Chapter 1.

What is IoT

Internet of Things (IoT) "connect the unconnected" 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.

Instead of viewing IoT as a single technology domain, it is good to view it as an umbrella of various concepts, protocols, and technologies, all of which are at times somewhat dependent on a particular industry.

Genesis of IoT

The IoT started between the years 2008 and 2009 where the number of devices/things connected to the Internet than the people. 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 and he said IOT adds sense to computer.

It is widely accepted that IoT is a major technology shift, but what is its scale and importance? Where does it fit in the evolution of the Internet? As shown in Figure 1-1, the evolution of the Internet can be categorized into four phases. Each of these phases has had a profound impact on our society and our lives. These four phases are further defined in Table 1-1.

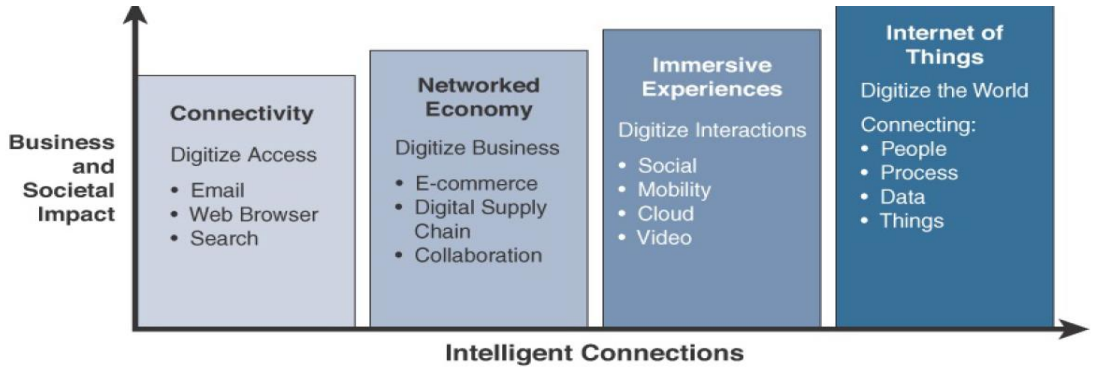

Figure1.1*Evolutionary Phases of the Internet*

Internet Phase	Definition
Connectivity (Digitize access)	This phase connected people to email, web services, and search so that information is easily accessed.
Networked Economy (Digitize business)	This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.
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.
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.

Table 1-1 *Evolutionary Phases of the Internet*

- The first phase, Connectivity, began in the mid-1990s.It may be hard to connect to Internet In the beginning, email and getting on the Internet were luxuries for universities and corporations. the average person working online basic connectivity often seemed like a small miracle.

- The second phase focus was now on leveraging connectivity for efficiency and profit. This inflection marked the beginning of the Internet evolution, called the Networked Economy. e-commerce and digitally connected supply chains became the rage Vendors and suppliers became closely interlinked with producers, and online shopping experienced incredible growth. The victims of this shift were traditional brick-and-mortar retailers. The economy itself became more digitally intertwined as suppliers, vendors, and consumers all became more directly connected.

- The third phase, Immersive Experiences, is characterized by the emergence of social media, collaboration, and widespread mobility on a variety of devices. Connectivity is now pervasive In essence, person-to-person interactions have become digitized.

- Machines and objects in this phase connect with other machines and objects, along with humans. Business and society have already started down this path and are experiencing huge increases in data and knowledge. In turn, this is now leading to previously unrecognized insights, along with increased automation and new process efficiencies.

IoT and Digitization

- Digitization, as defined in its simplest form, is the conversion of information into a digital format.
- used interchangeably
- IoT focuses on connecting “things,” such as objects and machines, to a computer network, such as the Internet.
- 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.

For example, in a shopping mall where Wi-Fi location tracking has been deployed, the "things" are the Wi-Fi devices

For example The digitization of photography has completely changed our experience when it comes to capturing images digital cameras either standalone devices or built into their mobile phones

- digitization includes the video rental industry and transportation
- In the context of IoT, digitization brings together things, data, and business process to make networked connections more relevant and valuable. A good example of this that many people can relate to is in the area of home automation with popular products, such as Nest.
- Nest, sensors determine your desired climate settings and also tie in other smart objects, such as smoke alarms, video cameras, and various third-party devices.
- Companies today look at digitization as a differentiator for their businesses, and IoT is a prime enabler of digitization. Smart objects and increased connectivity drive digitization, and this is one of the main reasons that many companies, countries, and governments are embracing this growing trend.

IoT Impact

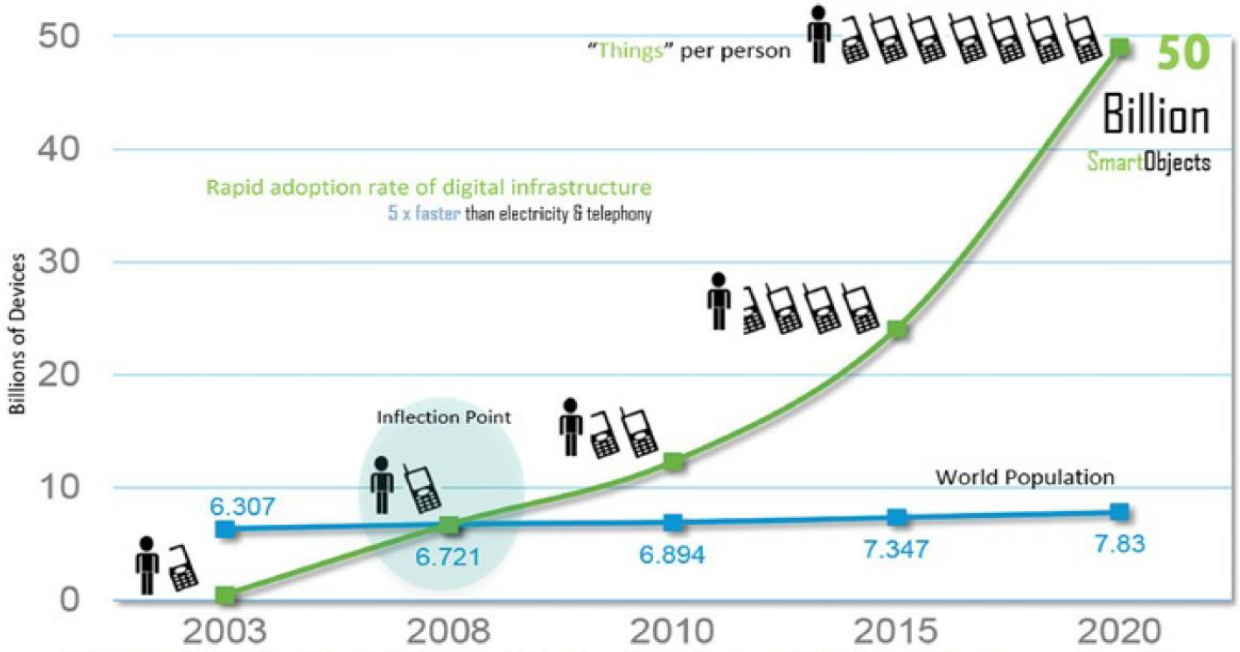

Figure 1-2 *The Rapid Growth in the Number of Devices Connected to the Internet*

- Cisco Systems predicts that by 2020, this number will reach 50 billion. further estimates that these new connections will lead to $19 trillion in profits and cost savings
- Managing and monitoring smart objects using real-time connectivity enables a whole new level of data-drive decision making.
- Google's self-driving car, IoT is also a necessary component for implementing a fully connected transportation infrastructure.
-
-

Connected Roadways

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

Figure 1-3 *Google's Self-Driving Car*

- **I**n self Driving car Basic sensors reside in cars. They monitor oil pressure, tire pressure, temperature, and other operating conditions, and provide data around the core car functions.
- the driver can access this data while also controlling the car using equipment such as a steering wheel, pedals, and so on.
- automobiles produced with thousands of sensors, to measure everything from fuel consumption to location to the entertainment your family is watching during the ride
- sensors are becoming IP-enabled to allow easy communication with other systems both inside and outside the car and allow vehicles to "talk" to other vehicles, traffic signals, school zones, and other elements of the transportation infrastructure

connected roadways challenges

Challenge	Supporting Data
Safety	According to the US Department of Transportation, 5.6 million crashes were reported in 2012 alone, resulting in more than 33,000 fatalities. 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.
Mobility	More than a billion cars are on the roads worldwide. Connected vehicle mobility applications can enable system operators and drivers to make more informed decisions, which can, in turn, reduce travel delays. Congestion causes 5.5 billion hours of travel delay per year, and reducing travel delays is more critical than ever before. In addition, communication between mass transit, emergency response vehicles, and traffic management infrastructures help optimize the routing of vehicles, further reducing potential delays.
Environment	According to the American Public Transportation Association, each year transit systems can collectively reduce carbon dioxide (CO_2) emissions by 16.2 million metric tons by reducing private vehicle miles. Connected vehicle environmental applications will give all travelers the real-time information they need to make "green" transportation choices.

Sources: Traffic Safety Facts, 2010; National Highway Traffic Safety Administration, June 2012; and WHO Global Status Report on Road Safety, 2013.

Table 1-2 *Current Challenges Being Addressed by Connected Roadways*

IoT-connected roadways, a concept known as Intersection Movement Assist (IMA)

- This application warns a driver (or triggers the appropriate response in a self-driving car) when it is not safe to enter an intersection due to a high probability of a collision—perhaps because another car has run a stop sign or strayed into the wrong lane.

Figure 1-4 *Application of Intersection Movement Assist*

- With automated vehicle tracking, a vehicle's location is used for notification of arrival times, theft prevention, or highway assistance
- Cargo management provides precise positioning of cargo

- Road weather communications use sensors and data from satellites, roads, and bridges to warn vehicles of dangerous conditions or inclement weather on the current route.

