Module-1

1. Discuss different challenges of IOT.

Ans:

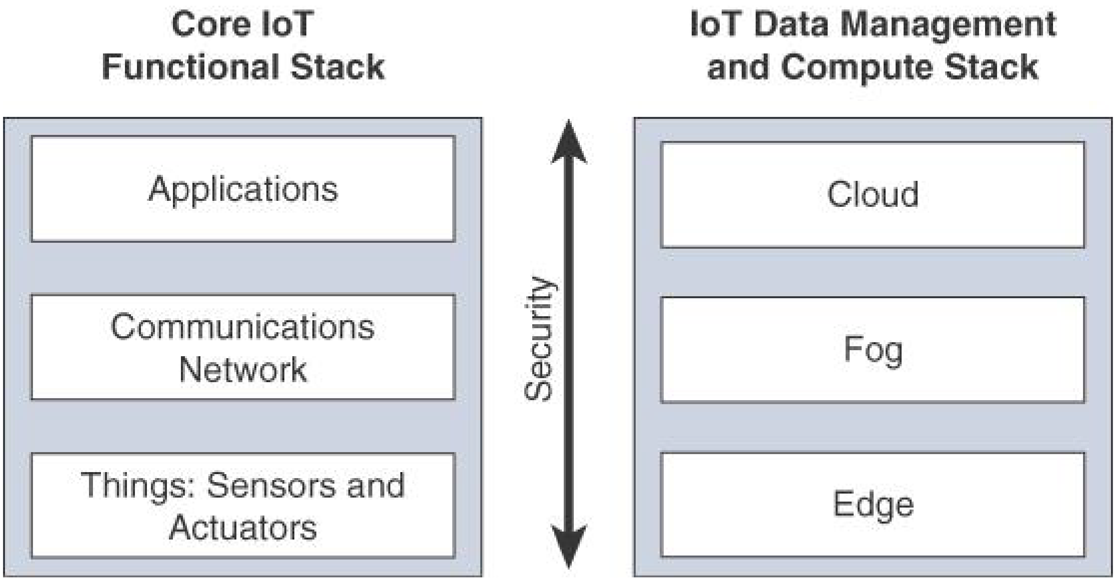
IOT CHALLENGES

Challenge	Description
Scale	While the scale of IT networks can be large, the scale of OT can be several orders of magnitude larger. For example, one large electrical utility in Asia recently began deploying IPv6-based smart meters on its electrical grid. While this utility company has tens of thousands of employees (which can be considered IP nodes in the network), the number of meters in the service area is tens of millions. This means the scale of the network the utility is managing has increased by more than 1,000-fold! Chapter 5, "IP as the IoT Network Layer," explores how new design approaches are being developed to scale IPv6 networks into the millions of devices.
Security	With more "things" becoming connected with other "things" and people, security is an increasingly complex issue for IoT. Your threat surface is now greatly expanded, and if a device gets hacked, its connectivity is a major concern. A compromised device can serve as a launching point to attack other devices and systems. IoT security is also pervasive across just about every facet of IoT. For more information on IoT security, see Chapter 8, "Securing IoT."
Privacy	As sensors become more prolific in our everyday lives, much of the data they gather will be specific to individuals and their activities. This data can range from health information to shopping patterns and transactions at a retail establishment. For businesses, this data has monetary value. Organizations are now discussing who owns this data and how individuals can control whether it is shared and with whom.
Big data and data analytics	IoT and its large number of sensors is going to trigger a deluge of data that must be handled. This data will provide critical information and insights if it can be processed in an efficient manner. The challenge, however, is evaluating massive amounts of data arriving from different sources in various forms and doing so in a timely manner. See Chapter 7 for more information on IoT and the challenges it faces from a big data perspective.
Interoperability	As with any other nascent technology, various protocols and architectures are jockeying for market share and standardization within IoT. Some of these protocols and architectures are based on proprietary elements, and others are open. Recent IoT standards are helping minimize this problem, but there are often various protocols and implementations available for IoT networks. The prominent protocols and architectures—especially open, standards-based implementations—are the subject of this book. For more information on IoT architectures, see Chapter 2, "IoT Network Architecture and Design." Chapter 4, "Connecting Smart Objects," Chapter 5, "IP as the IoT Network Layer," and Chapter 6, "Application Protocols for IoT," take a more in-depth look at the protocols that make up IoT.

