FUTURE VISION BIE

By K B Hemanth Raj

Visit : https://hemanthrajhemu.github.io

A Small Contribution Would Support Us.

Dear Viewer,

Future Vision BIE is a free service and so that any Student/Research Personal **Can Access Free of Cost**.

If you would like to say **thanks**, you can make a **small contribution** to the author of this site.

Contribute whatever you feel this is worth to you. This gives **us support** & to bring **Latest Study Material** to you. After the Contribution Fill out this Form (https://forms.gle/tw3T3bUVpLXL8omX7). To Receive a **Paid E-Course for Free**, from our End within 7 Working Days.

Regards

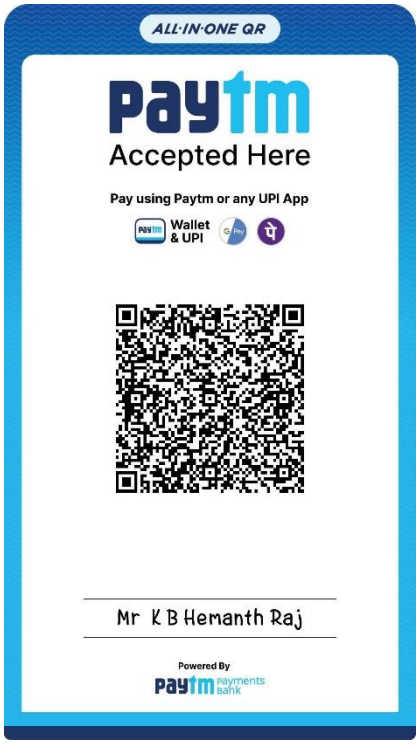
- K B Hemanth Raj (Admin)

Contribution Methods

UPI ID

1. futurevisionbie@oksbi
2. futurevisionbie@paytm

Scan & Pay



Account Transfer

Account Holder's Name: K B Hemanth Raj

Account Number: 39979402438

IFSC Code: SBIN0003982

MICR Code: 560002017

More Info: https://hemanthrajhemu.github.io/Contribution/

Gain Access to All Study Materials according to VTU,
CSE – Computer Science Engineering,
ISE – Information Science Engineering,
ECE - Electronics and Communication Engineering & MORE...

Stay Connected... get Updated... ask your queries...

Join Telegram to get Instant Updates: https://bit.ly/VTU_TELEGRAM

Contact: MAIL: futurevisionbie@gmail.com

INSTAGRAM: www.instagram.com/futurevisionbie/

WHATSAPP SHARE: https://bit.ly/FVBIESHARE

Introduction

- What is Internet?
  - The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and peer-to-peer networks for file sharing.

- What is things?
  - Object like Sensor, Computer, Mobile Phone

IoT

- Novel paradigm
  - Rapidly gaining ground in the wireless scenario
- Basic idea
  - Pervasive presence around us a variety of things or objects
  - Objects can see, hear, perform jobs
  - Which are able to interact/talk to each other
  - To reach a common goal
- IoT transforms these objects from traditional to smart
  - Exploiting underlying technology
  - Embedded device, communication, sensor network, IP

- Growing number of objects are being connected to internet
  - Connecting –Thermostats and Heating/Ventilation/AC monitoring and control
  - Enable smart homes

Evolution of Internet

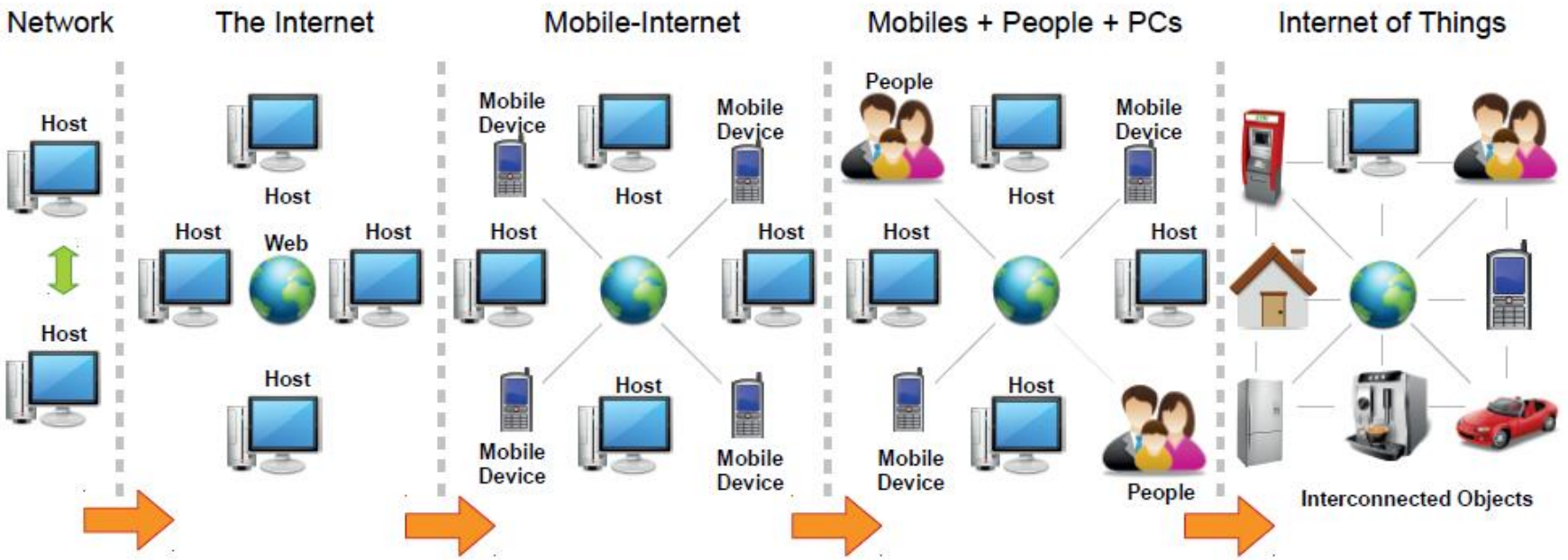


Fig. 1. Evolution of the Internet in five phases. The evolution of Internet begins with connecting two computers together and then moved towards creating World Wide Web by connecting large number of computers together. The mobile-Internet emerged by connecting mobile devices to the Internet. Then, peoples' identities joined the Internet via social networks. Finally, it is moving towards Internet of Things by connecting every day objects to the Internet.

Introduction

Fig. 1. The overall picture of IoT emphasizing the vertical markets and the horizontal integration between them.

- “Anytime, anywhere, anymedia” – vision pushing forward the advances in communication
  - Add “anything”
  - Increase the radio connection
  - Reduction in size, weight, energy, cost

What is IOT?

Fig. 2. Definition of the Internet of Things: The Internet of Things allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service [21].

Challenges

- Full inter-operability of interconnected devices
- Providing them higher degree of smartness
  - Adaptation and autonomous power
  - Guaranteeing trust, security, privacy
- Things are low resource
  - Energy and computation power
- Scalability
  - Solutions should pay attention

IOT Elements

Fig. 4. The IoT elements.

IOT Elements

- Communication
  - Low power communication over noisy channel
  - Various methods like NFC (Near field communication), RFID (Radio-Frequency IDentification), WiFi, LTE
- Computation
  - Hardware platform (Raspberry PI)
  - Software Platform(RTOS)-Contiki, Cooja simulator, TiniOS, IoV
  - Cloud platform

IOT Elements

- Services
  - Identity-related services
  - Information Aggregation Services
    - Smart health
  - Collaborative-Aware Services
    - Smart home,
  - Ubiquitous Services

Enabling Technologies

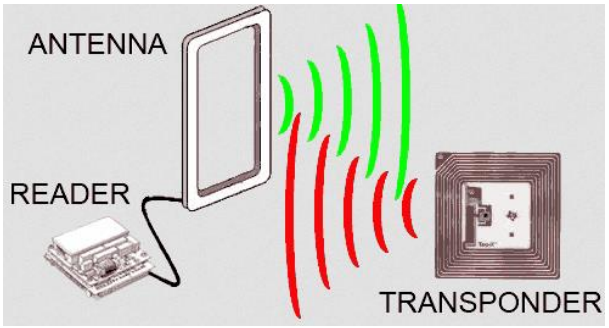
- IoT concept to realization
  - Integration of several enabling technology
  - Building blocks
- Identification
  - Name each object-Match the service with their demand
  - Electronic Product Code (EPC), Ubiquitous code
- Addressing objects
  - Object ID and address
  - “T1” name of the temperature sensor (not globally unique)
  - Object address=>address in the communication network (IPv4, 6)

RFID

- RFID stands for **Radio-Frequency IDentification.** The acronym refers to small electronic devices that consist of a small chip and an antenna. The chip typically is capable of carrying 2,000 bytes of data or less.
- The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card; it provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scanned to retrieve the identifying information.

Key concept–RFID system

- Identification of objects
- Two components
- Composed (a) Readers (b) RFID tags
- Tags
  - Passive
  - Active
  - Battery assisted passive
- Read only/Read-write
- Contains IC & Antenna
- Reader
  - Active reader
  - Passive reader

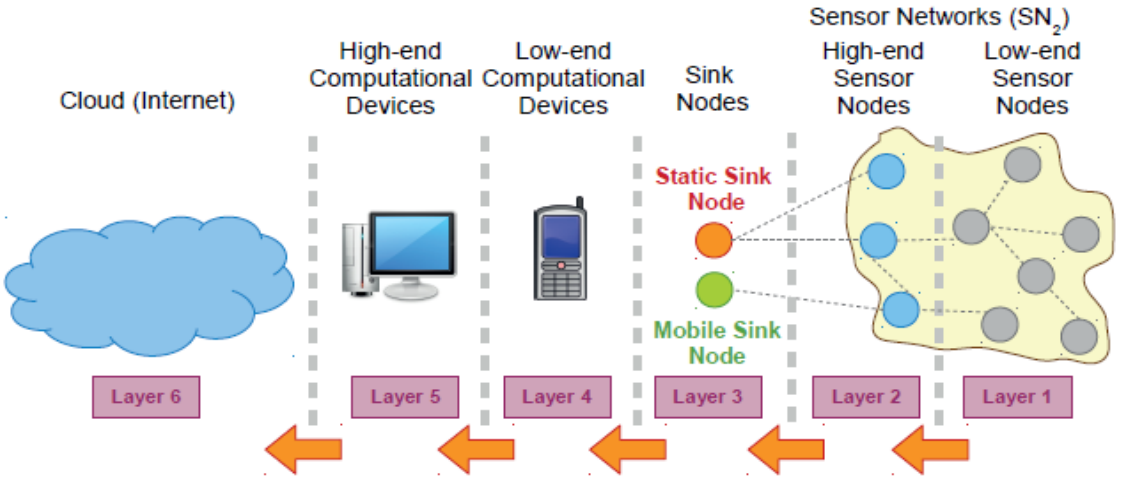


- Monitors objects in real time
  - Without line of sight
  - Maps real to virtual world

Sensors

- Sensor networks play a major role in IoT
- Co-operate with RFID system to better track objects
  - Location, temp, movement etc
- Consists a (large) number of sensing nodes
  - Homogenous/ heterogeneous
  - Communicating in wireless, multihop fashion
- Three different architecture
  - Flat
    - Data transfer from static sensor to a sink
  - Two layer arch.
    - Multiple static and mobile sink
  - Three layer arch.
    - Multiple sensor networks are connected over Internet
    - IoT

Layers in sensor network



Data flow

Fig. 3. Layered structure of a sensor network: These layers are identified based on the capabilities posed by the devices. In IoT, this layered architecture may have additional number of sub layers as it is expected to comprises large verity of in sensing capabilities.