- fully connected car will generate more than 25 gigabytes of data per hour, much of which will be sent to the cloud.

Figure 1-5 provides an overview of the sort of sensors and connectivity that you will find in a connected car.

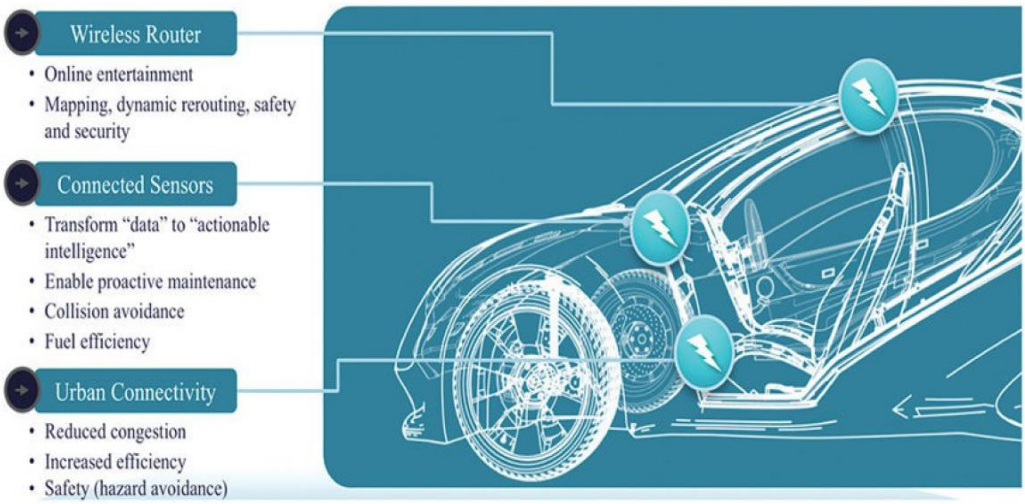

Figure 1-5 *The Connected Car*

- the data generated by your car needs to be handled in a secure and reliable way, which must provide authentication and verification of the driver and car, and it needs to be highly available.
- Automobile manufacturers can collect information from sensors to better understand how the cars are being driven, details that will help them build better cars in the future

- car sensors will be able to interact with third-party applications, such as GPS/maps

- Internet-based entertainment, including music, movies.

- the IoT data broker. Imagine the many different types of data generated by an automobile and the plethora of different parties interested in this data.

- the data generated by the car can be separated and sold selectively by the data broker for example, tire companies will pay for information from sensors related to your tires

- advancements in roadway fibre-optic sensing technology is now able to record not only how many cars are passing but their speed and type

Connected Factory

- traditional factories have been operating at a disadvantage

The main challenges facing manufacturing in a factory environment today include the following.

- Accelerating new product and service introductions to meet customer and market opportunities
- Increasing plant production, quality, and uptime while decreasing cost
- Mitigating unplanned downtime (which wastes, on average, at least 5% of production)
- Securing factories from cyber threats
- Decreasing high cabling and re-cabling costs (up to 60% of deployment costs)
- Improving worker productivity and safety

A convergence of factory-based operational technologies and architectures with global IT networks is starting to occur, and this is referred to as the *connected factory*.

with IoT, sensors not only become more advanced but also attain a new level of connectivity. They are smarter and gain the ability to communicate, mainly using the Internet Protocol (IP) over an Ethernet infrastructure.

- the devices on the plant floor are becoming smarter in their ability to transmit and receive large quantities of real-time informational and diagnostic data. Ethernet connectivity is becoming pervasive and spreading beyond just the main controllers in a factory to devices such as the robots on the plant floor. In addition, more IP-enabled devices, including video cameras, diagnostic smart objects, and even personal mobile devices, are being added to the manufacturing environment.
- "machine-to people" connections are implemented to bring sensor data directly to operators on the floor via mobile devices.
- a real-time location system (RTLS) utilizes small and easily deployed Wi-Fi RFID tags that attach to virtually any material and provide real-time location and status.

Industrial Revolution

- The first Industrial Revolution occurred in Europe in the late eighteenth century, with the application of steam and water to mechanical production.
- The second Industrial Revolution, which took place between the early 1870s and the early twentieth century, saw the introduction of the electrical grid and mass production.
- The third revolution came in the late 1960s/early 1970s, as computers and electronics began to make their mark on manufacturing and other industrial systems.
- The fourth Industrial Revolution is happening now, and the Internet of Things is driving it.

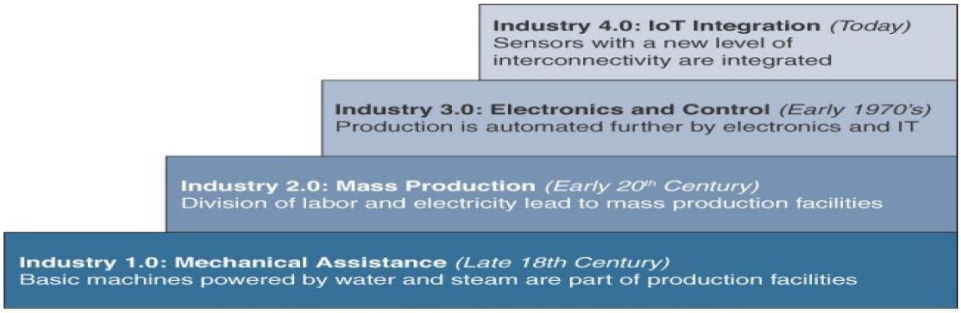

Figure 1-6 *The Four Industrial Revolutions*

Smart Connected Buildings

- To keep building and people safe, the fire alarm and suppression system needs to be carefully managed, as do the door and physical security alarm systems.
- intelligent systems for modern buildings are being deployed and improved for each of these functions
- Buildings are beginning to deploy sensors throughout the building to detect occupancy. motion sensors or sensors tied to video cameras automatically shut the lights off when everyone has left.
- sensors are often used to control the heating, ventilation, and air conditioning (HVAC) system, building management system's (BMS's)
- In workplace floor efficiency and usage evidence tends to be anecdotal at best. When smart building sensors and occupancy detection are combined with the power of data analytics it becomes easy to demonstrate floor plan usage and prove your case.
- Alternatively, the building manager can use a similar approach to see where floor is not used efficiently its empowered by IOT

- connect these systems into a single framework the building automation system (BAS)

- Bring together heterogeneous systems, they need to converge at the network layer and support a common services layer that allows application integration. CISCO and other companies convergence of voice and video onto single IP networks that were shared with other IT applications.
- For example, the de facto communication protocol responsible for building automation is known as BACnet (Building Automation and Control Network). the BACnet protocol defines a set of services that allow Ethernet based communication between building devices such as HVAC.
- intersection point to the IP network (which is run by the IT department) through the use of a gateway device.

- BACnet/IP has been defined to allow the "things" in the building network to communicate over IP, thus allowing closer consolidation of the building management system on a single network.

FIG 1

- 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.
- Central to digital ceiling technology is the lighting system. As you are probably aware, the lighting market is currently going through a major shift toward light emitting diodes (LEDs). Compared to traditional lighting, LEDs offer lower energy consumption and far longer life. The lower power requirements of LED fixtures allow them to run on Power over Ethernet (PoE), permitting them to be connected to standard network switches.
- The energy savings value of PoE-enabled LED lighting in the ceiling is clear. However, having an IP-enabled sensor device in the ceiling at every point people may be present opens an entirely new set of possibilities. For example, most modern LED ceiling fixtures support occupancy Sensors.
- occupancy-sensing technologies, including Bluetooth low energy (BLE) and Wi-Fi. The science here is simple: Because almost every person these days carries a smart device that supports BLE and Wi-Fi, all the sensor has to do is detect BLE or Wi-Fi beacons from a nearby device.

Smart Creatures

- One of the most well-known applications of IoT with respect to animals focuses on what is often referred to as the "connected cow" a sensor that 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.

- environmental factors may be affecting the herd as a whole and about changes in diet. This enables early detection of disease as cows tend to eat less days before they show symptoms. These sensors even allow the detection of pregnancy in cows.
- IoT-enabled roaches could make a life-saving difference in disaster situations. Researchers at North Carolina State University are working with Madagascarm hissing cockroaches in the hopes of helping emergency personnel rescue survivors after a disaster
- an electronic backpack attaches to a roach. This backpack communicates with the roach through parts of its body. Low-level electrical pulses to an antenna on one side makes the roach turn to the opposite side because it believes it is encountering an obstacle. The cerci of the roach are sensory organs on the abdomen that detect danger through changing air currents. When the backpack stimulates the cerci, the roach moves forward because it thinks a predator is approaching. The electronic backpack uses wireless communication to a controller and can be "driven" remotely.

Convergence of IT and OT

Criterion	Industrial OT Network	Enterprise IT Network
Operational focus	Keep the business operating 24x7	Manage the computers, data, and employee communication system in a secure way
Priorities	1. Availability 2. Integrity 3. Security	1. Security 2. Integrity 3. Availability
Types of data	Monitoring, control, and supervisory data	Voice, video, transactional, and bulk data
Security	Controlled physical access to devices	Devices and users authenticated to the network
Implication of failure	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible
Network upgrades (software or hardware)	Only during operational maintenance windows	Often requires an outage window when workers are not onsite; impact can be mitigated
Security	Low: OT networks are	High: continual patching of hosts is

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

Chapter 2. IoT Network Architecture and Design

This chapter examines some of the unique challenges posed by IoT networks and how these challenges have driven new architectural models

Drivers Behind New Network Architectures: OT networks drive core industrial business operations. They have unique characteristics and constraints that are not easily supported by traditional IT network architectures.