2. With a neat diagram, explain architecture of IOT.

Ans:

- The framework is presented as two parallel stacks:
- The IoT Data Management and Compute Stack and
- The Core IoT Functional Stack.



- The network communications layer of the IoT stack itself involves a significant amount of detail and incorporates a vast array of technologies.
- Consider for a moment the heterogeneity of IoT sensors and the many different ways that exist to connect them to a network.
- The network communications layer needs to consolidate these together, offer gateway and backhaul technologies, and ultimately bring the data back to a central location for analysis and processing.
- The three data management layers are:
    - The edge layer (data management within the sensors themselves),
    - The fog layer (data management in the gateways and transit network),
    - The cloud layer (data management in the cloud or central data center).

3. What does IOT and digitization mean? Elaborate on this concept.

Ans:

- IoT and digitization are terms that are often used interchangeably.
- In most contexts, this duality is fine, but there are key differences to be aware of.
- At a high level, IoT focuses on connecting "things," such as objects and machines, to a computer network, such as the Internet. IoT is a well-understood term used across the industry as a whole.
- On the other hand, digitization can mean different things to different people but generally encompasses the connection of "things" with the data they generate and the business insights that result.
- Digitization, as defined in its simplest form, is the conversion of information into a digital format.
- For example, the whole photography industry has been digitized.
- The video industry.
- Transportation industry -Uber.
- In the context of IoT, digitization brings together things, data, and business process to make networked connections more relevant and valuable.

4. What are the elements of one M2M IOT architecture? Explain.

Ans:

- To standardize the rapidly growing field of machine-to-machine (M2M) communications, the European Telecommunications Standards Institute (ETSI) created the M2M Technical Committee in 2008
- The goal of oneM2M is to create a common services layer, which can be readily embedded in field devices to allow communication with application servers
- oneM2M's framework focuses on IoT services, applications, and platforms
- One of the greatest challenges in designing an IoT architecture is dealing with the heterogeneity of devices, software, and access methods
- By developing a horizontal platform architecture, oneM2M is developing standards that allow interoperability at all levels of the IoT stack
- For example, you might want to automate your HVAC system by connecting it with wireless temperature sensors spread throughout your office
- Three major domains:
  - The application layer:
    - The oneM2M architecture gives major attention to connectivity between devices and their applications

        - This domain includes the application-layer protocols and attempts to standardize northbound API definitions for interaction with business intelligence (BI) systems
    - The services layer:
        - This layer is shown as a horizontal framework across the vertical industry applications
        - At this layer, horizontal modules include the physical network that the IoT applications run on, the underlying management protocols, and the hardware.
        - Examples include backhaul communications via cellular, MPLS networks, VPNs, and so on.
        - Riding on top is the common services layer.
        - This conceptual layer adds APIs and middleware supporting third-party services and applications
    - The network layer:
        - This is the communication domain for the IoT devices and endpoints.
        - It includes the devices themselves and the communications network that links them.
        - Communications infrastructure include wireless mesh technologies, such as IEEE 802.15.4, and wireless point-to-multipoint systems, such as IEEE 801.11ah.

5. Describe IOT World Forum (IOTWF) Standardized architecture.

Ans:

- A seven-layer IoT architectural reference model published by IoTWF architectural committee (Cisco, IBM, Rockwell Automation)
- Edge computing
- Data storage
- Access
- Using this reference model, we are able to achieve the following:
- Decompose the IoT problem into smaller parts
- Identify different technologies at each layer and how they relate to one another
- Define a system in which different parts can be provided by different vendors
- Have a process of defining interfaces that leads to interoperability
- Define a tiered security model that is enforced at the transition points between levels.

