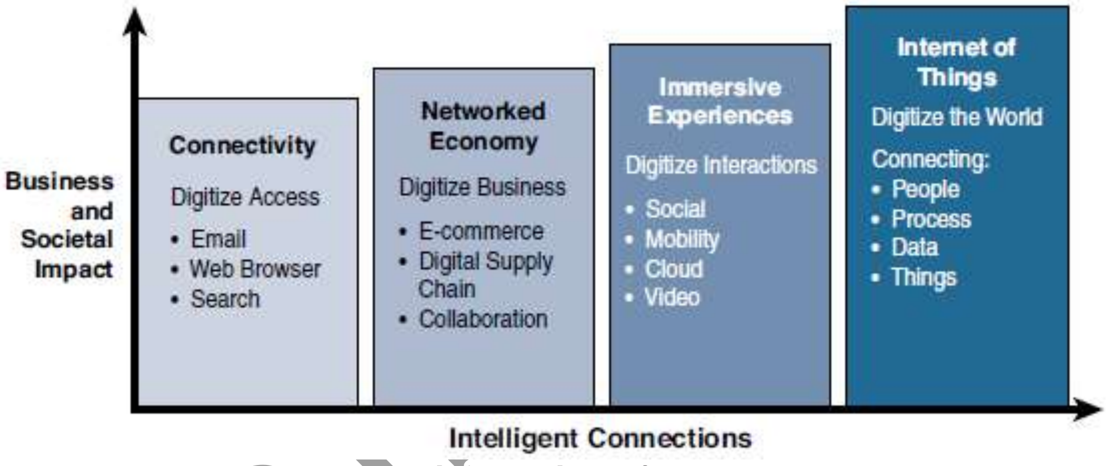
1. What is IOT? What are the evolutionary phases of IOT (Genesis of IOT)?

Answer: What is IOT?

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. It is an umbrella of various concepts, protocols, and technologies.

Evolutionary phases of IOT are as follows:



Evolutionary phases of IOT

a. **Connectivity (Digitize access):** This phase connected people to email, web services, and search so that information is easily accessed.

b. **Networked Economy (Digitize business):** This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.

c. **Immersive Experiences (Digitize interactions):** This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud.

d. **Internet of Things (Digitize the world):** This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences. It is connecting the unconnected.

\

2. List and explain some of the differences between IT and OT networks and their various challenges.

Answer: Differences between IT and OT networks with their challenges are:

Sl.no	Operational Technology (OT)	Information Technology (IT)
1	OT monitors and controls devices and processes on physical operational systems.	IT supports connections to the Internet along with related data and technology systems and is focused on the secure flow of data across an organization.
2	OT is responsible for the devices and processes acting on industrial equipment, such as factory machines, meters, actuators, electrical distribution automation devices, SCADA (supervisory control and data acquisition) systems,	IT organization is responsible for the information systems of a business, such as email, file and print services, databases,
3	Keep the business operating 24x7	Manage the computers, data, and employee communication system in a secure way
4	Priorities are Availability, Integrity, Security	Priorities are Security, Integrity, Availability
5	Types of Monitoring, control, and supervisory data	Types of Voice, video, transactional, and bulk data
6	Controlled physical access to devices	Devices and users authenticated to the network
7	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible
8	Network upgrades (software or hardware) only during operational maintenance windows	Network upgrades often requires an outage window when workers are not onsite; impact can be mitigated
9	Security vulnerability are Low: OT networks are isolated and often use proprietary protocols	Security vulnerability are high: Continual patching of hosts is required, and the network is connected to Internet and requires vigilant protection

3. List and explain a few of the most significant challenges and problems that IoT is currently facing.

Answer:

Scale: scale of IT networks can be large; the scale of OT can be several orders of magnitude larger.

Security: With more “things” becoming connected with other “things” and people, security is an increasingly complex issue for IoT. 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.

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. Data has monetary value.

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.

Interoperability: 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.

4. Discuss IOT and Digitization.

Answer:

a. IoT focuses on connecting “things,” such as objects and machines, to a computer network, such as the Internet.

b. Analysis of this data can lead to significant changes to the locations of product displays and advertising.

c. Digitization encompasses the connection of “things” with the data they generate and the business insights that result.

d. Digitization is the conversion of information into a digital format. In the context of IoT, digitization brings together things, data, and business process to make networked connections more relevant and valuable.

e. Digitization is a differentiator for the businesses, and IoT is a prime enabler of digitization.