Comparing IoT Architectures: Several architectures have been published for IoT, including those by ETSI and the IoT World Forum. This section discusses and compares these architectures.
A Simplified IoT Architecture: While several IoT architectures exist, a simplified model is presented in this section to lay a foundation for rest of the material discussed in this book.
The Core IoT Functional Stack: The IoT network must be designed to support its unique requirements and constraints. This section provides an overview of the full networking stack, from sensors all the way to the applications layer.
IoT Data Management and Compute Stack: This section introduces data management, including storage and compute resource models for IoT, and involves edge, fog, and cloud computing.

Drivers Behind New Network Architectures

The difference between IT and IoT networks is much like the difference between residential architecture and stadium architecture.

The key difference between IT and IoT is the data. While IT systems are mostly concerned with reliable and continuous support of business applications such as email, web, databases, CRM systems, and so on, IoT is all about the data generated by sensors and how that data is used. The essence of IoT architectures thus involves how the data is transported, collected, analysed, and ultimately acted upon.

Challenge	Description	IoT Architectural Change Required
Scale	The massive scale of IoT end-points (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.

Table 2-1 *IoT Architectural Drivers*

.

Scale

The scale of a typical IT network is on the order of several thousand devices—typically printers, mobile wireless devices, laptops, servers, and so on. the scale of a network goes from a few thousand endpoints to a few million. IoT introduces a model where an average-sized utility, factory, transportation system, or city could easily be asked to support a network of this scale. Based on scale requirements of this order, IPv6 is the natural foundation for the IoT network layer.

Security

The frequency and impact of cyber attacks in recent years has increased dramatically. Protecting corporate data from intrusion and theft is one of the main functions of the IT department. IT departments go to great lengths to protect servers, applications, and the network, setting up defense-in-depth models with layers of security designed to protect the cyber crown jewels of the corporation. However, despite all the efforts mustered to protect networks and data, hackers still find ways to penetrate trusted networks.

In IT networks firewall It would be unthinkable to position critical IT endpoints outside the firewall, visible to anyone who cared to look. IoT endpoints are often located in wireless sensor networks that use unlicensed spectrum and are not only visible to the world through a spectrum analyser but often physically accessible and widely distributed in the field.

IoT systems require consistent mechanisms of authentication, encryption, and intrusion prevention techniques that understand the behaviour of industrial protocols and can respond to attacks on critical infrastructure.

IoT systems must:

- Be able to identify and authenticate all entities involved in the IoT service (that is, gateways, endpoint devices, home networks, roaming networks, service platforms)
- Ensure that all user data shared between the endpoint device and back-end applications is encrypted
- Comply with local data protection legislation so that all data is protected and stored correctly
- Utilize an IoT connectivity management platform and establish rules-based security policies so immediate action can be taken if anomalous behaviour is detected from connected devices
- Take a holistic, network-level approach to security

Constrained Devices and Networks

Most IoT sensors are designed for a single job, and they are typically small and inexpensive. This means they often have limited power, CPU, and memory, and they transmit only when there is something important. Because of the massive scale of these devices and the large, uncontrolled environments where they are usually deployed, the networks that provide connectivity also tend to be very lossy and support very low data rates.

Data

- IoT devices generate a mountain of data it is what enables businesses to deliver new IoT services that enhance the customer experience, reduce cost, and deliver new revenue opportunities.
- most IoT-generated data is unstructured, the insights it provides through analytics can revolutionize processes and create new business models.
- IoT systems are designed to stagger data consumption throughout the architecture, both to filter and reduce unnecessary data going upstream and to provide the fastest possible response to devices when necessary.

Legacy Device Support

- Supporting legacy devices in an IT organization is not usually a big problem. If someone's computer or operating system is outdated, simply upgrades. In OT systems, end devices are likely to be on the network for a very long time—sometimes decades. As IoT networks are deployed, they need to support the older devices already present on the network, as well as devices with new capabilities.
- the IoT network must either be capable of some type of protocol translation or use a gateway device to connect these legacy endpoints to the IoT network.

Comparing IoT Architectures

Two of the best-known architectures are those supported by one M2M and the IoT World Forum (IoTWF)

The oneM2M IoT Standardized Architecture

- European Telecommunications Standards Institute (ETSI) created the M2M Technical Committee in 2008. The goal of this committee was to create a common architecture.
- One of the greatest challenges in designing an IoT architecture is dealing with the heterogeneity of devices, software, and access methods. One M2M is developing standards that allow interoperability at all levels of the IoT stack.
- The oneM2M architecture divides IoT functions into three major domains: the application layer, the services layer, and the network layer.

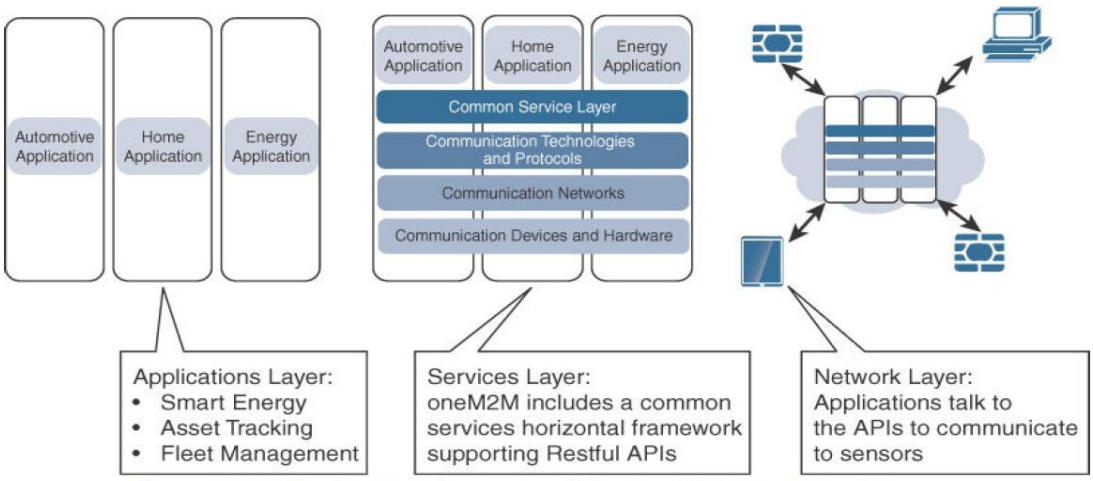

Figure 2-1 *The Main Elements of the oneM2M IoT Architecture*

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. 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,

develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software nodes, and rely upon connecting the myriad of devices in the field area network to M2M application servers, which typically reside in a cloud or data centre.

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. Also included are wired device connections, such as IEEE 1901 power line communications.

The IoT World Forum (IoTWF) Standardized Architecture

In 2014 the IoTWF architectural committee (led by Cisco, IBM, Rockwell Automation, and others) published a seven-layer IoT architectural reference model.

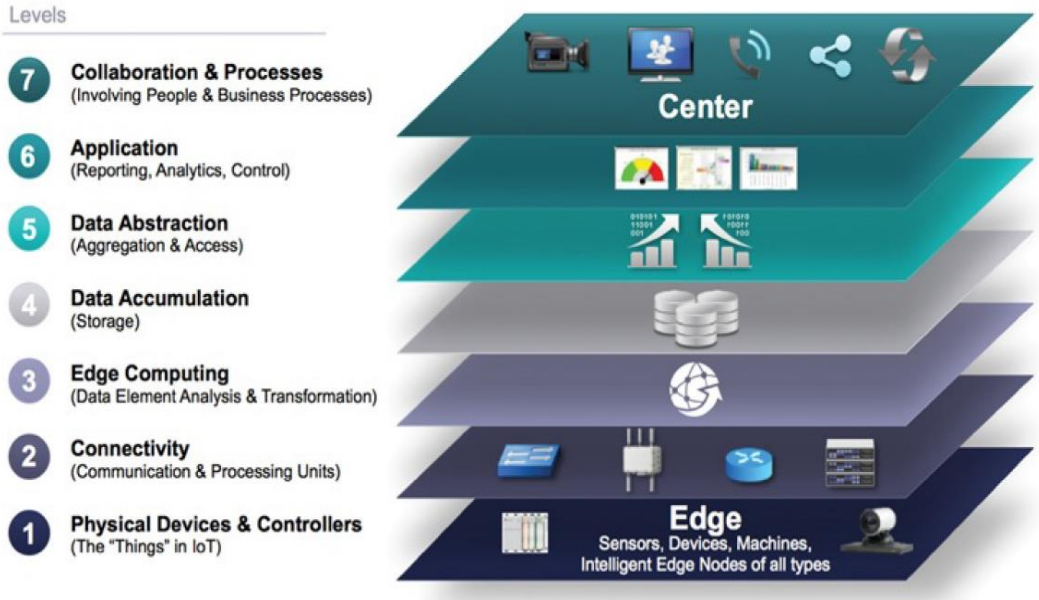

Figure 2-2 *IoT Reference Model Published by the IoT World Forum*

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

Layer 1: 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. The size of these "things" can range from almost microscopic sensors to giant machines in a factory. Their primary function is generating data and being capable of being queried and/or controlled over a network.

Layer 2: Connectivity Layer

- second layer , focus is on connectivity.
- transmissions between Layer 1 devices and the network and between the network and information processing that occurs at Layer 3 (the edge computing layer).