6. What is IOT? Explain in detail on genesis of IOT

Ans:

- Imagine a world where just about anything you can think of is online and communicating to other things and people in order to enable new services that enhance our lives.
- From self-driving drones delivering your grocery order to sensors in your clothing monitoring your health and so on.
- The world you know is set to undergo a major technological shift forward.
- This shift is known collectively as the Internet of Things (IoT).
- The basic premise and goal of IoT is to "connect the unconnected."
- This means that objects that are not currently joined to a computer network, namely the Internet, will be connected so that they can communicate and interact with people and other objects.
- IoT is a technology transition in which devices will allow us to sense and control the physical world by making objects smarter and connecting them through an intelligent network.
- When objects and machines can be sensed and controlled remotely across a network, a tighter integration between the physical world and computers is enabled.
- This allows for improvements in the areas of efficiency, accuracy, automation, and the enablement of advanced applications.

Genesis of IoT:

- The age of IoT is often said to have started between the years 2008 and 2009.
- The person credited with the creation of the term "Internet of Things" is Kevin Ashton.
- While working for Procter & Gamble in 1999, Kevin used this phrase to explain a new idea related to linking the company's supply chain to the Internet.
- "In the twentieth century, computers were brains without senses—they only knew what we told them."
- Computers depended on humans to input data and knowledge through typing, bar codes, and so on.
- IoT is changing this paradigm; in the twenty-first century, computers are sensing things for themselves.

7. Explain IOT Data management and Compute Stack.

Ans:

- The data generated by IoT sensors is one of the single biggest challenges in building an IoT system.
- In sensor networks, the vast majority of data generated is unstructured and of very little use on its own.
- In most cases, the processing location is outside the smart object.
- A natural location for this processing activity is the cloud.
- Smart objects need to connect to the cloud, and data processing is centralized.
- One advantage of this model is simplicity.
- Limitations.
- As data volume, the variety of objects connecting to the network, and the need for more efficiency increase, new requirements appear, and those requirements tend to bring the need for data analysis closer to the IoT system.
- Minimizing latency.
- Conserving network bandwidth.
- Increasing local efficiency.

Module-2

1. List and explain different types of sensors.

Ans:

- Active or passive:
    - Sensors can be categorized based on whether they produce an energy output and typically require an external power supply (active)or
    - Whether they simply receive energy and typically require no external power supply (passive).
- Invasive or non-invasive:
    - Sensors can be categorized based on whether a sensor is part of the environment it is measuring (invasive) or
    - External to it (non-invasive).
- Contact or no-contact:
    - Sensors can be categorized based on whether they require physical contact with what they are measuring (contact) or not (no-contact).
- Absolute or relative:
    - Sensors can be categorized based on whether they measure on an absolute scale (absolute) or based on a difference with a fixed or variable reference value (relative).
- Area of application:
    - Sensors can be categorized based on the specific industry or vertical where they are being used.
- How sensors measure:
    - Sensors can be categorized based on the physical mechanism used to measure sensory input (for example, thermoelectric, electrochemical, piezoresistive, optic, electric, fluid mechanic, photo elastic).

2. Briefly explain protocol stack utilization IEEE 802.15.4.

Ans:

- Wireless access technology for low-cost and low-data-rate devices that are powered or run-on batteries.
- This access technology enables easy installation while remaining both simple and flexible.
- IEEE 802.15.4 is commonly found in the following types of deployments:
    - Home and building automation
    - Automotive networks
    - Industrial wireless sensor networks
    - Interactive toys and remote controls

Protocol	Description
ZigBee	Promoted through the ZigBee Alliance, ZigBee defines upper-layer components (network through application) as well as application profiles. Common profiles include building automation, home automation, and healthcare. ZigBee also defines device object functions, such as device role, device discovery, network join, and security. For more information on ZigBee, see the ZigBee Alliance webpage, at www.zigbee.org. ZigBee is also discussed in more detail later in the next Section.
6LoWPAN	6LoWPAN is an IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers. RFCs document header compression and IPv6 enhancements to cope with the specific details of IEEE 802.15.4. (For more information on 6LoWPAN, see Chapter 5.)
ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol. In addition, it offers improvements to IP security. ZigBee IP is discussed in more detail later in this chapter.
ISA100.11a	ISA100.11a is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial Automation: Process Control and Related Applications." It is based on IEEE 802.15.4-2006, and specifications were published in 2010 and then as IEC 62734. The network and transport layers are based on IETF 6LoWPAN, IPv6, and UDP standards.
WirelessHART	WirelessHART, promoted by the HART Communication Foundation, is a protocol stack that offers a time-synchronized, self-organizing, and self-healing mesh architecture, leveraging IEEE 802.15.4-2006 over the 2.4 GHz frequency band. A good white paper on WirelessHART can be found at http://www.emerson.com/resource/blob/system-engineering-guidelines-iec-62591-wirelesshart--data-79900.pdf
Thread	Constructed on top of IETF 6LoWPAN/IPv6, Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home. Specifications are defined and published by the Thread Group at www.threadgroup.org.