5. Explain the benefits of IOT and their impact.

Answer:

Connected Roadways: Connected roadways is the term associated with both the driver and driverless cars fully integrating with the surrounding transportation infrastructure. Automobiles are produced with thousands of sensors, to measure everything from fuel consumption to location to the entertainment your family is watching during the ride. As automobile manufacturers strive to reinvent the driving experience, these sensors are becoming IP-enabled to allow easy communication with other systems both inside and outside the car.

Current Challenges Being Addressed by Connected Roadways are

i) Safety: IoT and the enablement of connected vehicle technologies will empower drivers with the tools they need to anticipate potential crashes and significantly reduce the number of lives lost each year.

ii) Mobility: Connected vehicle mobility applications can enable system operators and drivers to make more informed decisions, which can, in turn, reduce travel delays.

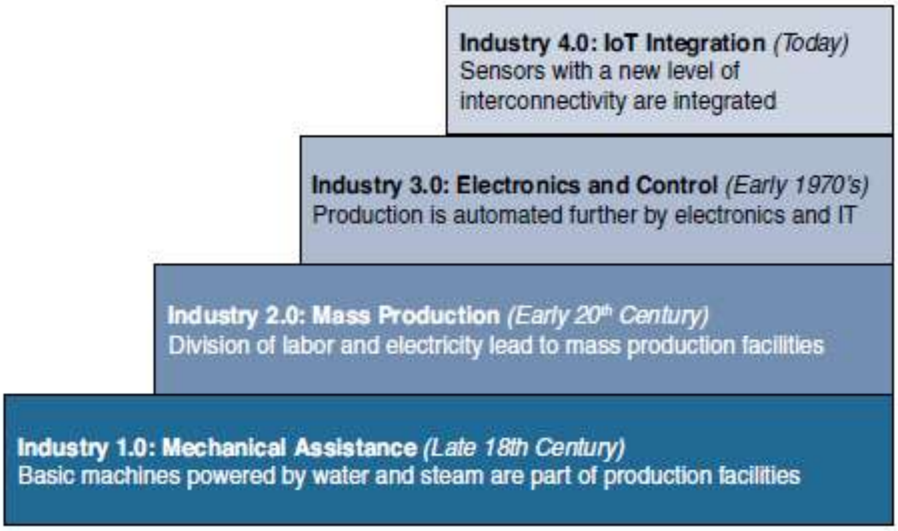
iii) Environment: Connected vehicle environmental applications will give all travellers the real-time information they need to make "green" transportation choices.

Example: Google's Self-Driving Car. IoT is going to allow self-driving vehicles to better interact with the transportation system around them through bidirectional data exchanges while also providing important data to the riders.

Connected Factory: The main challenges facing manufacturing in a factory environment today include the following:

i) Accelerating new product and service introductions to meet customer and market opportunities.
ii) Increasing plant production, quality, and uptime while decreasing cost.
iii) Mitigating unplanned downtime.
iv) Securing factories from cyber threats.
v) Improving worker productivity and safety

IOT can provide solutions to these challenges. A convergence of factory-based operational technologies and architectures with global IT networks is referred to as the connected factory. The devices on the plant floor will become smarter in their ability to transmit and receive large quantities of real-time informational and diagnostic data. With IoT and a connected factory solution, true "machine-to-people" connections are implemented to bring sensor data directly to operators on the floor via mobile devices. Time is no longer wasted moving back and forth between the control rooms and the plant floor.


Industry 4.0: IoT Integration (Today)
Sensors with a new level of interconnectivity are integrated
Industry 3.0: Electronics and Control (Early 1970's)
Production is automated further by electronics and IT
Industry 2.0: Mass Production (Early 20th Century)
Division of labor and electricity lead to mass production facilities
Industry 1.0: Mechanical Assistance (Late 18th Century)
Basic machines powered by water and steam are part of production facilities

The four industrial revolutions

Smart Connected Buildings: The function of a building is to provide a work environment that keeps the workers comfortable, efficient, and safe. To keep workers safe, the fire alarm and suppression system needs to be carefully managed. Intelligent systems for modern buildings are being deployed and improved for each of these functions. Sensors are often used to control the heating, ventilation, and air-conditioning (HVAC) system. Temperature sensors are spread throughout the building and are used to influence the building management system's (BMS's) control of air flow into a room. Another promising IoT technology in the smart connected building, and one that is seeing widespread adoption, is the "digital ceiling." The digital ceiling is more than just a lighting control system. This technology encompasses several of the building's different networks—including lighting, HVAC, blinds, CCTV (closed-circuit television), and security systems—and combines them into a single IP network. In a digital ceiling environment, every lighting fixture is directly network attached.