- Data generated by sensors
- Data collected by sinks
- Sink nodes send the data to low-end computational device =>high end->cloud
  - Shared, stored, processed
- Information processing and communication at different layers
  - Capability and trade off

Sensor network and IoT

- Sensor network-Most essential component of IoT
  - Data collected from sensors
  - Processed and decision made
  - Actuators perform action

Differences

- (1) SN=> thin layer of software
  - IoT=> thick layer (middleware, API)
- (2) SN application specific (monitoring)

  IoT is not focused on specific application

  Example-pressure sensor – health of a bridge

  IoT: track traffic

  Middleware should provide generic services

Relationship between Sensor Network and IOT

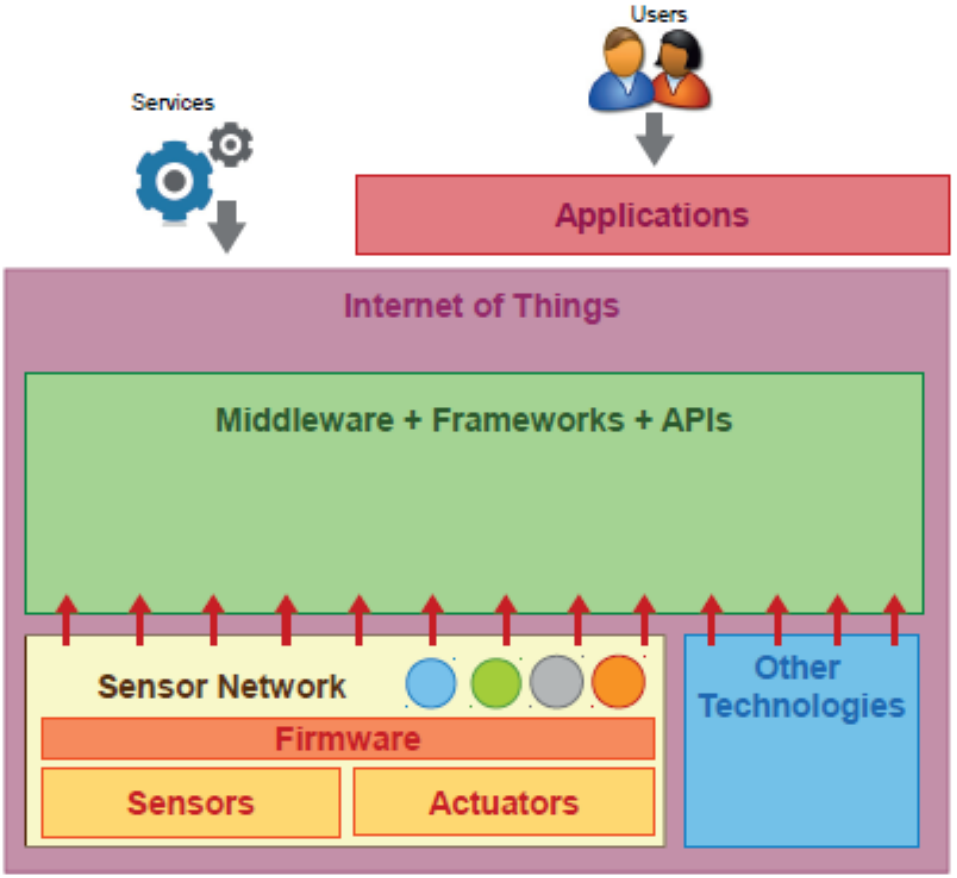


Fig. 4. Relationship between sensor networks and IoT.

Features of IoT

- Intelligence : Application of knowledge
  - Collect data and infer rules (high level info)
  - Modelling data
- Scale and Architecture : Hybrid arch.

Event driven–door sensor

Time driven – temperature sensor

- Complex system : Large number of objects
  - Interact
  - Appear/disappear
  - Various capability
- Time consideration – real time event detection
- Space – Location of the objects
  - Context detection

Module-1

- What Is IoT?
- IoT Network Architecture and Design

What Is IoT?

- IoT is to “connect the unconnected.”
- This means that objects that are not currently joined to a computer network or 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 improves in the areas of efficiency, accuracy, automation, and the enablement of advanced applications.

What Is IoT?

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

What Is IoT?

- Will explores the following topics:
- Genesis of IoT: This highlights IoT's place in the evolution and development of the Internet.
- IoT and Digitization: This details the differences between IoT and digitization and defines a framework for better understanding their relationship.
- IoT Impact: This shares a few high-level scenarios and examples to demonstrate the influence IoT will have on our world.
- Convergence of IT and OT: This explores how IoT is bringing together information technology (IT) and operational technology (OT).
- IoT Challenges: This provides a brief overview of the difficulties involved in transitioning to an IoT-enabled world.

Genesis of IoT

- The age of IoT is often said to have started between the years 2008 and 2009.
- The person credited 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.
- Kevin has explained that IoT now involves the addition of senses to computers.
- He was quoted as saying:
  - “In the twentieth century, computers were brains without senses—they only knew what we told them.” Computers depended on humans to input data and knowledge through typing, bar codes, and so on.
  - IoT is changing this paradigm; in the twenty-first century, computers are sensing things for themselves.
- 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?

Genesis of IoT

- The evolution of the Internet can be categorized into four phases.

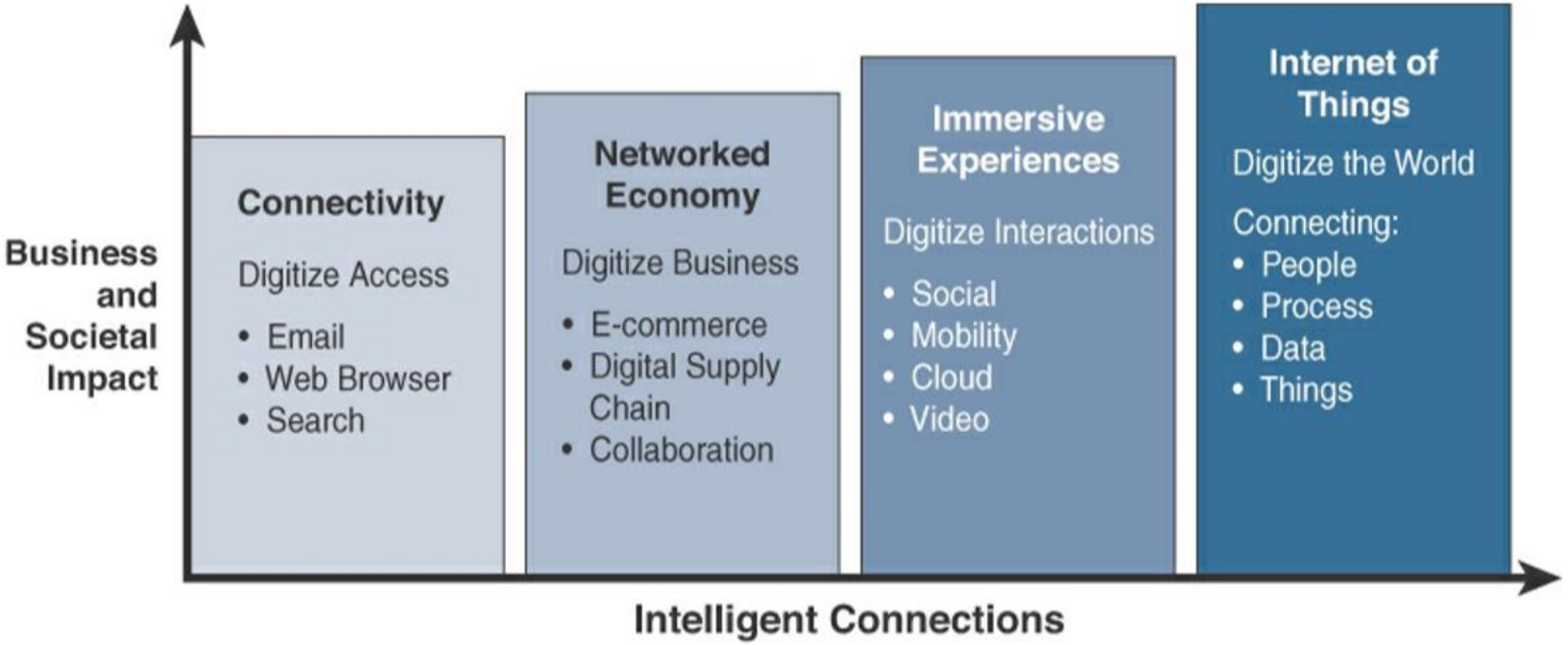


Figure 1-1 Evolutionary Phases of the Internet

Genesis of IoT

- Four phases are defined as.

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

Genesis of IoT

- The first phase, Connectivity, began in the mid-1990s. the world was not always connected as it is today.
  - In the beginning, email and getting on the Internet were luxuries for universities and corporations. Getting the average person online involved dial-up modems, and even basic connectivity often seemed like a small miracle.
- Even though connectivity and its speed continued to improve, a saturation point was reached where connectivity was no longer the major challenge.
- The focus was now on leveraging connectivity for efficiency and profit.
- This is the beginning of the second phase of the Internet evolution, called the Networked Economy.
  - With the Networked Economy, e-commerce and digitally connected supply chains became the rage, and this caused one of the major disruptions of the past 100 years.
  - The economy itself became more digitally intertwined as suppliers, vendors, and consumers all became more directly connected.

Genesis of IoT

- 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, using multiple platforms from mobile phones to tablets to laptops and desktop computers. This pervasive connectivity in turn enables communication and collaboration as well as social media across multiple channels, via email, texting, voice, and video.
  - In essence, person-to-person interactions have become digitized.
- The latest phase is the Internet of Things.
  - Despite all the talk and media coverage of IoT, in many ways we are just at the beginning of this phase. When you think about the fact that 99% of "things" are still unconnected.
  - 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

- IoT focuses on connecting “things,” such as objects and machines, to a computer network, or 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.
  - This is obvious and appreciated by shoppers, tracking real-time location of Wi-Fi clients provides a specific business benefit to the mall and shop owners.
  - It helps the business understand where shoppers tend to congregate and how much time they spend in different parts of a mall or store. Analysis of this data can lead to significant changes to the locations of product displays and advertising, where to place certain types of shops, how much rent to charge, and even where to station security guards.