3. List and explain the characteristics and attributes concerned when selecting and dealing with connecting smart objects.

Ans:

- The characteristics and attributes you should consider when selecting and dealing with connecting smart objects
  - Range:
    - How far does the signal need to be propagated?
    - That is, what will be the area of coverage for a selected wireless technology?

    - Should indoor versus outdoor deployments be differentiated?
  - Frequency Bands:
    - Radio spectrum is regulated by countries and/or organizations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission (FCC).
    - These groups define the regulations and transmission requirements for various frequency bands.
    - For example, portions of the spectrum are allocated to types of telecommunications such as radio, television, military, and so on.
  - Power Consumption:
    - Powered nodes and battery-powered nodes.
    - A powered node has a direct connection to a power source, and communications are usually not limited by power consumption criteria.
    - However, ease of deployment of powered nodes is limited by the availability of a power source, which makes mobility more complex.
  - Topology:
    - Among the access technologies available for connecting IoT devices, three main topology schemes are dominant: star, mesh, and peer-to-peer.
    - For long-range and short-range technologies, a star topology is prevalent.
    - Star topologies utilize a single central base station or controller to allow communications with endpoints.
  - Constrained-Node Networks:
    - Constrained-node networks are often referred to as low-power and lossy networks (LLNs).
    - Low power –battery powered constraints.
    - Lossy network - network performance may suffer from interference and variability due to harsh radio environments.

4. Define Sensors and actuators. Explain how they are interacting with the physical world.

Ans:

- Sensor:
  More specifically, a sensor measures some physical quantity and converts that measurement reading into a digital representation.
- Actuators:

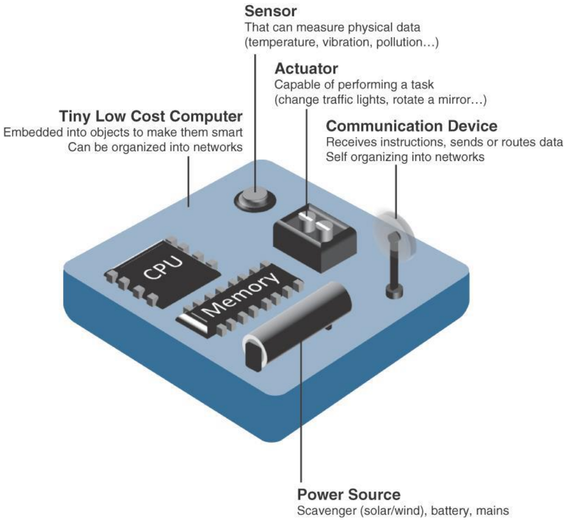
Actuators are natural complements to sensors and receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.

- Sensors are designed to sense and measure practically any measurable variable in the physical world.
- They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human).

5. Define Smart object, explain its characteristics.

Ans:

- Smart objects are, quite simply, the building blocks of IoT.
- They are what transform everyday objects into a network of intelligent objects that are able to learn from and interact with their environment in a meaningful way.
- The real power of smart objects in IoT comes from being networked together rather than being isolated as standalone objects.
- If a sensor is a standalone device that simply measures the humidity of the soil, it is interesting and useful, but it isn't revolutionary
- If that same sensor is connected as part of an intelligent network that is able to coordinate intelligently with actuators to trigger irrigation systems as needed based on those sensor readings, we have something far more powerful
- Extending that even further, imagine that the coordinated sensor/actuator set is intelligently interconnected with other sensor/actuator sets to further coordinate fertilization, pest control, and so on—and even communicate with an intelligent backend to calculate crop yield potential.
- A smart object, is a device that has, at a minimum, the following four defining characteristics.