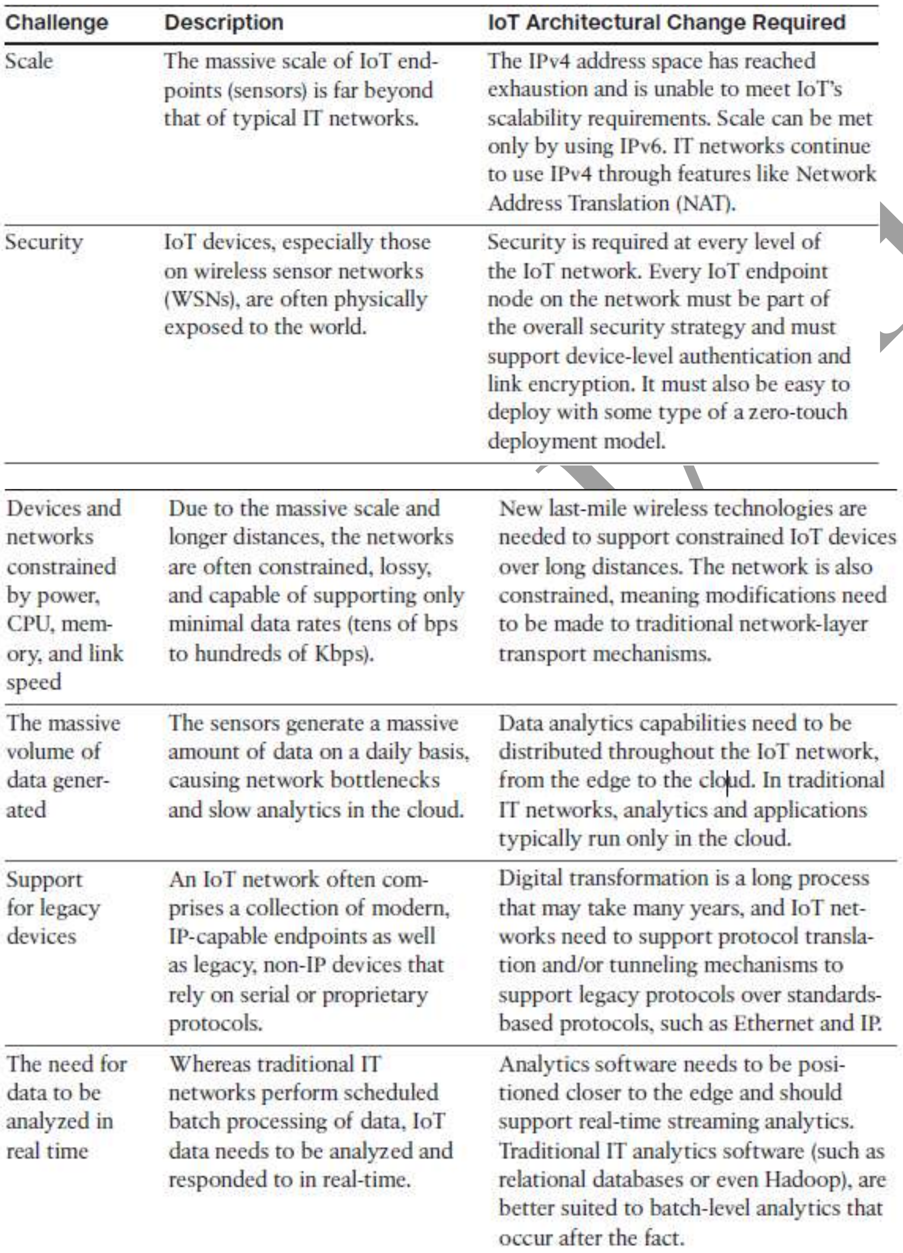
Smart Creatures: Sensors can be placed on animals and even insects just as easily as on machines. IoT with respect to animals focuses on what is often referred to as the "connected cow." A sensor is placed in a cow's ear. The sensor monitors various health aspects of the cow as well as its location and transmits the data wirelessly for analysis by the farmer. Another application of IoT to organisms involves the placement of sensors on roaches. An electronic backpack attaches to a roach. This backpack communicates with the roach through parts of its body. The electronic backpack uses wireless communication to a controller and can be "driven" remotely.