IoT and Digitization

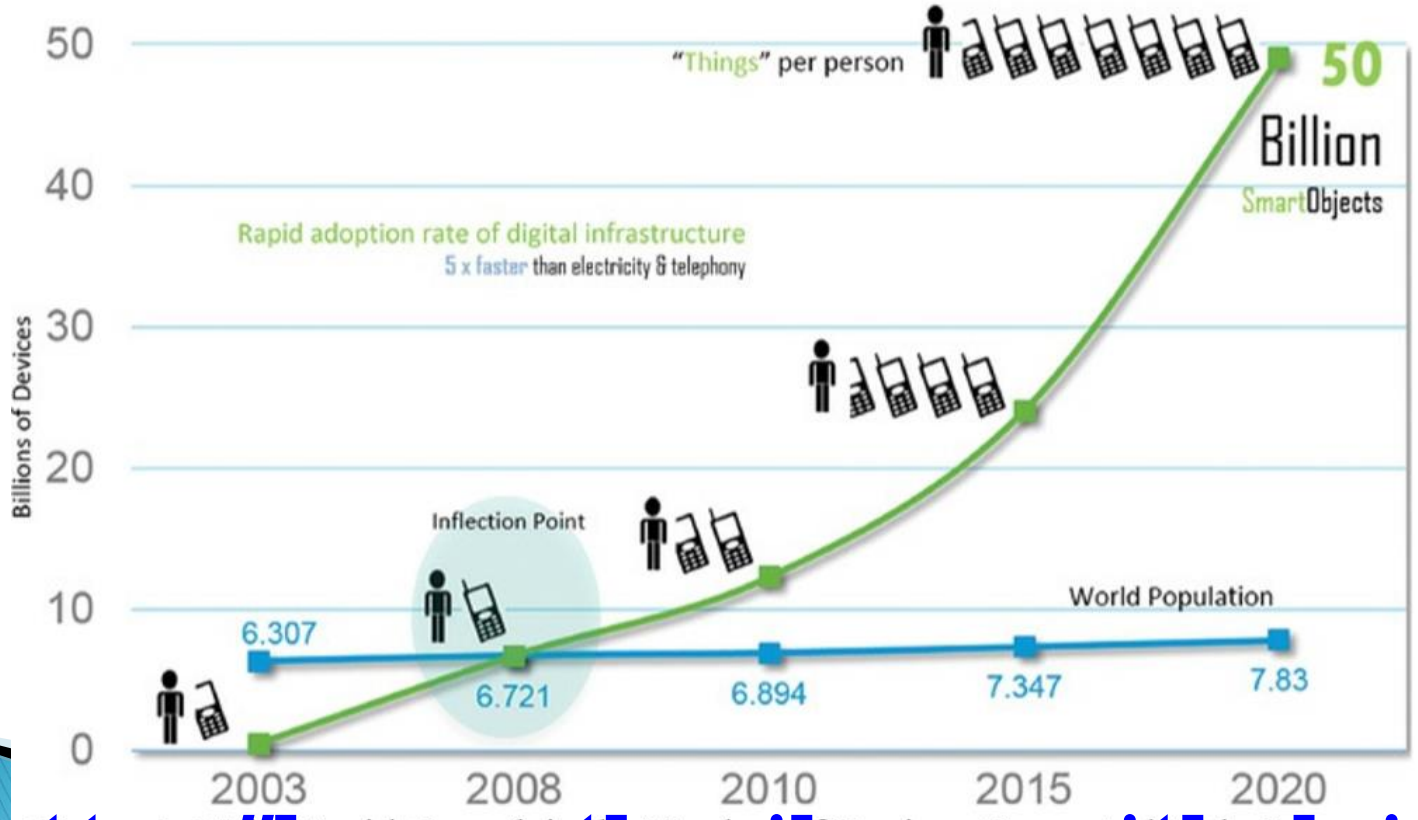
- Digitization, is the conversion of information into a digital format. Digitization has been happening in one form or another for several decades.
  - For example:
    - The whole **photography industry** has been digitized. Pretty much everyone has digital cameras these days, either standalone devices or built into their mobile phones.
    - digitization include the **video rental industry** and transportation.
    - The **transportation industry** is currently undergoing digitization in the area of taxi services. Businesses such as Uber and Ola.
    - For Example: **home automation**
- In the context of IoT, digitization brings together things, data, and business process to make networked connections more relevant and valuable.
- 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

- Projections on the potential impact of IoT are impressive. About 14 billion, or just 0.06%, of “things” are connected to the Internet today.
- By 2020, this number will reach 50 billion or more.

IoT Impact

- A graphical look at the growth in the number of devices being connected



https://hemanthrajhemu.github.io

IoT Impact

- What these numbers mean is that IoT will fundamentally shift the way people and businesses interact with their surroundings.
- Managing and monitoring smart objects using real-time connectivity enables a whole new level of data-driven decision making.
- This in turn results in the optimization of systems and processes and delivers new services that save time for both people and businesses while improving the overall quality of life.
- Following examples illustrate some of the benefits of IoT and their impact.
  - Connected Roadways
  - Connected Factory
  - Smart Connected Buildings
  - Smart Creatures

IoT Impact E.g. Connected Roadways

- People have been fantasizing about the self-driving car, or autonomous vehicle, in literature and film for decades.
- 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.
- Self-driving vehicles need always-on, reliable communications and data from other transportation-related sensors to reach their full potential.
- Connected roadways is the term associated with both the driver and driverless cars fully integrating with the surrounding transportation infrastructure.
- E.g. Self-driving car designed by Google.

IoT Impact E.g. Connected Roadways

https://hemanthrajhemu.github.io

IoT Impact E.g. Connected Roadways

- Basic sensors reside in cars already.
- They monitor oil pressure, tire pressure, temperature, and other operating conditions, and provide data around the core car functions. From behind the steering wheel, the driver can access this data while also controlling the car using equipment such as a steering wheel, pedals, and so on.
- The need for all this sensory information and control is obvious.
- It mimics like the driver.
  - 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.
  - In addition, new sensors and communication technologies are being developed to allow vehicles to "talk" to other vehicles, traffic signals, school zones, and other elements of the transportation infrastructure.

IoT Impact E.g. Connected Roadways

- Most connected roadways solutions focus on resolving today's transportation challenges. These challenges are:
  - Safety
  - Mobility
  - Environment
- These challenges (in connected roadways) will bring many benefits to society.
- These benefits include **reduced traffic jams** and urban congestion, decreased casualties and fatalities, increased response time for emergency vehicles, and reduced vehicle emissions.

IoT Impact E.g. Connected Roadways

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 Impact E.g. Connected Roadways

- **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.**
  - IMA is one of many possible roadway solutions that emerge when we start to integrate IoT with both traditional and self-driving vehicles.
    - Vehicle tracking
    - Notification of arrival times
    - Theft prevention
    - Highway assistance
    - Road weather communications

IoT Impact E.g. Connected Roadways

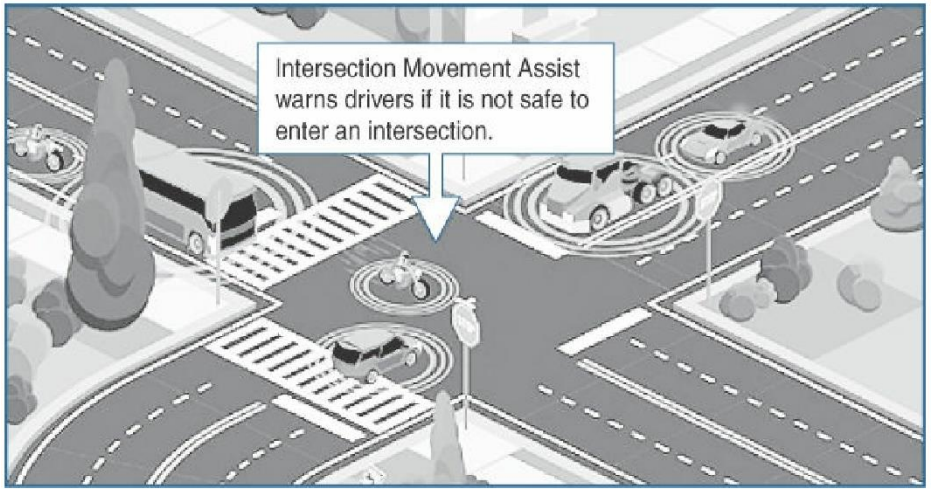


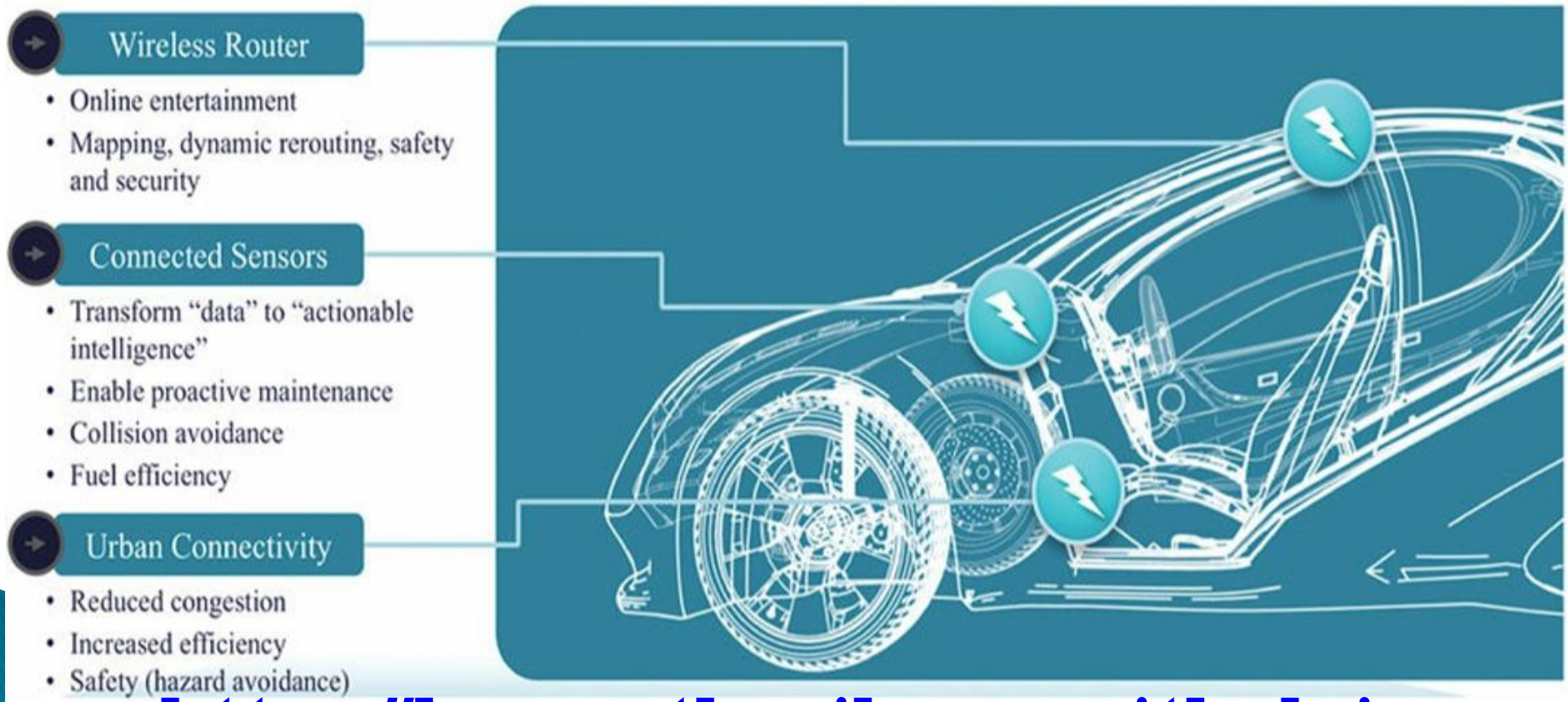
Figure 1-4 Application of Intersection Movement Assist