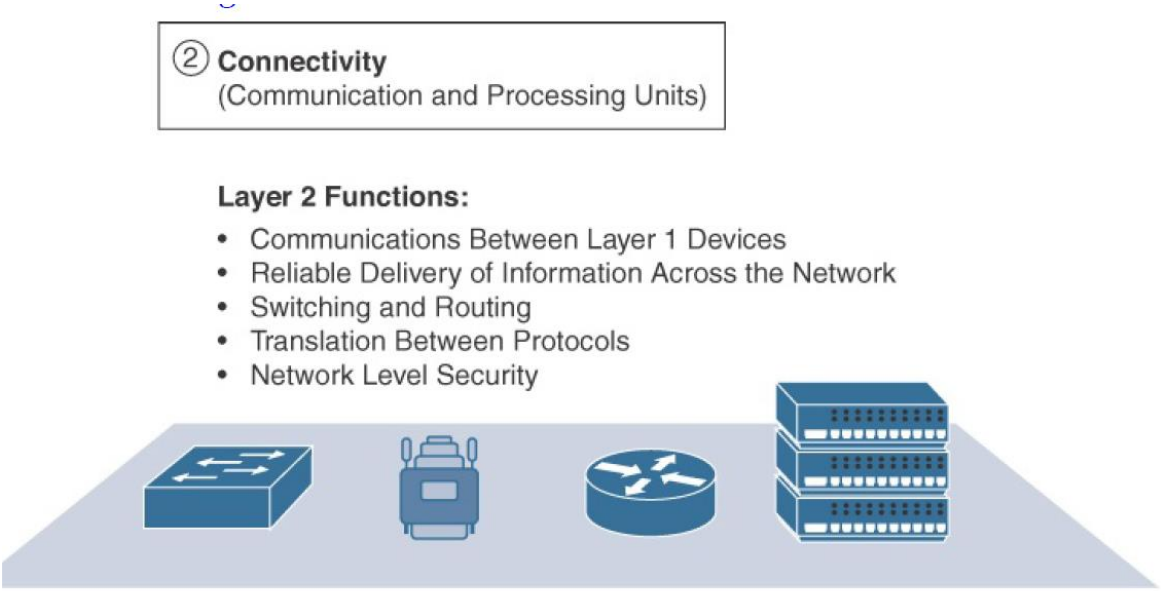

Figure 2-3 *IoT Reference Model Connectivity Layer Functions*

Layer 3: Edge Computing Layer

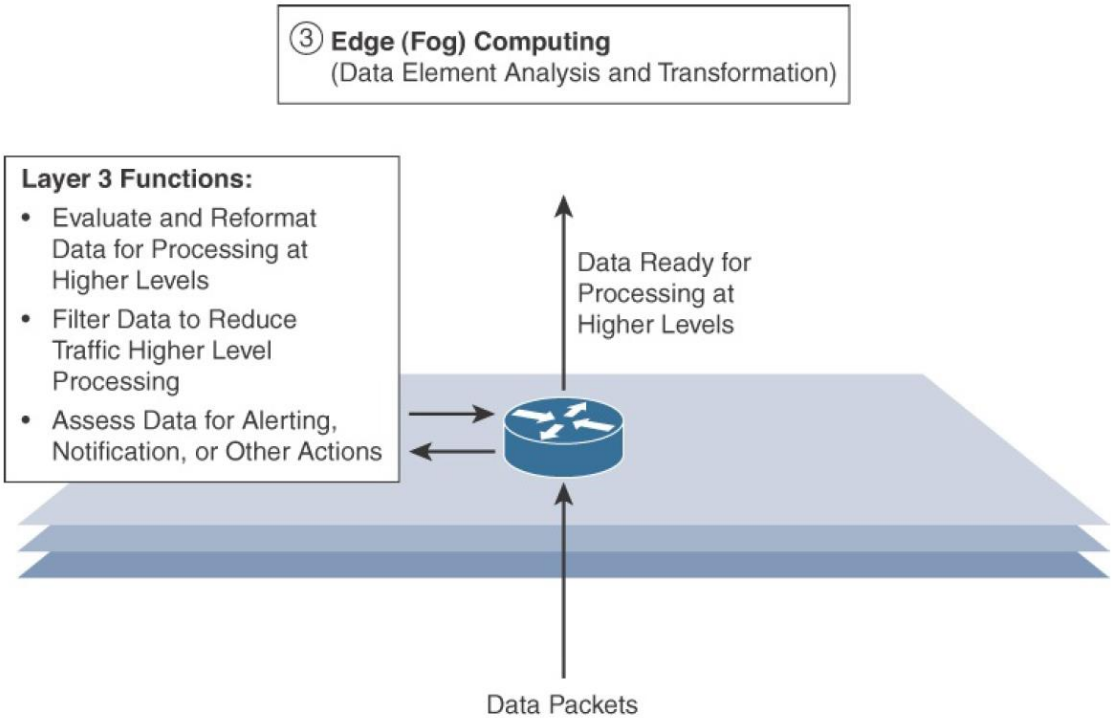

Figure 2-4 *IoT Reference Model Layer 3 Functions*

- Edge computing is the role of Layer 3. 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.
- Another Important function that occurs at Layer 3 is the evaluation of data to see if it can be filtered or aggregated before being sent to a higher layer and data can be reformatted or decoded, making additional processing by other systems easier. Thus, a

critical function is assessing the data to see if predefined thresholds are crossed and any action or alerts need to be sent.

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.

Table 2-2 *Summary of Layers 4–7 of the IoTWF Reference Model*

IT and OT Responsibilities in the IoT Reference Model

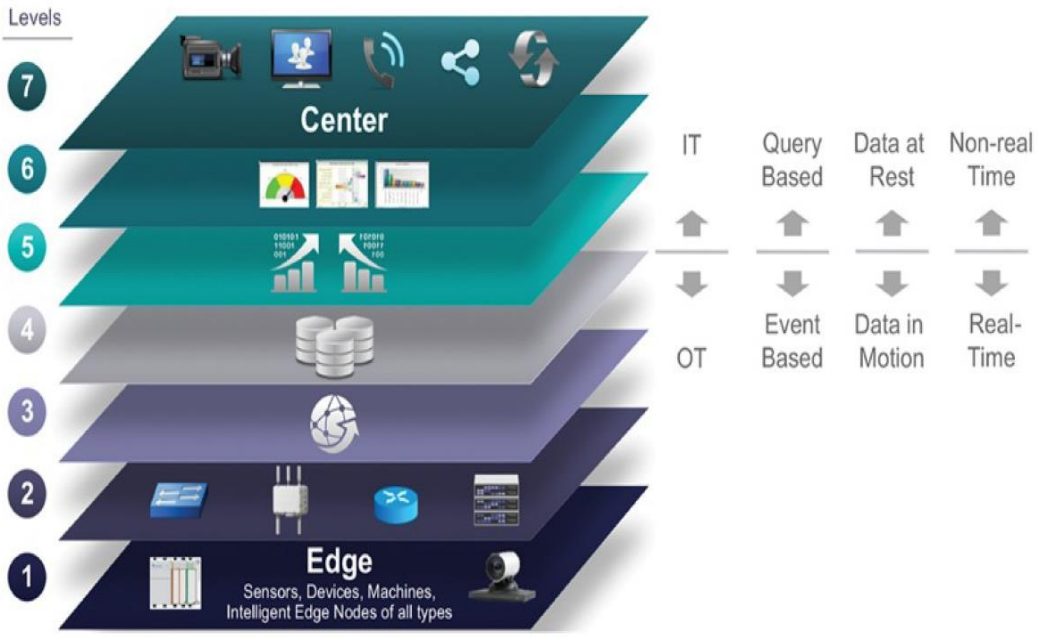

Figure 2-5 *IoT Reference Model Separation of IT and OT*

The bottom of the stack is generally in the domain of OT. For an industry like oil and gas, this includes sensors and devices connected to pipelines, oil rigs, refinery machinery, and so on. The top of the stack is in the IT area and includes things like the servers, databases, and applications, all of which run on a part of the network controlled by IT.

At the bottom, in the OT layers, the devices generate real-time data at their own rate and huge amount of data transiting the IoT network, but the sheer volume of data suggests that applications at the top layer will be able to ingest that much data at the rate required. To meet this requirement, data has to be buffered or stored at certain points within the IoT stack. Layering data management in this way throughout the stack helps the top four layers handle data at their own speed.

The real-time "data in motion" close to the edge has to be organized and stored so that it becomes "data at rest" for the applications in the IT tiers. The IT and OT organizations need to work together for overall data management.

A Simplified IoT Architecture

To solve the IoT heterogeneity problem an IoT framework that highlights the fundamental building blocks that are common to most IoT systems and which is intended to help you in designing an IoT network.

This framework is presented as two parallel stacks: The IoT Data Management and Compute Stack and the Core IoT Functional Stack.
This model no lacks the detail necessary to develop a sophisticated IoT strategy the intention is to simplify the IoT architecture into its most basic building blocks and applied to industry specific use cases.

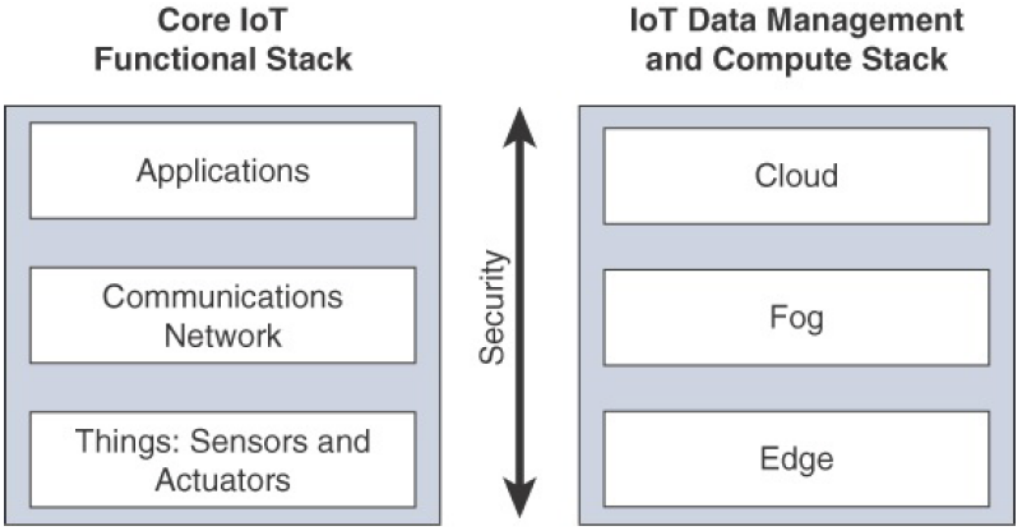

Figure 2-6 *Simplified IoT Architecture*

The core layer includes "things," a communications network, and applications. the core IoT and data management are separated into parallel and aligned stacks This gives you better visibility into the functions of each layer.
The presentation of the Core IoT Functional Stack in three layers simple architecture needs to be expanded on. The network communications layer of the IoT stack itself involves a significant amount of detail and incorporates a vast array of technologies to incorporate heterogeneity of IoT sensors uses gateway and backhaul technologies and ultimately bring the data back to a central location for analysis and processing.