6. List and explain the requirements driving specific architectural Changes for IoT.

   OR

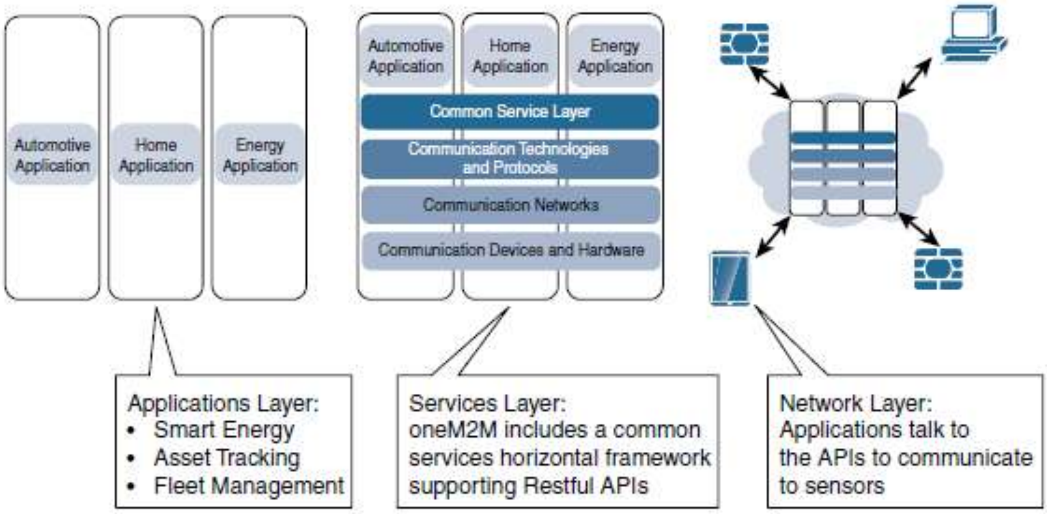
   List and explain the Drivers behind New Network Architectures.

Answer:



Challenge	Description	IoT Architectural Change Required
Scale	The massive scale of IoT endpoints (sensors) is far beyond that of typical IT networks.	The IPv4 address space has reached exhaustion and is unable to meet IoT's scalability requirements. Scale can be met only by using IPv6. IT networks continue to use IPv4 through features like Network Address Translation (NAT).
Security	IoT devices, especially those on wireless sensor networks (WSNs), are often physically exposed to the world.	Security is required at every level of the IoT network. Every IoT endpoint node on the network must be part of the overall security strategy and must support device-level authentication and link encryption. It must also be easy to deploy with some type of a zero-touch deployment model.
Devices and networks constrained by power, CPU, memory, and link speed	Due to the massive scale and longer distances, the networks are often constrained, lossy, and capable of supporting only minimal data rates (tens of bps to hundreds of Kbps).	New last-mile wireless technologies are needed to support constrained IoT devices over long distances. The network is also constrained, meaning modifications need to be made to traditional network-layer transport mechanisms.
The massive volume of data generated	The sensors generate a massive amount of data on a daily basis, causing network bottlenecks and slow analytics in the cloud.	Data analytics capabilities need to be distributed throughout the IoT network, from the edge to the cloud. In traditional IT networks, analytics and applications typically run only in the cloud.
Support for legacy devices	An IoT network often comprises a collection of modern, IP-capable endpoints as well as legacy, non-IP devices that rely on serial or proprietary protocols.	Digital transformation is a long process that may take many years, and IoT networks need to support protocol translation and/or tunneling mechanisms to support legacy protocols over standards-based protocols, such as Ethernet and IP.
The need for data to be analyzed in real time	Whereas traditional IT networks perform scheduled batch processing of data, IoT data needs to be analyzed and responded to in real-time.	Analytics software needs to be positioned closer to the edge and should support real-time streaming analytics. Traditional IT analytics software (such as relational databases or even Hadoop), are better suited to batch-level analytics that occur after the fact.

7. With a neat diagram explain the oneM2M IoT Standardized Architecture.



Main elements of oneM2M IoT Standardized Architecture.