IoT Impact E.g. Connected Roadways

- **Vehicle Digitization**
  - As cars continue to become more connected and capable of generating continuous data streams related to location, performance, driver behavior, and much more, the data generation potential of a single car is staggering.
  - Automobile manufacturers can collect information from sensors to better understand how the cars are being driven, when parts are starting to fail, or whether the car has broken down details that will help them build better cars in the future.
    - For example, tire companies can collect data related to use and durability of their products in a range of environments in real time.

IoT Impact E.g. Connected Roadways

- The sort of sensors and connectivity that you will find in a connected car.



IoT Impact E.g. Connected Roadways

- GPS/maps,
  - to enable dynamic rerouting to avoid traffic, accidents, and other hazards.
- Internet-based
  - entertainment, including music, movies, and other streamings or downloads, can be personalized and customized to optimize a road trip.

IoT Impact E.g. Connected Factory

- 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

IoT Impact E.g. Connected Factory

- Adding another level of complication to these challenges is the fact that they often need to be **addressed at various levels of the manufacturing business.**
  - For example,
  - **Executive management** is looking for new ways to manufacture in a more cost-effective manner while balancing the rising energy and material costs.
  - Product development has time to market as the top priority.
  - **Plant managers** are entirely focused on gains in plant efficiency and operational agility.
  - **The controls and automation department** looks after the plant networks, controls, and applications and therefore requires complete visibility into all these systems.

IoT Impact E.g. Connected Factory

- With IoT solution, the sensors and 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.
- 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.

IoT Impact E.g. Connected Factory

- **Real-time location system (RTLS)**
  - An RTLS utilizes small and easily deployed Wi-Fi RFID tags that attach to virtually any material and provide real-time location and status.
  - These tags enable a facility to track production as it happens.
  - These IoT sensors allow components and materials on an assembly line to “talk” to the network.
  - If each assembly line’s output is tracked in real time, decisions can be made to speed up or slow production to meet targets, and it is easy to determine how quickly employees are completing the various stages of production.

IoT Impact E.g. Connected Factory

- Figure summarizes these four Industrial Revolutions as Industry 1.0 through Industry 4.0

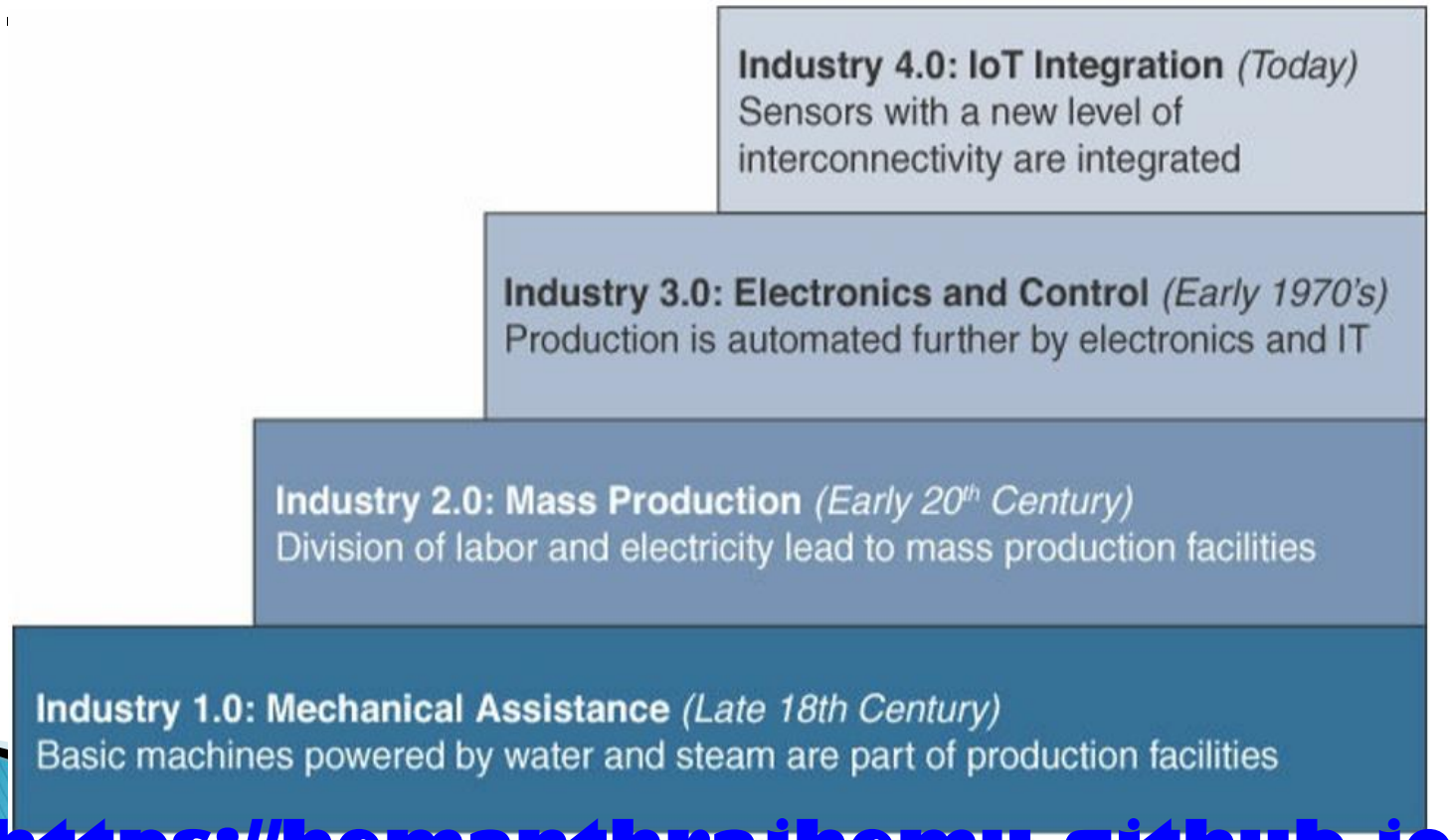


Figure 1-6 The Four Industrial Revolutions

IoT Impact E.g. Connected Factory

- The IoT wave of Industry 4.0
  - takes manufacturing from a **purely automated assembly line** model of production to a model where the machines are intelligent and communicate with one another.
  - IoT in manufacturing brings with it the opportunity for inserting intelligence into factories.
  - This starts with creating smart objects, which involves embedding sensors, actuators, and controllers into just about everything related to production.
  - Connections tie it all together so that people and machines work together to analyze the data and make intelligent decisions.
  - Eventually this leads to machines predicting failures and self-healing and points to a world where human monitoring and intervention are no longer necessary.

IoT Impact
E.g. Smart Connected Buildings

- Buildings have become increasingly complex intersections of structural, mechanical, electrical, and IT components.
- **The function of a building**
  - is to provide a work environment that keeps the workers comfortable, efficient, and safe.
  - Work areas need to be well lit and kept at a comfortable temperature.
  - To keep workers safe, the fire alarm and suppression system needs to be carefully managed, as do the door and physical security alarm systems.
- Many buildings are beginning to deploy **sensors throughout the building to detect occupancy.**
  - These tend to be motion sensors or sensors tied to video cameras.
  - Motion detection occupancy sensors work great if everyone is moving around in a crowded room and can automatically shut the lights off when everyone has left,
    - but what if a person in the room is out of sight of the sensor?
  - 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.**

IoT Impact
E.g. Smart Connected Buildings

- **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.
- The smart building is that it makes them easier and cheaper to manage.
- **Building automation**
- The **building automation system (BAS)** has been developed to provide a **single management system for the HVAC, lighting, fire alarm, and detection systems, and access control**.
  - **Heterogeneity of IoT systems.**
- Heterogeneous systems, they need to **converge at the network** layer and support a common services layer that allows application integration.

IoT Impact
E.g. Smart Connected Buildings

- **BACnet (Building Automation and Control Network)** protocol defines a set of services that allow Ethernet-based communication between building devices such as HVAC, lighting, access control, fire detection systems and IT.
  - BACnet/IP has been defined to allow the “things” in the building network to communicate over IP.