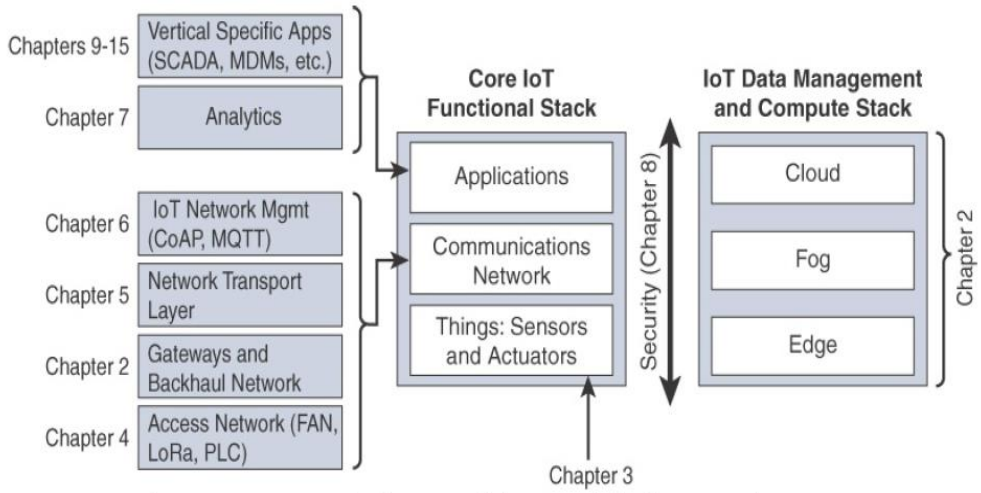

Figure 2-7 *Expanded View of the Simplified IoT Architecture*

the network between the gateway and the data centre is composed
mostly of traditional technologies that tunnelling and VPN technologies, IP-based quality of service (QoS), conventional Layer 3 routing protocols such as BGP and IP-PIM, and security capabilities such as encryption, access control lists (ACLs), and firewalls.

IT networks, the applications and analytics layer of IoT doesn't necessarily exist only in the data center or in the cloud. Due to the unique challenges and requirements of IoT, it is often necessary to deploy applications and data management throughout the architecture in a tiered approach, allowing data collection, analytics, and intelligent controls at multiple points in the IoT system.

The data management is aligned with each of the three layers of the Core IoT Functional Stack. 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), and the cloud layer(data management in the cloud or central data centre).

The Core IoT Functional Stack

IoT networks are built around the concept of "things," or smart objects
performing functions and delivering new connected services. the "thing" interacts with an external system to report information that the smart object collects, to exchange with other objects, or to interact with a management platform. The management platform can be used to process data collected from the smart object and also guide the behaviour of the smart object.

an IoT network to be operational:
"Things" layer: At this layer, the physical devices need to fit the constraints of the environment in which they are deployed while still being able to provide the information needed.
Communications network layer: When smart objects are not self-contained, they need to communicate with an external system. In many cases, this communication uses a wireless technology. This layer has four sublayers:

1. **Access network sublayer:** The last mile of the IoT network is the access network. This is typically made up of wireless technologies such as 802.11ah, 802.15.4g, and LoRa. The sensors connected to the access

network may also be wired.

2. **Gateways and backhaul network sublayer:** A common

communication system organizes multiple smart objects in a given area around a common gateway. The gateway communicates directly with the smart objects. The role of the gateway is to forward the collected information through a longer-range medium (called the backhaul) to a headend central station where the information is processed. This information exchange is a Layer 7 (application) function, which is the reason this object is called a gateway. On IP networks, this gateway also forwards packets from one IP network to another, and it therefore acts as a router.

3. **Network transport sublayer:** For communication to be successful, network and transport layer protocols such as IP and UDP must be implemented to support the variety of devices to connect and media to use.
4. **IoT network management sublayer:** Additional protocols must be in place to allow the headend applications to exchange data with the sensors. Examples include CoAP and MQTT.

Application and analytics layer: At the upper layer, an application need to process the collected data, not only to control the smart objects when necessary, but to make intelligent decision based on the information collected and, in turn, instruct the "things" or other systems to adapt to the analysed conditions and change their behaviours or parameters.

Layer 1: Things: Sensors and Actuators Layer:

From an architectural standpoint, the variety of smart object types, shapes, and needs drive the variety of IoT protocols and architectures. The classification of Smart Objects.

- **Battery-powered or power-connected:** This classification is based on

whether the object carries its own energy supply or receives continuous power from an external power source. Battery-powered things can be moved more easily than line-powered objects. However, batteries limit the lifetime and amount of energy that the object is allowed to consume, thus driving transmission range and frequency.

- **Mobile or static:** based on whether the "thing" should move or always stay at the same location. A sensor may be mobile because it is moved from one object to another (for example, a viscosity sensor moved from batch to batch in a chemical plant) or because it is attached to a moving object (for example, a location sensor on moving goods in a warehouse or factory floor). The frequency of the movement may also vary, from occasional to permanent. The range of mobility (from a few inches to miles away) often drive the possible power source.

- **Low or high reporting frequency:** This classification is based on how often the object should report monitored parameters. A rust sensor may report values once a month. A motion sensor may report acceleration several hundred times per second. Higher frequencies drive higher energy consumption, which may create constraints on the possible power source (and therefore, the object mobility) and the transmission range.

- **Simple or rich data:** This classification is based on the quantity of data exchanged at each report cycle. A humidity sensor in a field may report a simple daily index value (on a binary scale from 0 to 255), while an engine sensor may report hundreds of

parameters, from temperature to pressure, gas velocity, compression speed, carbon index, and many others. Richer data typically drives higher power consumption. This classification is often combined with the previous to determine the object data throughput (low throughput to high throughput). You may want to keep in mind that throughput is a combined metric. A medium-throughput object may send simple data at rather high frequency (in which case the flow structure looks continuous), or may send rich data at rather low frequency (in which casethe flow structure looks bursty).

- **Report range:** This classification is based on the distance at which the

gateway is located. For example, for your fitness band to communicate with your phone, it needs to be located a few meters away at most.

- **Object density per cell:** This classification is based on the number of

smart objects (with a similar need to communicate) over a given area,
connected to the same gateway. An oil pipeline use single sensor at key location .but SETI Colossus telescope use hundreds of multiple gyroscopes, gravity, and vibration sensors.

examples of applications matching the combination of mobility and throughput requirements.

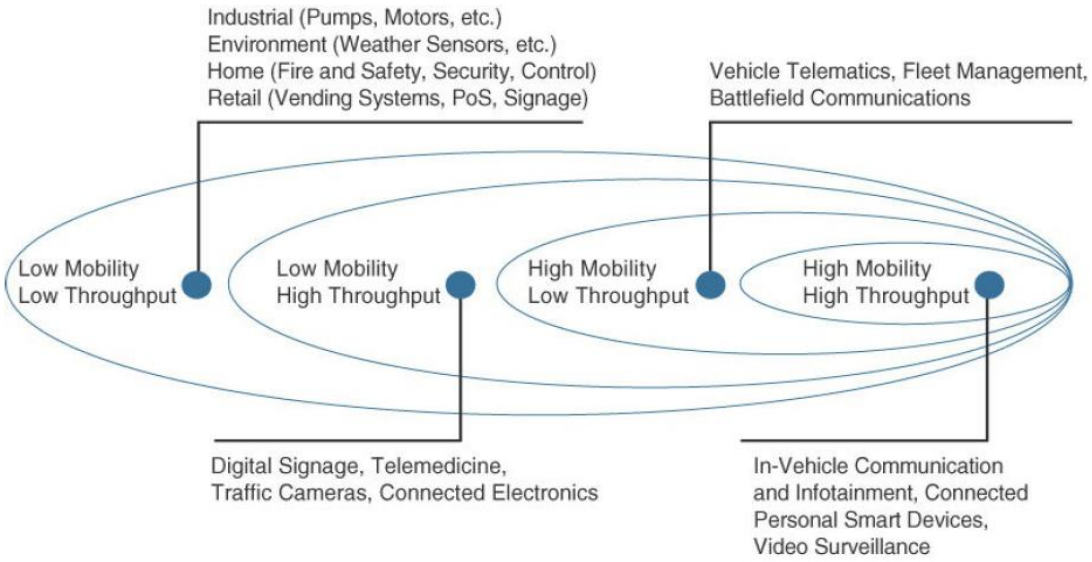

Figure 2-8 *Example of Sensor Applications Based on Mobility and Throughput*

Layer 2: Communications Network Layer

Knowing the transmission capabilities (transmission range, data volume and frequency, sensor density and mobility) of sensor connect the object and communicate

Access Network Sublayer

- There is a direct relationship between the IoT network technology and the type of connectivity topology. This got designed based on use cases the frequency band that was expected to be most suitable, the frame structure matching the expected data pattern (packet size and communication intervals), and the possible topologies that these use cases illustrate.