The oneM2M architecture divides IoT functions into three major domains: the application layer, the services layer, and the network layer.

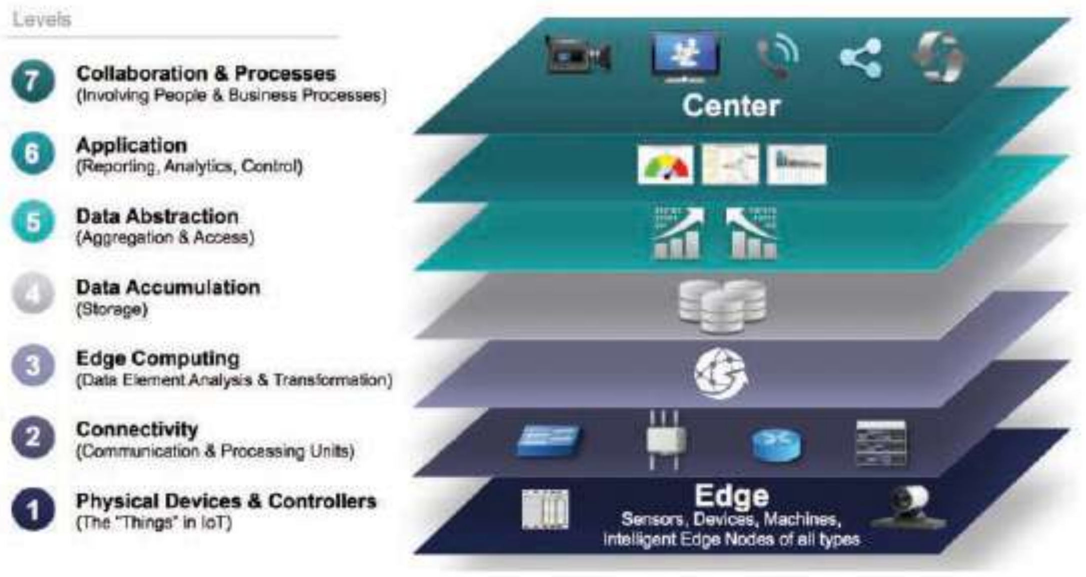
Applications layer: The oneM2M architecture gives major attention to connectivity between devices and their applications. This domain includes the application-layer protocols and attempts to standardize northbound API definitions for interaction with business intelligence (BI) systems. Applications tend to be industry-specific and have their own sets of data models, and thus they are shown as vertical entities.

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.

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. Embodiments of this communications infrastructure include wireless mesh technologies, such as IEEE 802.15.4, and wireless point-to-multipoint systems, such
as IEEE 801.11ah.

.

8. With a neat block diagram illustrate The IoT World Forum (IoTWF) Standardized Architecture.


Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types

IoT Reference Model Published by the IoT World Forum

Layer 1: Physical Devices and Controllers Layer: The first layer of the IoT Reference Model is the physical devices and controllers layer. This layer is home to the “things” in the Internet of Things, including the various endpoint devices and sensors that send and receive information.

Layer 2: Connectivity Layer: In the second layer of the IoT Reference Model, the focus is on connectivity. The most important function of this IoT layer is the reliable and timely transmission of data. this includes transmissions between Layer 1 devices and the network and between the network and information processing that occurs at Layer 3

Layer 2 Functions:

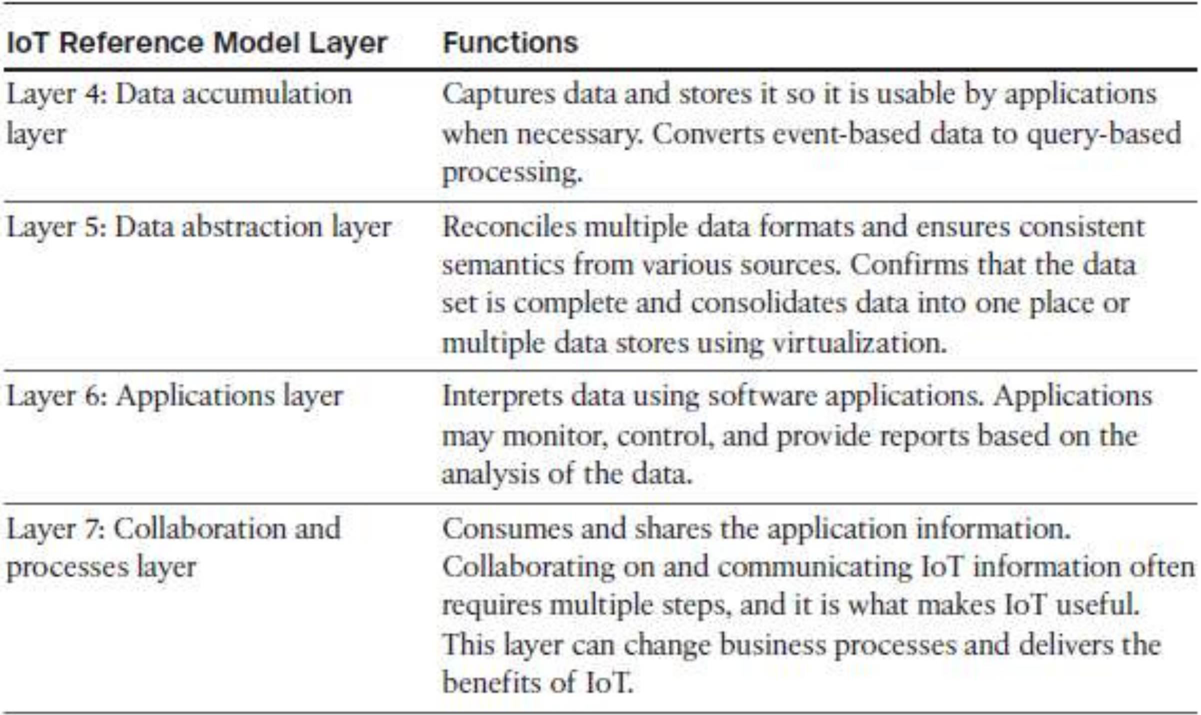
- Communications between Layer 1 Devices
- Reliable Delivery of Information across the Network
- Switching and Routing
- Translation between Protocols
- Network Level Security

Layer 3: Edge Computing Layer: At this layer, the emphasis is on data reduction and converting network data flows into information that is ready for storage and processing by higher layers.

Layer 3 Functions:

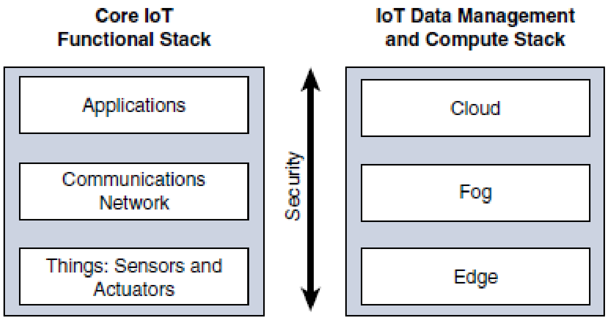
- Evaluate and Reformat Data for Processing at Higher Levels
- Filter Data to Reduce Traffic Higher Level Processing
- Assess Data for Alerting, Notification, or Other Actions

Upper Layers: Layers 4–7: The upper layers deal with handling and processing the IoT data generated by the bottom layer.



IoT Reference Model Layer	Functions
Layer 4: Data accumulation layer	Captures data and stores it so it is usable by applications when necessary. Converts event-based data to query-based processing.
Layer 5: Data abstraction layer	Reconciles multiple data formats and ensures consistent semantics from various sources. Confirms that the data set is complete and consolidates data into one place or multiple data stores using virtualization.
Layer 6: Applications layer	Interprets data using software applications. Applications may monitor, control, and provide reports based on the analysis of the data.
Layer 7: Collaboration and processes layer	Consumes and shares the application information. Collaborating on and communicating IoT information often requires multiple steps, and it is what makes IoT useful. This layer can change business processes and delivers the benefits of IoT.