IoT Impact
E.g. Smart Connected Buildings

- Conversion of building protocols to IP over time

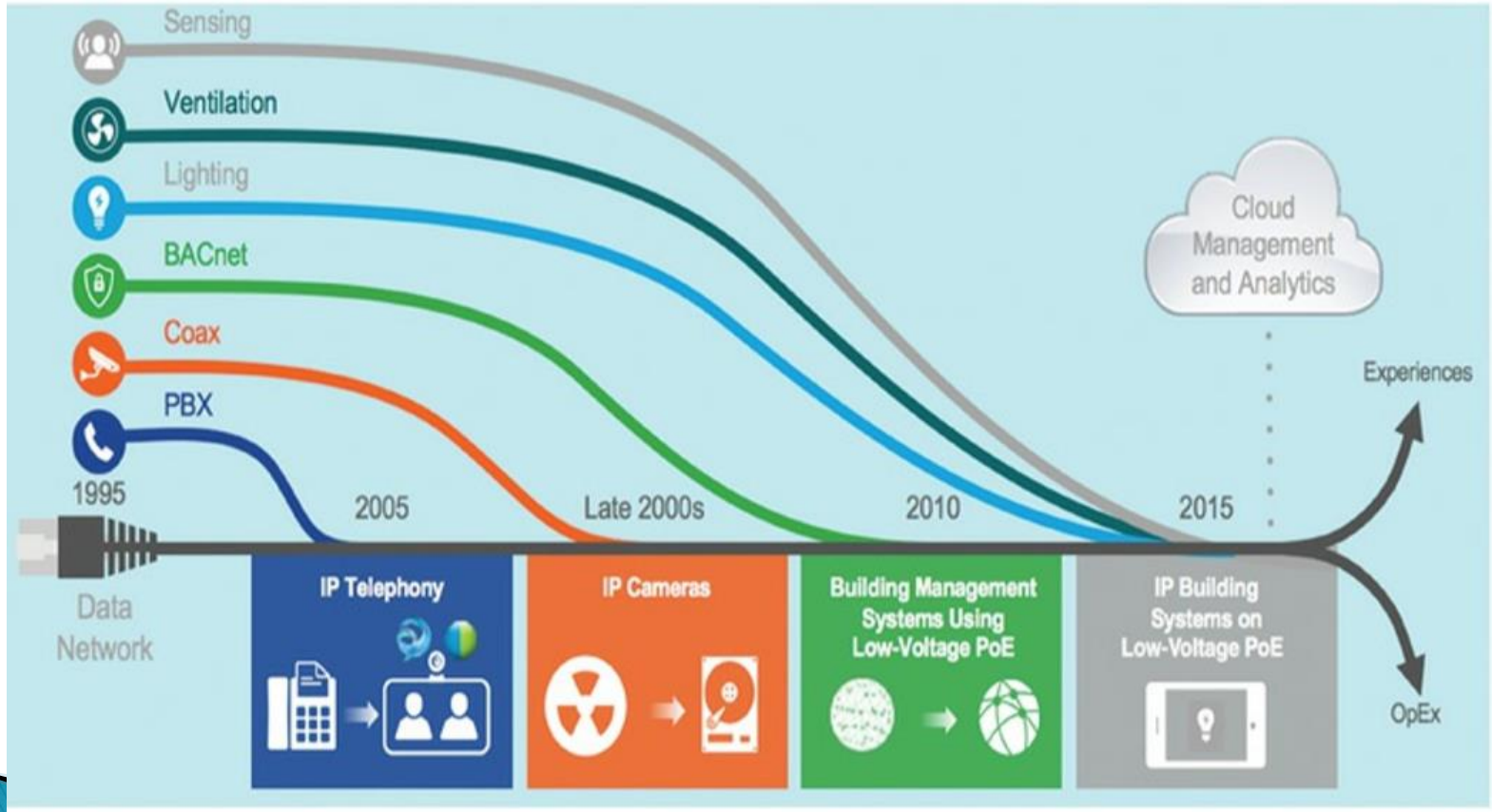


Figure 1-7 Convergence of Building Technologies to IP

IoT Impact
E.g. Smart Connected Buildings

- **Digital ceiling**
  - It is 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.

IoT Impact
E.g. Smart Connected Buildings

- Digital ceiling

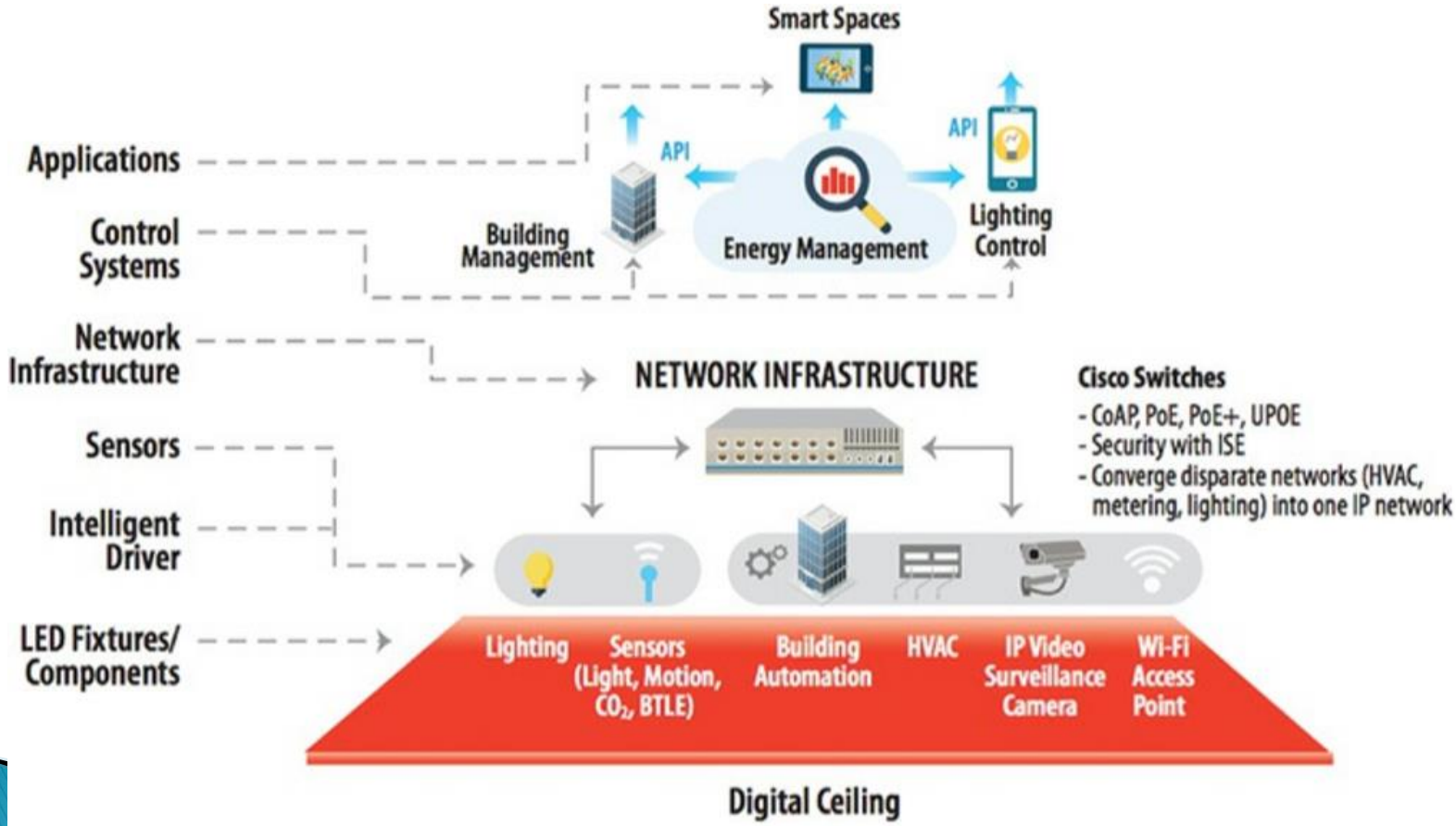
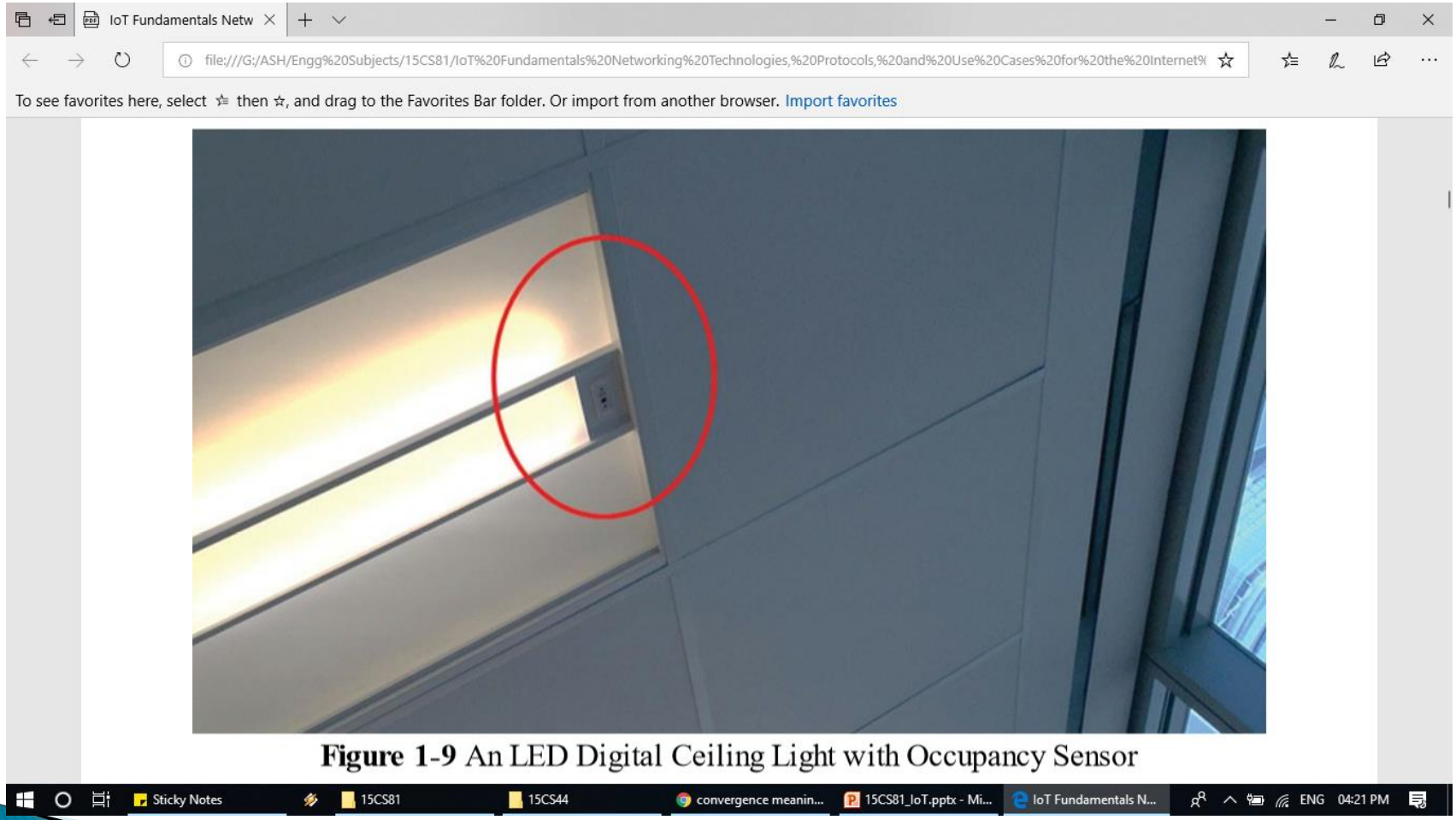


Figure 1.8 A Framework for the Digital Ceiling

IoT Impact
E.g. Smart Connected Buildings

- **Digital ceiling**
- Central to digital ceiling technology is the lighting system.
- 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.
- In a digital ceiling environment, every luminaire or lighting fixture is directly networ kattached, providing control and power over the same infrastructure.
  - The quantity of lights easily outnumbers the number of physical wired ports by a hefty margin.
  - Supporting the larger number of Ethernet ports and density of IP addresses requires some redesign of the network
  - But an **IP-enabled sensor** device in the ceiling at every point people may be present opens up an entirely new set of possibilities.
    - Most modern LED ceiling fixtures support occupancy sensors or motion sensors.