One key parameter determining the choice of access technology is the range between the smart object and the information collector i.e IoT world and the expected transmission distances.

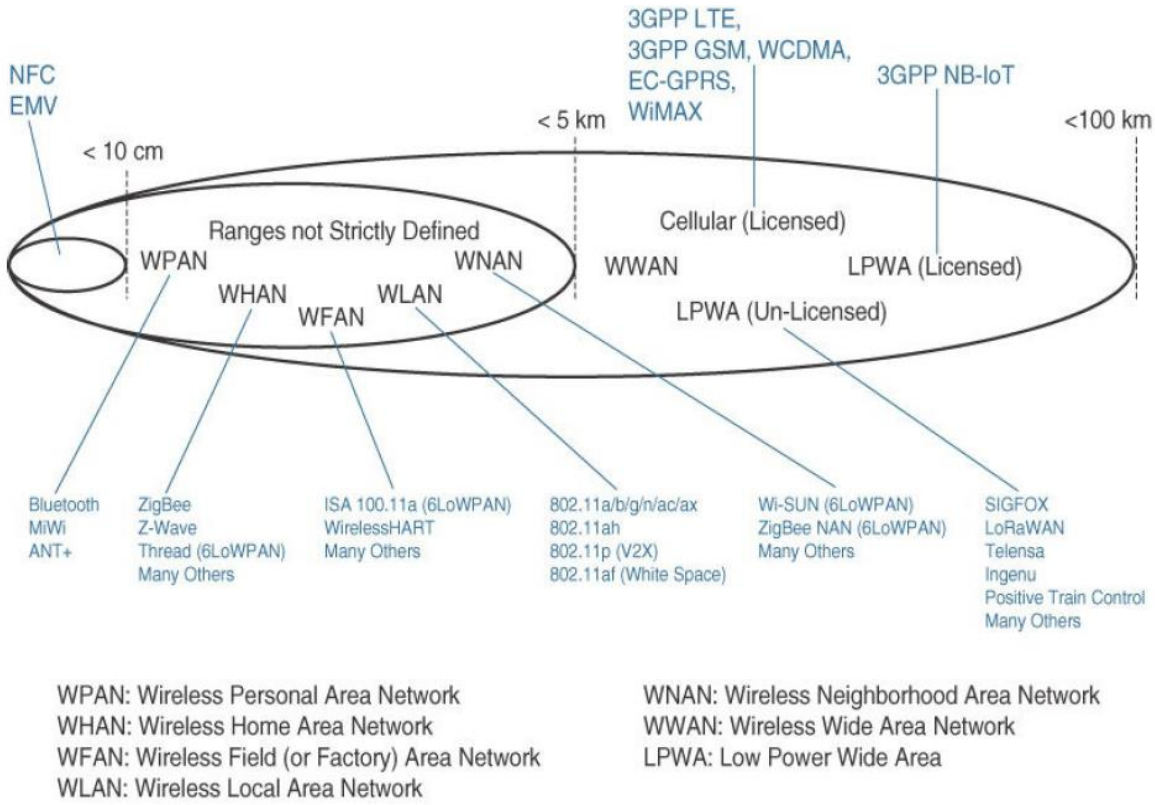

Figure 2-9 *Access Technologies and Distances*

Range estimates are grouped by category names that illustrate the environment or the vertical where data collection over that range is expected. Common groups are as follows:

- **PAN (personal area network):** Scale of a few meters. This is the personal space around a person. A common wireless technology for this scale is Bluetooth.
- **HAN (home area network):** Scale of a few tens of meters. At this scale, common wireless technologies for IoT include ZigBee and Bluetooth Low Energy (BLE).
- **NAN (neighbourhood area network):** Scale of a few hundreds of meters. The term NAN is often used to refer to a group of house units from which data is collected.
- **FAN (field area network):** Scale of several tens of meters to several hundred meters. FAN typically refers to an outdoor area larger than asingle group of house units. The FAN is often seen as "open space" (and therefore not secured and not controlled). A FAN is sometimes viewed as a group of NANs, but some verticals see the FAN as a group of HANs or a group of smaller outdoor cells. As you can see, FAN and NAN may sometimes be used interchangeably. In most cases, the vertical context is clear enough to determine the grouping hierarchy.

- **LAN (local area network):** Scale of up to 100 m. This term is very common in networking, and it is therefore also commonly used in the IoT space when standard networking technologies (such as Ethernet or IEEE 802.11) are used. Other networking classifications, such as MAN (metropolitan area network, with a range of

up to a few kilometers) and WAN (wide area network, with a range of more than a few kilometers), are also commonly used.

Note that for all these places in the IoT network, a "W" can be added to specifically indicate wireless technologies used in that space. For example, HomePlug is a wired technology found in a HAN environment, but a HAN is often referred to as a WHAN (wireless home area network) when a wireless technology, like ZigBee, is used in that space.

- Increasing the throughput and achievable distance typically comes with an increase in power consumption. Therefore, after determining the smart object requirements (in terms of mobility and data transfer), a second step is to determine the target quantity of objects in a single collection cell, based on the transmission range and throughput required. This parameter in turn determines the size of the cell.

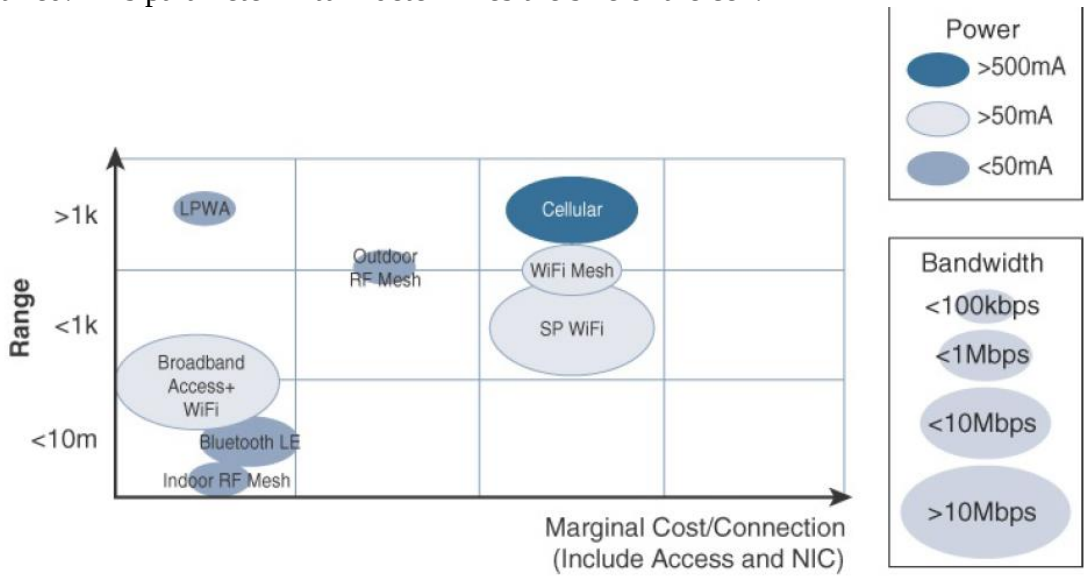

Figure 2-11 *Comparison Between Common Last-Mile Technologies in Terms of Range Versus Cost, Power, and Bandwidth*

- Some technologies offer flexible connectivity structure to extend communication possibilities:

Point-to-point topologies: These topologies allow one point to communicate with another point. a single object can communicate only with a single gateway. several technologies are referred to as "point-to-point" when each object establishes an individual session with the gateway communication structure more than the physical topology.

Point-to-multipoint topologies: These topologies allow one point to communicate with more than one other point. Most IoT technologies where one or more than one gateways communicate with multiple smart objects are in this category IoT networks is that some nodes (for example, sensors) support both data collection and forwarding functions, while some other nodes (for example, some gateways) collect the smart object data, sometimes instruct the sensor to perform specific operations, and also interface with other networks or possibly other gateways. the central point can be in charge of the overall network coordination, taking care of the beacon transmissions and connection to each sensor.

In the IEEE 802.15.4 standard, the central point is called a *coordinator* for the network. With this type of deployment, each sensor is not intended to do anything other than communicate with the coordinator in a master/slave type of relationship. The sensor can implement a subset

of protocol functions to perform just a specialized part (communication with the coordinator). Such a device is called a reduced-function device (RFD).

The coordinator that implements the full network functions is called, by contrast, a full-function device (FFD). An FFD can communicate directly with another FFD or with more than one FFD,