9. With the help of a diagram explain extended simplified IOT architecture.



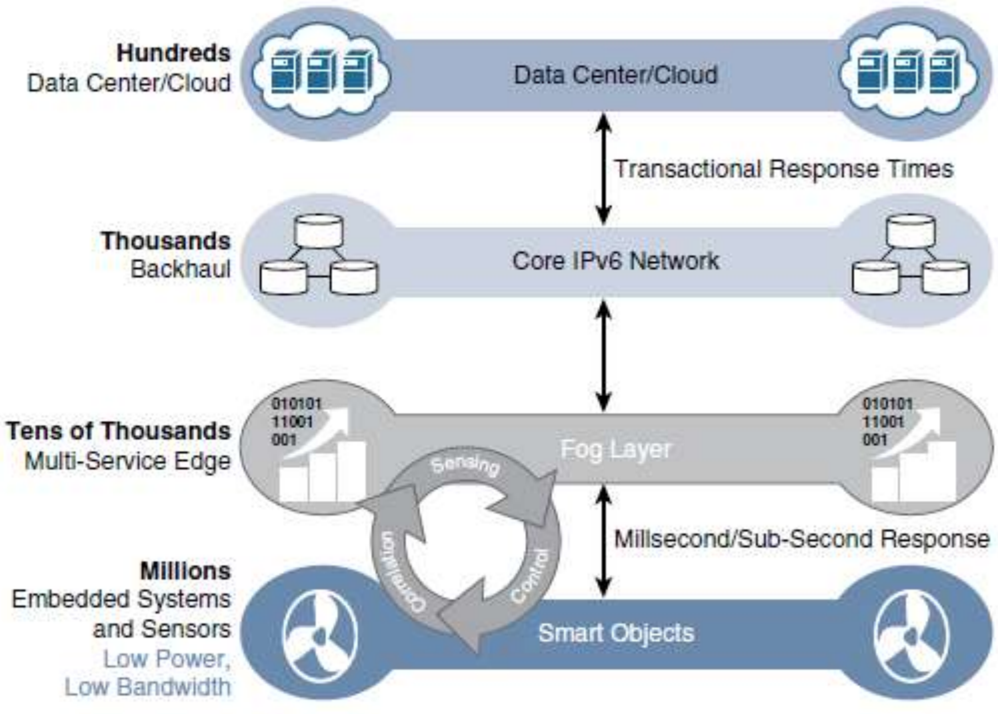
a. This framework is presented as two parallel stacks: The IoT Data Management and Compute Stack and the Core IoT Functional Stack.
b. IoT model includes core layers including “things,” a communications network, and applications.
c. The framework separates the core IoT and data management into parallel and aligned stacks, allowing to carefully examine the functions of both the network and the applications at each stage of a complex IoT system.
d. The presentation of the Core IoT Functional Stack in three layers is meant to simplify the IoT architecture into its most foundational building blocks.
e. Things layer consists of sensors and actuators, homogeneous or heterogeneous.
f. The network communications layer needs offer gateway and backhaul technologies, and ultimately brings the data back to a central location for analysis and processing.

10. Write a short note on The IoT Data Management and Compute Stack with Fog Computing.

IOT tend to bring the need for data analysis closer to the IoT system. These new requirements include Minimizing latency, Conserving network bandwidth, Increasing local efficiency. Several data-related problems need to be addressed like

- Bandwidth in last-mile IoT networks is very limited.
- Latency can be very high
- Network backhaul from the gateway can be unreliable
- The volume of data transmitted over the backhaul can be high
- Big data is getting bigger.

The solution to the challenges mentioned in the previous section is to distribute data management throughout the IoT system, as close to the edge of the IP network as possible. The best-known embodiment of edge services in IoT is fog computing. Any device with computing, storage, and network connectivity can be a fog node.



The IoT Data Management and Compute Stack with Fog Computing

An advantage of this structure is that the fog node allows intelligence gathering and control from the closest possible point, and in doing so, it allows better performance over constrained networks. Fog services are typically accomplished very close to the edge device, sitting as close to the IoT endpoints as possible. One significant advantage of this is that the fog node has contextual awareness of the sensors it is managing because of its geographic proximity to those sensors. In this way, it is performing distributed analytics such that the volume of data sent upstream is greatly reduced and is much more useful to application and analytics servers residing in the cloud.

The defining characteristic of fog computing are as follows:

Contextual location awareness and low latency: The fog node sits as close to the IoT endpoint as possible to deliver distributed computing.

Geographic distribution: The services and applications targeted by the fog nodes demand widely distributed deployments.

Deployment near IoT endpoints: Fog nodes are typically deployed in the presence of a large number of IoT endpoints.

Wireless communication between the fog and the IoT endpoint: Although it is possible to connect wired nodes, the advantages of fog are greatest when dealing with a large number of endpoints, and wireless access is the easiest way to achieve such scale.

Use for real-time interactions: Important fog applications involve real-time interactions rather than batch processing. Pre-processing of data in the fog nodes allows upper-layer applications to perform batch processing on a subset of the data.