IoT Impact
E.g. Smart Connected Buildings



https://hemanthrajhemu.github.io

IoT Impact E.g. Smart Creatures

- When you think about IoT, you probably picture only inanimate objects and machines being connected.
- IoT also provides the ability to connect living things to the Internet.
  - Sensors can be placed on animals and even insects just as easily as on machines.
    - **Connected cow**
    - Electronic backpack attaches to **a Roach**

IoT Impact E.g. Smart Creatures

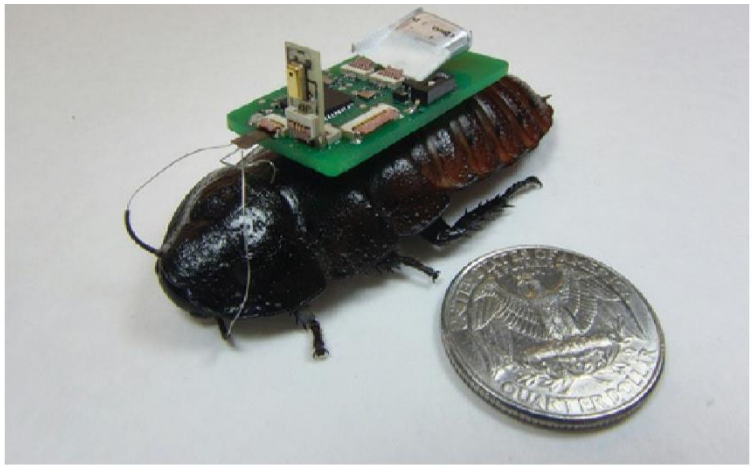


Figure 1-10 IoT-Enabled Roach Can Assist in Finding Survivors After a Disaster

Convergence of IT and OT

- Until recently, information technology (IT) and operational technology (OT) have for the most part lived in separate worlds.
  - 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.
  - OT monitors and controls devices and processes on physical operational systems.
    - These systems include assembly lines, utility distribution networks, production facilities, roadway systems, and many more.

Convergence of IT and OT

- The **IT organization** is responsible for the information systems of a business, such as email, file and print services, databases, and so on.
- **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.
- Traditionally, OT has used dedicated networks with specialized communications protocols to connect these devices, and these networks have run completely separately from the IT networks.

Convergence of IT and OT

- **Management of OT** is tied to the lifeblood of a company.
  - **Network connecting the machines in a factory fails**, the machines cannot function, and production may come to a standstill, **negatively impacting business on the order of millions of dollars**.
- **If the email server (run by the IT department) fails for a few hours**, it may irritate people, but it is unlikely to impact business at anywhere near the same level.

Convergence of IT and OT

- Comparing Operational Technology (OT) and Information Tech

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 vulnerability	Low: OT networks are isolated and often use proprietary protocols	High: continual patching of hosts is required, and the network is connected to Internet and requires vigilant

Convergence of IT and OT

- The IT and OT worlds are converging or, more accurately, OT is beginning to adopt the network protocols, technology, transport, and methods of the IT organization, the IT organization is beginning to support the operational requirements used by OT.
- When IT and OT begin using the same networks, protocols, and processes, there are clear economies of scale.
- With the merging of OT and IT, improvements are being made to both systems.
  - OT is looking more toward IT technologies with open standards, such as Ethernet and IP.
  - IT is becoming more of a business partner with OT by better understanding business outcomes and operational requirements.

IoT Challenges

- Many parts of IoT have become reality, but certain obstacles need to be overcome for IoT to become ubiquitous throughout industry and our everyday life.

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."

IoT Challenges

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.

IoT Challenges

Interoperability	As with any other nascent technology, various protocols and architectures are jockeying for market share and standardization within IoT. Some of these protocols and architectures are based on proprietary elements, and others are open. Recent IoT standards are helping minimize this problem, but there are often various protocols and implementations available for IoT networks. The prominent protocols and architectures—especially open, standards-based implementations—are the subject of this book. For more information on IoT architectures, see Chapter 2, "IoT Network Architecture and Design." Chapter 4, "Connecting Smart Objects," Chapter 5, "IP as the IoT Network Layer," and Chapter 6, "Application Protocols for IoT," take a more in-depth look at the protocols that make up IoT.

Table 1-4 IoT Challenges

IoT Network Architecture and Design

Introduction

- Network Architecture:
  - Need for Architect
  - Challenges:
    - Information technology (IT) systems need to be designed to withstand “network earthquakes,” such as distributed denial of service (DDoS) attacks, future growth requirements, network outages, and even human error.
  - Some similarities between IT and IoT architectures do exist, for the most part,
    - the challenges and requirements of IoT systems are radically different from those of traditional IT networks.
  - Challenges posed by IoT networks and how these challenges have driven new architectural models.

Introduction

- Explores the following areas for design of IoT Network:
- **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.
- **A Simplified IoT Architecture:** While several IoT architectures exist, a simplified model is a foundation for rest of the architecture.
- **The Core IoT Functional Stack**: The IoT network must be designed to support its unique requirements and constraints.
- **IoT Data Management and Compute Stack**: Introduces of data management, including storage and compute resource models for IoT, and involves edge, fog, and cloud computing.

Drivers Behind New Network Architectures

- Concepts Covered:
  - Scale
  - Security
  - Constrained Devices and Networks
  - Data
  - Legacy Device Support

Drivers Behind New Network Architectures

- 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, analyzed, and ultimately acted upon.

Drivers Behind New Network Architectures

Differences between IT and IoT networks

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.

Drivers Behind New Network Architectures
Differences between IT and IoT networks

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

The following sections expand on the requirements driving specific architectural

Drivers Behind New Network Architectures
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 traditional three layer campus networking model, supporting access, distribution, and core (with sub-architectures for WAN, Wi-Fi, data center, etc.), is well understood.
  - But now consider what happens when 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.

Drivers Behind New Network Architectures
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, the first line of defense is often the perimeter 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 analyzer but often physically accessible and widely distributed in the field.
- Traditional models of IT security are simply not designed for the new attack vectors introduced by highly dispersed IoT systems.

Drivers Behind New Network Architectures
Security

- IoT systems require consistent mechanisms of authentication, encryption, and intrusion prevention techniques that understand the behavior of industrial protocols and can respond to attacks on critical infrastructure.
- For optimum security, 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 behavior is detected from connected devices
  - Take a holistic, network-level approach to security

Drivers Behind New Network Architectures

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.**
- In IT networks, which works with multigigabit connection speeds and endpoints with powerful CPUs.
- If an IT network has performance constraints, the solution is simple:
  - **Upgrade to a faster network.**
- If too **many devices are on one VLAN and are impacting performance,** you can simply carve out a new VLAN and continue to scale as much as you need.
  - However, this approach cannot meet the constrained nature of IoT systems.
- IoT requires a new breed of connectivity technologies that meet both the scale and constraint limitations.

Drivers Behind New Network Architectures

Data

- **IoT devices generate a mountain of data.**
  - IT shops don't really care much about the **unstructured chatty data** generated by devices on the network.
- **In IoT the data is like gold,**
  - as it is what enables businesses to deliver new IoT services that enhance the customer experience, reduce cost, and deliver new revenue opportunities.
  - Although most IoT-generated data is unstructured, the insights it provides through analytics can revolutionize processes and create new business models.
  - E.g. Imagine a smart city with a few hundred thousand **smart streetlights**, all connected through an IoT network. Although most of the information communicated between the lighting network modules and the control center is of little interest to anyone, patterns in this data can yield extremely useful insights that can help predict when lights need to be replaced or whether they can be turned on or off at certain times, thus saving operational expense.
- However, when all this data is combined, it can become difficult to manage and analyze effectively.
- Unlike IT networks, 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.**

Drivers Behind New Network Architectures

Legacy Device Support

- **Supporting legacy devices in an IT organization is not usually a big problem.**
  - Computer or operating system or mobile phone is outdated, can simply forcibly **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. In many cases, legacy devices are so old that they don't even support IP.
  - For example, **a factory may replace machines only once every 20 years or perhaps even longer.** It does not want to upgrade multi-million-dollar machines just so it can connect them to a network for better visibility and control. However, many of these legacy machines might support older protocols, such as serial interfaces, and use RS-232. In this case, 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

- Architecture Standards:
  - The oneM2M IoT Standardized Architecture
  - The IoT World Forum (IoTWF) Standardized Architecture
    - Layer 1: Physical Devices and Controllers Layer
    - Layer 2: Connectivity Layer
    - Layer 3: Edge Computing Layer
    - Upper Layers: Layers 4–7
  - IT and OT Responsibilities in the IoT Reference Model
  - Additional IoT Reference Models

Comparing IoT Architectures
The oneM2M IoT Standardized Architecture

- Standardising the machine-to-machine (M2M) communications.
  - The **European Telecommunications Standards Institute (ETSI)** created the **M2M common architecture** that would help accelerate the adoption of M2M applications and devices.
- **oneM2M** (launched by ETSI)
  - is to create a common services layer, which can be readily embedded in field devices to allow communication with application servers.
  - oneM2M's framework focuses on IoT services, applications, and platforms.
    - These include smart metering applications, smart grid, smart city automation, e-health, and connected vehicles.

Comparing IoT Architectures The oneM2M IoT Standardized Architecture

- **IoT architecture is dealing with the heterogeneity of devices, software, and access methods.**
  - oneM2M is developing standards that allow interoperability at all levels of the IoT stack.
  - E.g. Automate HVAC system by connecting it with wireless temperature sensors spread throughout your office.
  - Sensors that uses LoRaWAN (Long Range Wide Area Network) technology.
  - **The problem is that the LoRaWAN network and the BACnet system that HVAC and BMS run on are completely different systems and have no natural connection point.**
  - **This is where the oneM2M common services architecture comes in.**
    - oneM2M's horizontal framework and RESTful APIs allow the LoRaWAN system to interface with the building management system over an IoT network, thus promoting end-to-end IoT communications in a consistent way, no matter how heterogeneous the networks.
- oneM2M architecture divides IoT functions into three major domains: the application layer, the services layer, and the network layer.