6. What are constrained device and constrained node network? Classify them.

Ans:

Constrained Devices:

Class	Definition
Class 0	This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of Flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms. An example of a Class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging new unlicensed LPWA wireless technology.
Class 1	While greater than Class 0, the processing and code space characteristics (approximately 10 KB RAM and approximately 100 KB Flash) of Class 1 are still lower than expected for a complete IP stack implementation. They cannot easily communicate with nodes employing a full IP stack. However, these nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol (CoAP). This allows Class 1 nodes to engage in meaningful conversations with the network without the help of a gateway, and provides support for the necessary security functions. Environmental sensors are an example of Class 1 nodes.
Class 2	Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of Flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.

Constrained Node Network:

- IEEE 802.15.4 and 802.15.4g RF, IEEE 1901.2a PLC, LPWA, and IEEE 802.11ah access technologies.
- Constrained-node networks are often referred to as low-power and lossy networks (LLNs).
- Low power – battery powered constraints.
- Lossy network - network performance may suffer from interference and variability due to harsh radio environments.
- Protocols that can be used for constrained-node networks must be evaluated in the context of the following characteristics: data rate and throughput, latency and determinism, and overhead and payload.

7. With a neat diagram, explain how actuators and sensors interact with physical world. Classify actuators based on energy type.
Ans:

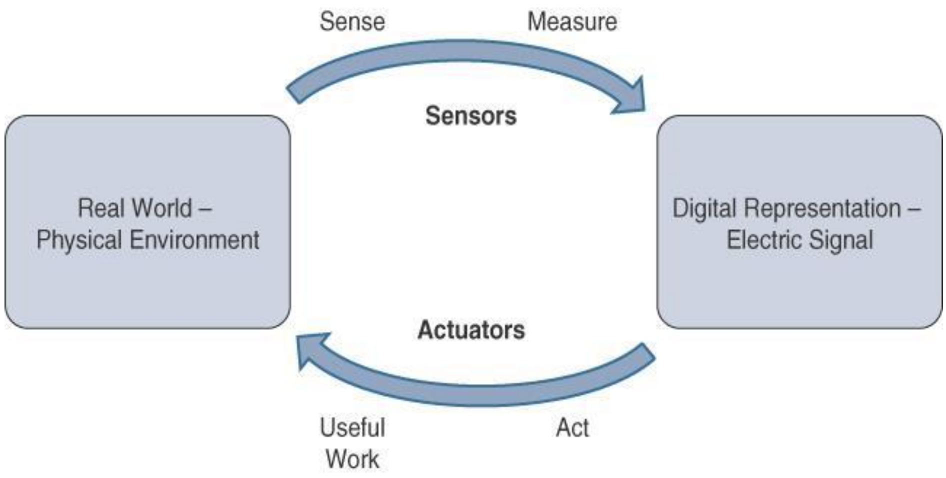


Fig: How sensors and actuators interact with the physical environment.

- In the diagram, it shows the symmetry and complementary nature of Sensors and Actuators.
- The IoT sensors sends and measures the physical world and signal their measurement as electrical signals are sent to some parts of the microcontroller and microprocessor.
- The interaction between sensors and actuators processor is a similar functionality in biological system. Basics of scientific fields like Robotics and Automation.

Type	**Examples**
Mechanical actuators	Lever, Screw jack, Hand crank
Electrical actuators	Thyristor, bipolar transistor, diode
Electromechanical actuators	AC motor, DC motor, step motor
Electromagnetic actuators	Electromagnet, liner solenoid
Hydraulic and pneumatic actuators	Hydraulic cylinder, pneumatic cylinder, piston, pressure control valves, air motors
Smart material actuators (includes thermal and magnetic actuators)	Shape memory alloy (SMA) , ion exchange fluid, magneto restrictive material, bimetallic strip, piezoelectric bimorph
Micro and Nano actuators	Electrostatic motor, microvalve, comb drive

Table: Classification of actuators based on energy type