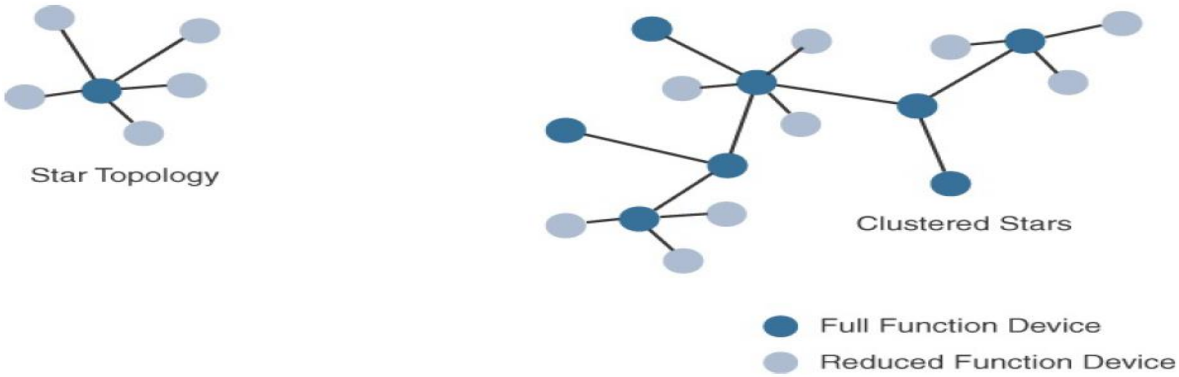

Figure 2-12 *Star and Clustered Star Topologies*

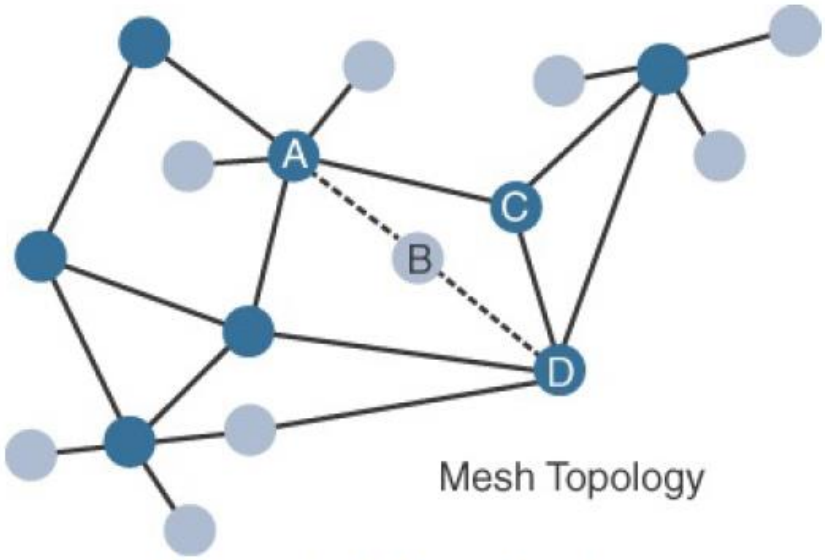

Figure 2-13 *Mesh Topology*

Gateways and Backhaul Sublayer

Data collected from a smart object may need to be forwarded to a central station where data is processed. As this station is often in a different location from the smart object, data directly received from the sensor through an access technology needs to be forwarded to another medium (the backhaul) and transported to the central station. The gateway is in charge of this inter-medium communication.

A wireless technology (DSRC operates in the upper 5 GHz range) is used for backhaul communication, peer-to-peer, or mesh communication between vehicles.

In the DSRC case, the entire "sensor field" is moving along with the gateway, but the general principles of IoT networking remain the same. The range at which DSRC can communicate is limited.

Network Transport Sublayer

Distribution automation (DA) also allows your meter to communicate with neighbouring meters or other devices in the electrical distribution grid. With such communication, consumption load balancing may be optimized. your smart meter may communicate with your house appliances to evaluate their type and energy demand. With this scheme, your washing machine can be turned on in times of lower consumption from other systems such as at night, while power to your home theatre system will never be deprived, always turning on when you need it.

consumption pattern A mesh system may appear at the scale of the house. More commonly, a partial mesh appears, with some central nodes connecting to multiple other nodes. Data may flow locally, or it may have to be orchestrated by a central application to coordinate the power budget between houses.

This communication structure thus may involve peer-to-peer (for example, meter to meter), point-to-point (meter to headend station), point-to-multipoint (gateway or head-end to multiple meters), unicast and multicast communications (software update to one or multiple systems). In a multitenant environment (for example, electricity and gas consumption management), different systems may use the same communication pathways. This communication occurs over multiple media (for example, power lines inside your house or a short-range wireless system like indoor Wi-Fi and/or ZigBee), a longer-range wireless system to the gateway, and yet another wireless or wired medium for backhaul transmission.

The flexibility of IP allows this protocol to be embedded in objects of very different natures, exchanging information over very different media, including low-power, lossy, and low-bandwidth networks.
Finally, the transport layer protocols built above IP (UDP and TCP) can easily be leveraged to decide whether the network should control the data packet delivery (with TCP) or whether the control task should be left to the application (UDP).

IoT Network Management Sublayer

- Upper-layer protocols need to take care of data transmission between the smart objects and other systems. IoT implementers HTTP has a client and server component the sensor could use the client part to establish a connection to the IoT central application (the server), and then data can be exchanged.
- HTTP was not designed to operate in constrained environments with low memory, low power, low bandwidth, and a high rate of packet failure. Despite these limitations, other web-derived protocols have been suggested for the IoT space. One example is WebSocket.
- XMPP is based on instant messaging and presence. It allows the exchange of data between two or more systems and supports presence and contact list maintenance. It

can also handle publish/subscribe, making it a good choice for distribution of information to multiple devices. A limitation of XMPP is its reliance on TCP

- Another common IoT protocol utilized in these middles to upper layers is Message Queue Telemetry Transport (MQTT). MQTT uses a broker-based architecture. The sensor can be set to be an MQTT publisher (publishes a piece of information), the application that needs to receive the information can be set as the MQTT subscriber, and any intermediary system can be set as a broker to relay the information between the publisher and the subscriber(s). MQTT runs over TCP. A consequence of the reliance on TCP is that an MQTT client typically always holds a connection open to the broker .

Layer 3: Applications and Analytics Layer

Once connected to a network, your smart objects exchange information with other systems.

Analytics Versus Control Applications

Multiple applications can help increase the efficiency of an IoT network. Each application collects data and provides a range of functions based on analysing the collected data.

basic classification can be as follows:

Analytics application: This type of application collects data from multiple smart objects, processes the collected data, and displays information resulting from the data that was processed. The display can be about any aspect of the IoT network, from historical reports, statistics, or trends to individual system states. The important aspect is that the application processes the data to convey a view of the network that cannot be obtained from solely looking at the information displayed by a single smart object.

Control application: This type of application controls the behavior of the smart object or the behavior of an object related to the smart object. For example, a pressure sensor may be connected to a pump. A control application increases the pump speed when the connected sensor detects a drop in pressure. Control applications are very useful for controlling complex aspects of an IoT network with a logic that cannot be programmed inside a single IoT object, either because the configured changes are too complex to fit into the local system or because the configured changes rely on parameters that include elements outside the IoT object.
An example of control system architecture is SCADA. SCADA was developed as a universal method to access remote systems and send instructions. One example where SCADA is widely used is in the control and monitoring of remote terminal units (RTUs) on the electrical distribution grid.

Many advanced IoT applications include both analytics and control modules. In most cases, data is collected from the smart objects and processed in the analytics module. The result of this processing may be used to modify the behaviour of smart objects or systems related to the smart objects. The control module is used to convey the instructions for behavioural changes. When evaluating an IoT data and analytics application, you need to determine the relative depth of the control part needed for your use case and match it against the type of analytics provided.

Data Versus Network Analytics

Analytics is a general term that describes processing information to make sense of collected data.

Data analytics: This type of analytics processes the data collected by smart objects and combines it to provide an intelligent view related to the IoT system. At a very basic level, a dashboard can display an alarm when a weight sensor detects that a shelf is empty in a store. In a more complex case, temperature, pressure, wind, humidity, and light levels collected from thousands of sensors may be combined and then processed to determine the likelihood of a storm and its possible path. In this case, data processing can be very complex and may combine multiple changing values over complex algorithms.

Network analytics: Most IoT systems are built around smart objects connected to the network. A loss or degradation in connectivity is likely to affect the efficiency of the system. Such a loss can have dramatic effects. For example, open mines use wireless networks to automatically pilot dump trucks. A lasting loss of connectivity may result in an accident or degradation of operations efficiency (automated dump trucks typically stop upon connectivity loss). On a more minor scale, loss of connectivity means that data stops being fed to your data analytics platform, and the system stops making intelligent analyses of the IoT system. A similar consequence is that the control module cannot modify local object behaviors anymore?

Data Analytics Versus Business Benefits

Data analytics object can be connected, and multiple types of sensors can be installed on a given object. Collecting and interpreting the data generated by these devices is where the value of IoT is realized.

Smart Services

- smart services use IoT and aim for efficiency
- Smart services can also be used to measure the efficiency of machines by detecting machine output, speed, or other forms of usage evaluation. Entire operations can be optimized with IoT.
- for example, presence and motion sensors can evaluate the number of guests in lobby and redirect personnel accordingly.

- Smart services can be integrated into an IoT system. For example, sensors can be integrated in a light bulb. A sensor can turn a light on or off based on the presence of a human in the room. An even smarter system can communicate with other systems in the house, learn the human movement pattern, and anticipate the presence of a human, turning on the light just before the person enters the room.
- smart grid applications can coordinate the energy consumption between houses to regulate the energy demand from the grid.
- Efficiency also applies to M2M communications. In mining environments, vehicles can communicate to regulate the flows between drills, draglines, bulldozers, and dump trucks

IoT Data Management and Compute Stack

IoT system includes new requirements include the following:
Minimizing latency: Milliseconds matter for many types of industrial systems, such as when you are trying to prevent manufacturing line shutdowns or restore electrical service. Analysing data close to the device that collected the data can make a difference between averting disaster and a cascading system failure.
Conserving network bandwidth: Offshore oil rigs generate 500 GB of data weekly. Commercial jets generate 10 TB for every 30 minutes of flight. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud. Nor is it necessary because many critical analyses do not require cloud-scale processing and storage.
Increasing local efficiency: Collecting and securing data across a wide geographic area with different environmental conditions may not be useful. The environmental conditions in one area will trigger a local response independent from the conditions of another site hundreds of miles away. Analysing both areas in the same cloud system may not be necessary for immediate efficiency.

data management in traditional IT systems is very simple. The endpoints (laptops, printers, IP phones, and so on) communicate over an IP core network to servers in the data center or cloud. Data is generally stored in the data center, and the physical links from access to core are typically high bandwidth, meaning access to IT data is quick.

