart buildings can, for instance, reduce energy costs using sensors that detect how many occupants are in a room. The temperature can adjust automatically -- for example, turning the air conditioner on if sensors detect a conference room is full or turning the heat down if everyone in the office has gone home.

In agriculture, IoT-based smart farming systems can help monitor, for instance, light, temperature, humidity and soil moisture of crop fields using connected sensors. IoT is also instrumental in automating irrigation systems.

In a smart city, IoT sensors and deployments, such as smart streetlights and smart meters, can help alleviate traffic, conserve energy, monitor and address environmental concerns and improve sanitation.

IoT security and privacy issues

The internet of things connects billions of devices to the internet and involves the use of billions of data points, all of which need to be secured. Due to its expanded attack surface, IoT security and IoT privacy are cited as major concerns.

In 2016, one of the most notorious recent IoT attacks was Mirai, a botnet that infiltrated domain name server provider Dyn and took down many websites for an extended period of time in one of the biggest distributed denial-of-service (DDoS) attacks ever seen. Attackers gained access to the network by exploiting poorly secured IoT devices.

Because IoT devices are closely connected, all a hacker has to do is exploit one vulnerability to manipulate all the data, rendering it unusable. Manufacturers that don't update their devices regularly -- or at all -- leave them vulnerable to cybercriminals.

Additionally, connected devices often ask users to input their personal information, including names, ages, addresses, phone numbers and even social media accounts -- information that's invaluable to hackers.

However, hackers aren't the only threat to the internet of things; privacy is another major concern for IoT users. For instance, companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data.

Beyond leaking personal data, IoT poses a risk to critical infrastructure, including electricity, transportation and financial services.

The future of IoT

There is no shortage of IoT market estimations. For example, a few include:

- Bain & Company expects annual IoT revenue of hardware and software to exceed $450 billion by 2020.
- McKinsey & Company estimates IoT will have an $11.1 trillion impact by 2025.
- IHS Markit believes the number of connected IoT devices will increase 12% annually to reach 125 billion in 2030.
- Gartner assesses that 20.8 billion connected things will be in use by 2020, with total spend on IoT devices and services to reach $3.7 trillion in 2018.