Several data-related problems need to be addressed:

- Bandwidth in last-mile IoT networks is very limited. When dealing with thousands/millions of devices, available bandwidth may be on order oftens of Kbps per device or even less.
- Latency can be very high. Instead of dealing with latency in the milliseconds range, large IoT networks often introduce latency of hundreds to thousands of milliseconds.
- Network backhaul from the gateway can be unreliable and often depends on 3G/LTE or even satellite links. Backhaul links can also be expensive if a per-byte data usage model is necessary.

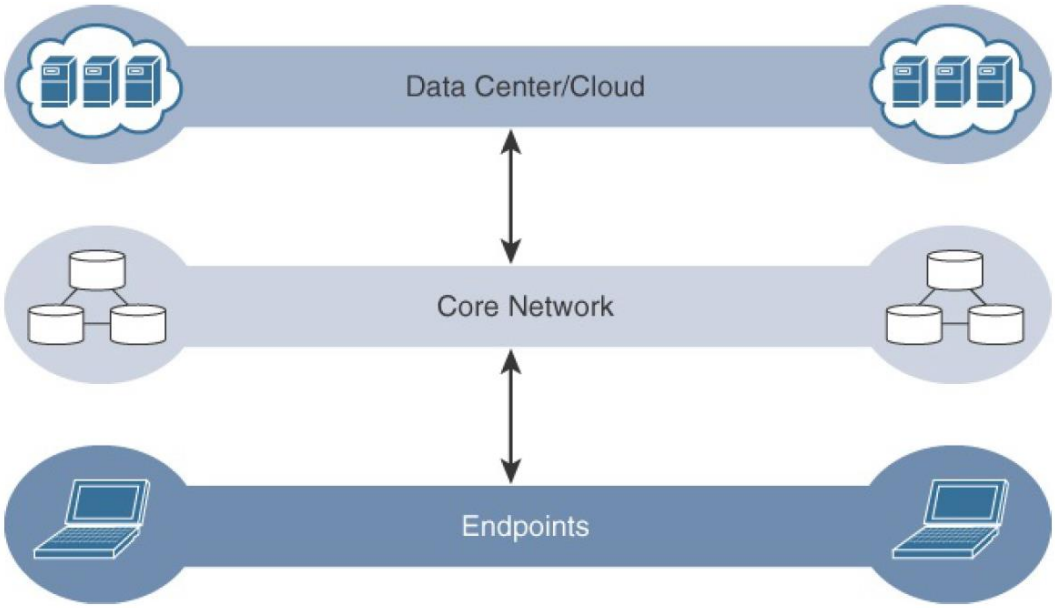

Figure 2-14 *The Traditional IT Cloud Computing Model*

- The volume of data transmitted over the backhaul can be high, and much of the data may not really be that interesting (such as simple polling messages).
- Big data is getting bigger. The concept of storing and analyzing all sensor data in the cloud is impractical. The sheer volume of data generated makes real-time analysis and response to the data almost impossible.

Fog Computing

- Any device with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and IoT gateways.

- An advantage of this structure is that the fog node allows intelligence gathering (such as analytics) 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.

- having contextual awareness gives fog nodes the ability to react to events in the IoT network much more quickly than in the traditional IT compute model, which would likely incur greater latency and have slower response times. The fog layer thus provides a distributed edge control loop capability where devices can be monitored, controlled, and analyzed in real time without the need to wait for communication from the central analytics and application servers in the cloud.

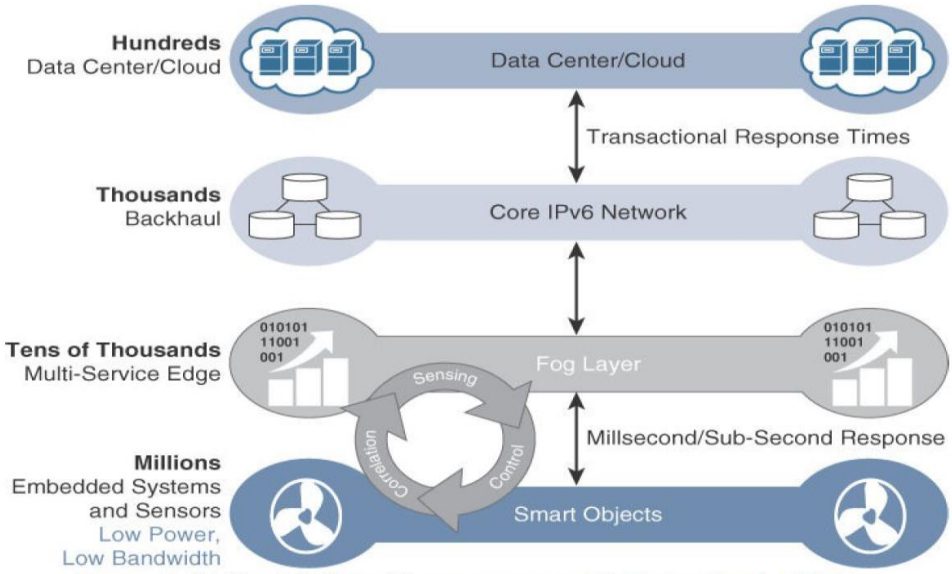

Figure 2-15 *The IoT Data Management and Compute Stack with Fog Computing*

IoT fog computing enables data to be pre processed and correlated with other inputs to produce relevant information

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: In sharp contrast to the more centralized cloud, 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. For example, typical metering deployments often see 3000 to 4000 nodes per gateway router, which also functions as the fog computing node.

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. Preprocessing of data in the fog nodes allows upper-layer applications to perform batch processing on a subset of the data.

Edge Computing

IoT computing has moved to the edge, and in some cases it now resides directly in the sensors and IoT devices.

IoT devices and sensors often have constrained resources, however, as compute capabilities increase. Some new classes of IoT endpoints have enough compute capabilities to perform at least low-level analytics and filtering to make basic decisions. For example, consider a water sensor on a fire hydrant.

Another example is in the use of smart meters. Edge compute–capable meters are able to communicate with each other to share information on small subsets of the electrical distribution grid to monitor localized power quality and consumption, and they can inform a fog node of

events that may pertain to only tiny sections of the grid. Models such as these help ensure the highest quality of power delivery to customers.

The Hierarchy of Edge, Fog, and Cloud

This model suggests a hierarchical organization of network, compute, and data storage resources. At each stage, data is collected, analyzed, and responded to when necessary, according to the capabilities of the resources at each layer. As data needs to be sent to the cloud, the latency becomes higher. The advantage of this hierarchy is that a response to events from resources close to the end device is fast and can result in immediate benefits, while still having deeper compute resources available in the cloud when necessary.

It is important to note that the heterogeneity of IoT devices also means a heterogeneity of edge and fog computing resources. While cloud resources are expected to be homogenous, it is fair to expect that in many cases both edge and fog resources will use different operating systems, have different CPU and data storage capabilities, and have different energy consumption profiles.

Edge and fog thus require an abstraction layer that allows applications to communicate with one another. The abstraction layer exposes a common set of APIs for monitoring, provisioning, and controlling the physical resources in a standardized way.

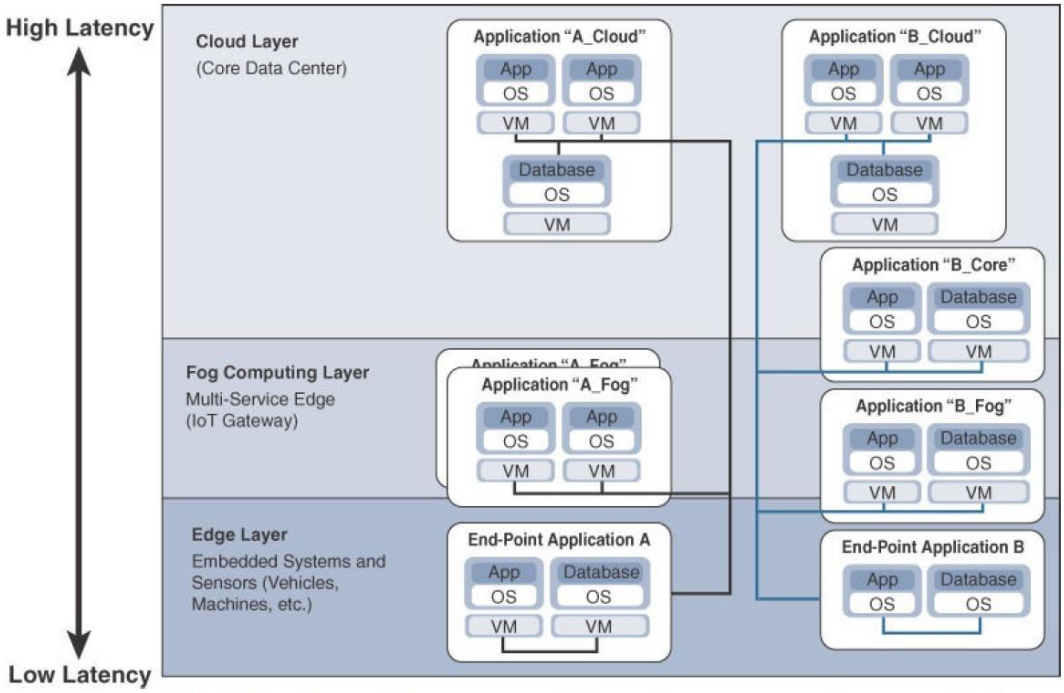

Figure 2-16 *Distributed Compute and Data Management Across an IoT System*

From an architectural standpoint, fog nodes closest to the network edge receive the data from IoT devices. The fog IoT application then directs different types of

data to the optimal place for analysis:

- The most time-sensitive data is analyzed on the edge or fog node closest to the things generating the data.
- Data that can wait seconds or minutes for action is passed along to an aggregation node for analysis and action.
- Data that is less time sensitive is sent to the cloud for historical analysis, big data analytics, and long-term storage. For example, each of thousands or hundreds of thousands of fog nodes might send periodic summaries of data to the cloud for historical analysis and storage.