Comparing IoT Architectures
The oneM2M IoT Standardized Architecture

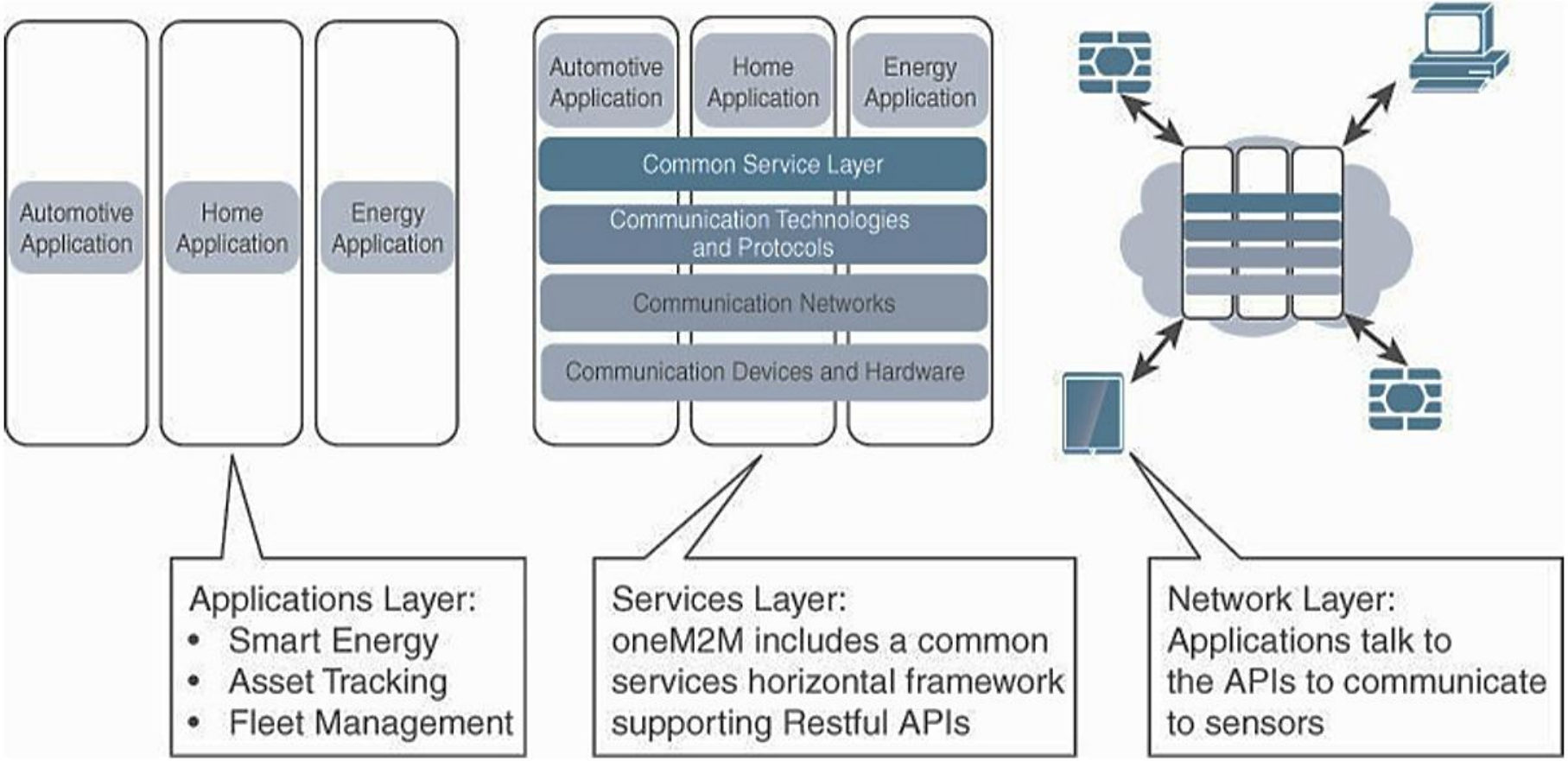


Figure 2-1 The Main Elements of the oneM2M IoT Architecture

Comparing IoT Architectures
The oneM2M IoT Standardized 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.

Comparing IoT Architectures
The oneM2M IoT Standardized Architecture

- **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 (Multiprotocol Label Switching), VPNs (virtual private network), and so on.
- Riding on top is the common services layer. This conceptual layer adds APIs and middleware supporting third-party services and applications.
- The goals of oneM2M is to "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."
  - A critical objective of oneM2M is to attract and actively involve organizations from M2Mrelated business domains, including telematics and intelligent transportation, healthcare, utility, industrial automation, and smart home applications, to name just a few.

Comparing IoT Architectures
The oneM2M IoT Standardized Architecture

- **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.
    - Wireless mesh technologies
      - IEEE 802.15.4,
    - Wireless point-to-multipoint systems
      - IEEE 801.11ah.
    - Wired device connections
      - IEEE 1901 power line communications

Comparing IoT Architectures
The oneM2M IoT Standardized Architecture

- In many cases, **the smart (and sometimes not-so-smart) devices communicate with each other.**
- In other cases, **machine-to-machine communication is not necessary, and the devices simply communicate through a field area network (FAN)** to usecase-specific apps in the IoT application domain.
- Therefore, the device domain also includes the gateway device, which provides communications up into the core network and acts as a demarcation point between the device and network domains.

Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

- A seven-layer IoT architectural reference model.
- IoT World Forum offers a clean, simplified perspective on IoT and includes edge computing, data storage, and access.

Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

model. Figure 2-2 details the IoT Reference Model published by the IoTWF.

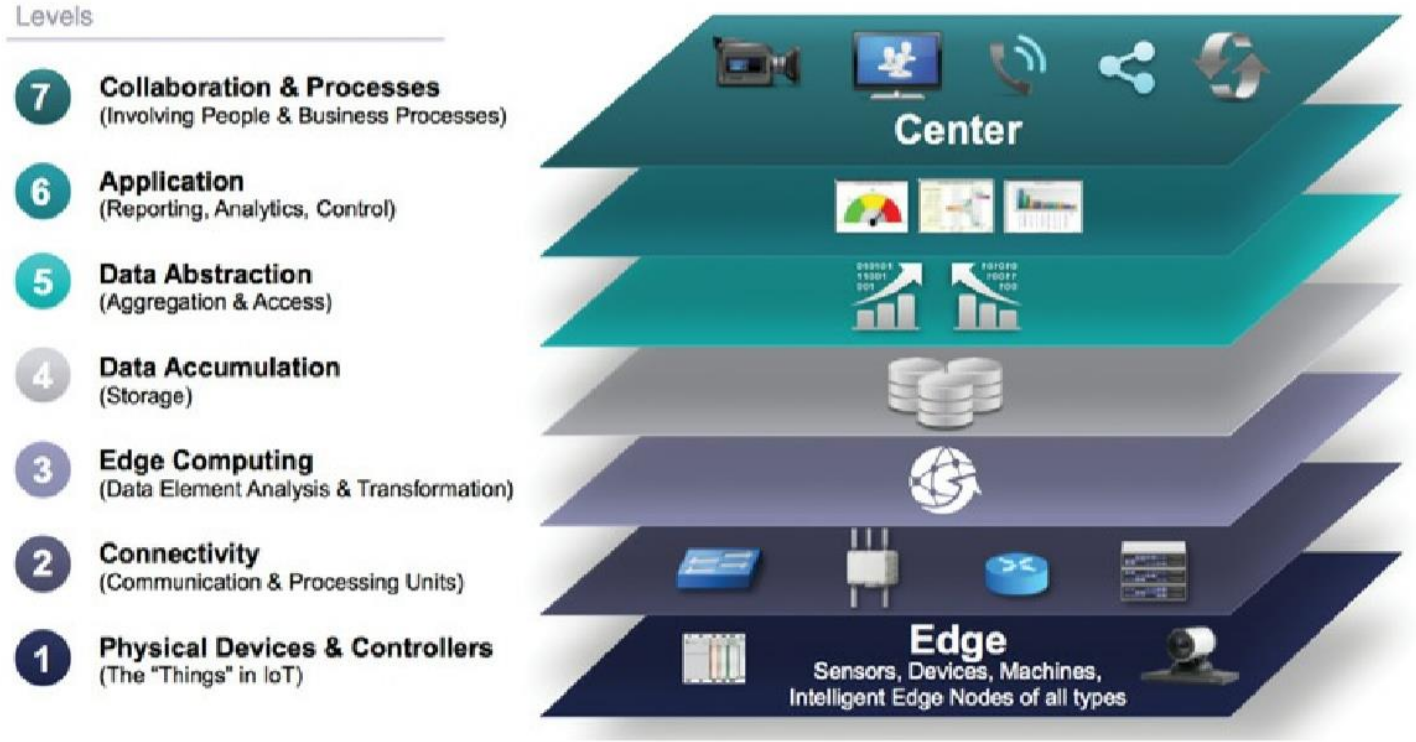


Figure 2-2 IoT Reference Model Published by the IoT World Forum

As shown in Figure 2-2, the IoT Reference Model defines a set of levels with control

Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

- The IoT Reference Model defines a set of levels with control flowing from
  - the center (this could be either a cloud service or a dedicated data center),
  - to the edge, which includes sensors, devices, machines, and other types of intelligent end nodes.
- In general, data travels up the stack, originating from the edge, and goes northbound to the center.

Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

- Using this reference model, 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

Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

- **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.

Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

- Layer 2: Connectivity Layer

② **Connectivity**
(Communication and Processing Units)

Layer 2 Functions:

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

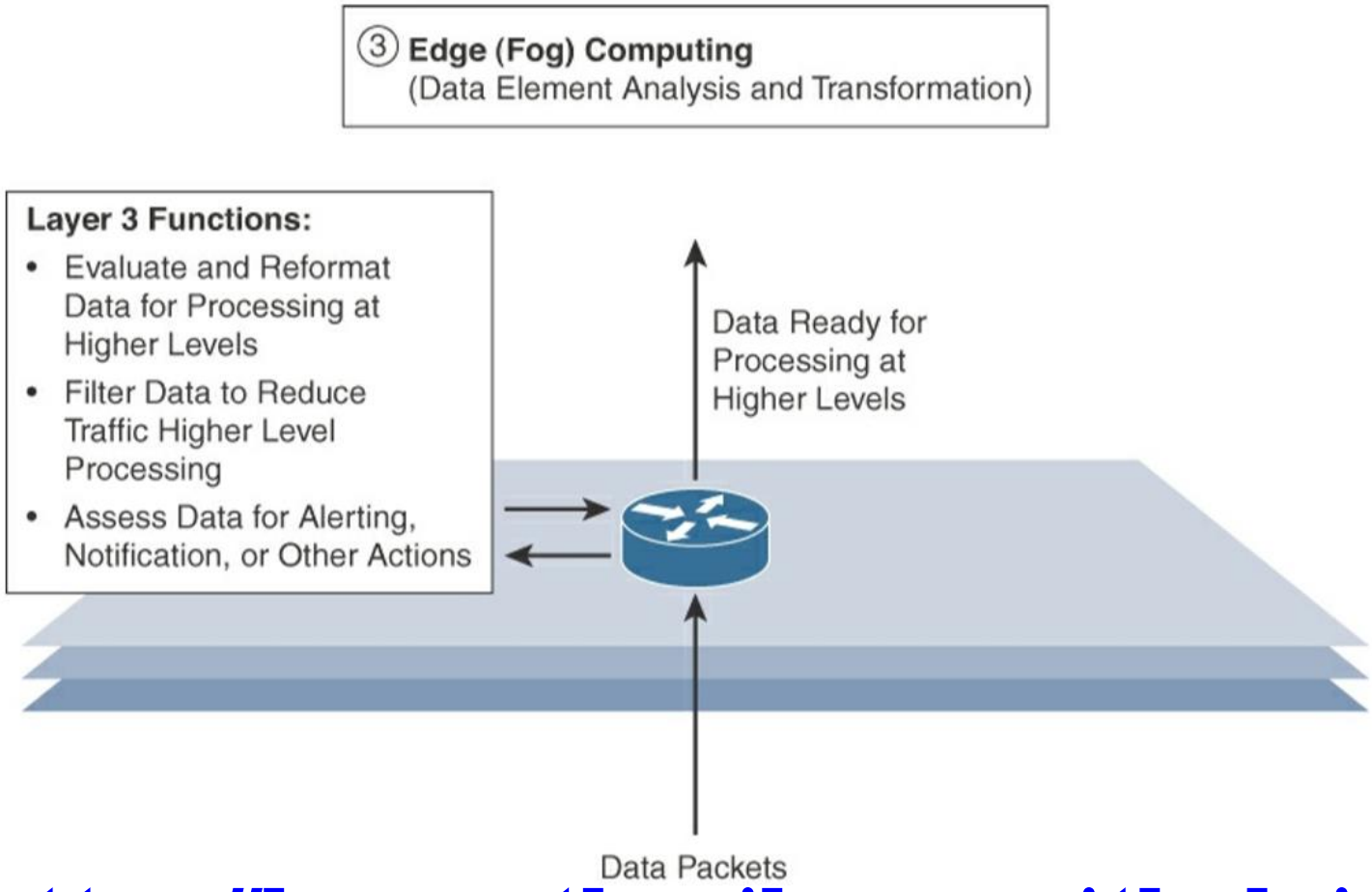
Figure 2-3 IoT Reference Model Connectivity Layer Functions

Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

- **Layer 2: Connectivity Layer**
- The connectivity layer encompasses all networking elements of IoT and doesn't really distinguish between the last-mile network (the network between the sensor/endpoint and the IoT gateway), gateway, and backhaul networks.

Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

- Layer 3: Edge Computing Layer



Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

- **Layer 3: Edge Computing Layer**
- Edge computing is often referred to as the "Fog Computing".
- 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.
- One of the basic principles of this reference model is that information processing is initiated as early and as close to the edge of the network as possible.
- The data can be filtered or aggregated before being sent to a higher layer.
  - This also allows for data to 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.

Comparing IoT Architectures
The IoT World Forum (IoTWF) Standardized Architecture

- Upper Layers: Layers 4–7

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.

Comparing IoT Architectures
IT and OT Responsibilities in the IoT Reference Model

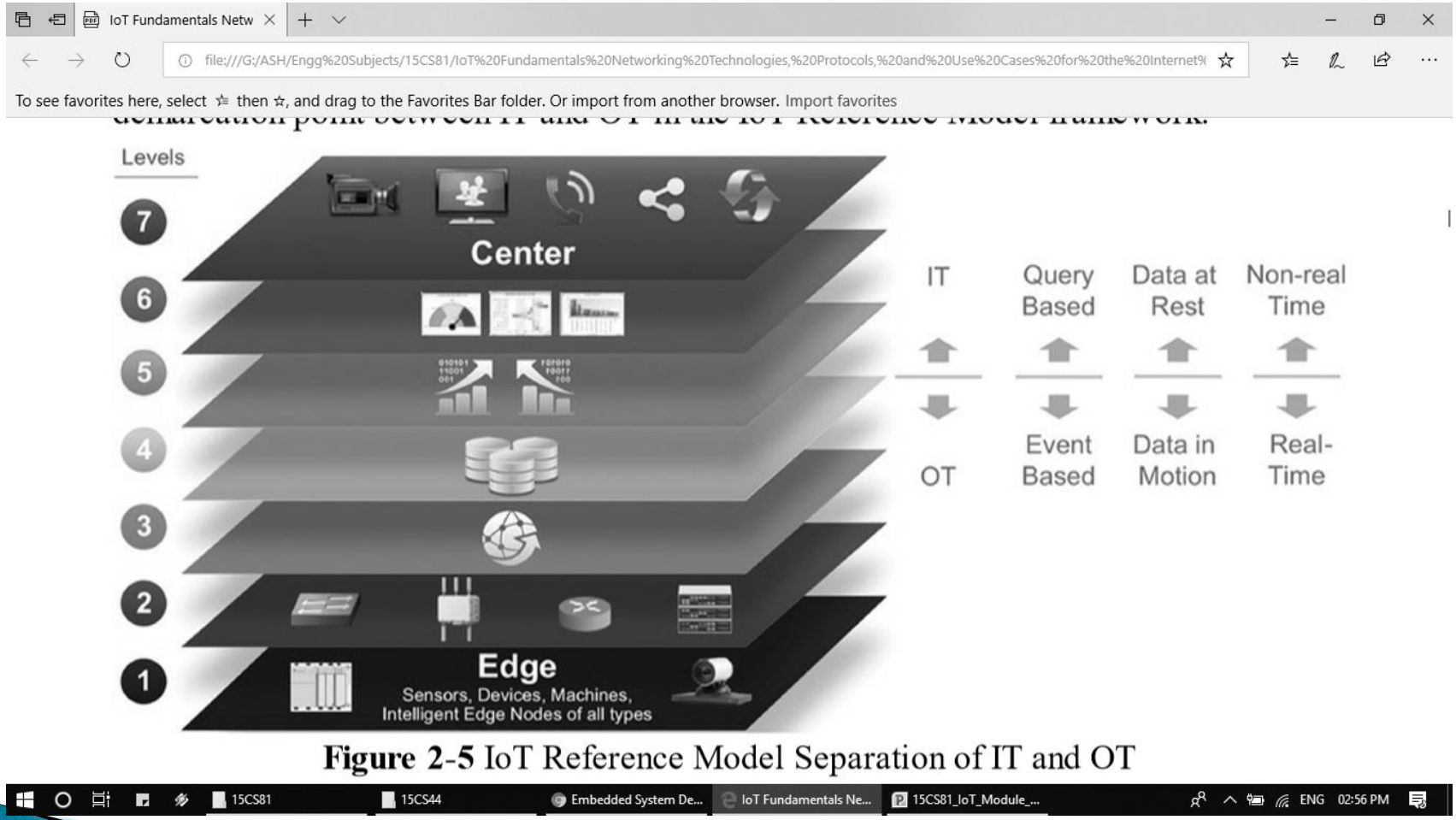


Figure 2-5 IoT Reference Model Separation of IT and OT

Comparing IoT Architectures
IT and OT Responsibilities in the IoT Reference Model

- 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
  - includes things like the servers, databases, and applications, all of which run on a part of the network controlled by IT.
- In the past, OT and IT have generally been very independent and had little need to even talk to each other.
- IoT is changing that paradigm.

Comparing IoT Architectures
IT and OT Responsibilities in the IoT Reference Model

- At the bottom, in the OT layers, the devices generate real-time data at their own rate sometimes vast amounts on a daily basis.
  - In a 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.
- As a result, 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.

Comparing IoT Architectures
Additional IoT Reference Models

IoT Reference Model	Description
Purdue Model for Control Hierarchy	The Purdue Model for Control Hierarchy (see www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG/ch2_EttF.pdf) is a common and well-understood model that segments devices and equipment into hierarchical levels and functions. It is used as the basis for ISA-95 for control hierarchy, and in turn for the IEC-62443 (formerly ISA-99) cyber security standard. It has been used as a base for many IoT-related models and standards across industry. The Purdue Model's application to IoT is discussed in detail in Chapter 9, "Manufacturing," and in Chapter 10, "Oil & Gas."
Industrial Internet Reference Architecture (IIRA) by Industrial Internet Consortium (IIC)	The IIRA is a standards-based open architecture for Industrial Internet Systems (IISs). To maximize its value, the IIRA has broad industry applicability to drive interoperability, to map applicable technologies, and to guide technology and standard development. The description and representation of the architecture are generic and at a high level of abstraction to support the requisite broad industry applicability. The IIRA distills and abstracts common characteristics, features and patterns from use cases well understood at this time, predominantly those that have been defined in the IIC. For more information, see www.iiconsortium.org/IIRA.htm.

Comparing IoT Architectures
Additional IoT Reference Models

Internet of Things–Architecture (IoT-A)	IoT-A created an IoT architectural reference model and defined an initial set of key building blocks that are foundational in fostering the emerging Internet of Things. Using an experimental paradigm, IoT-A combined top-down reasoning about architectural principles and design guidelines with simulation and prototyping in exploring the technical consequences of architectural design choices. For more information, see https://vdivde-it.de/en.

Table 2-3 Alternative IoT Reference Models

A Simplified IoT Architecture

- This framework is presented as two parallel stacks:
  - The IoT Data Management and Compute Stack and the Core IoT Functional Stack.
  - Reducing the framework down to a pair of three-layer stacks.
    - Basic model

A Simplified IoT Architecture

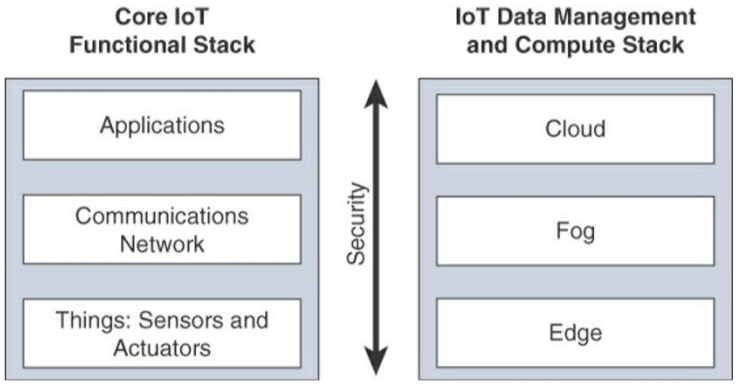


Figure 2-6 Simplified IoT Architecture

A Simplified IoT Architecture

- Nearly every IoT model includes core layers similar to those shown on the left side of architecture, including "things," a communications network, and applications.
- The framework presented here separates the core IoT and data management into parallel and aligned stacks.
- A simple architecture needs to be expanded on
  - The network communications layer: needs to consolidate the gateway and backhaul technologies, and ultimately bring the data back to a central location for analysis and processing. .
  - IoT sensors and the many different ways that exist to connect them to a network.

A Simplified IoT Architecture

- The network between the gateway and the data center is composed mostly of traditional technologies that experienced IT professionals would quickly recognize.
- These include
  - tunneling and VPN (Virtual Private Network) technologies,
  - IP-based quality of service (QoS),
  - conventional Layer 3 routing protocols
    - such as BGP and IP-PIM,
  - security capabilities
    - such as encryption, access control lists (ACLs), and firewalls.

A Simplified IoT Architecture

- In 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
  - allowing data collection, analytics, and intelligent controls at multiple points in the IoT system.
- In the model presented in figure 2-6, 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),
  - fog layer (data management in the gateways and transit network),
  - cloud layer (data management in the cloud or central data center).

A Simplified IoT Architecture

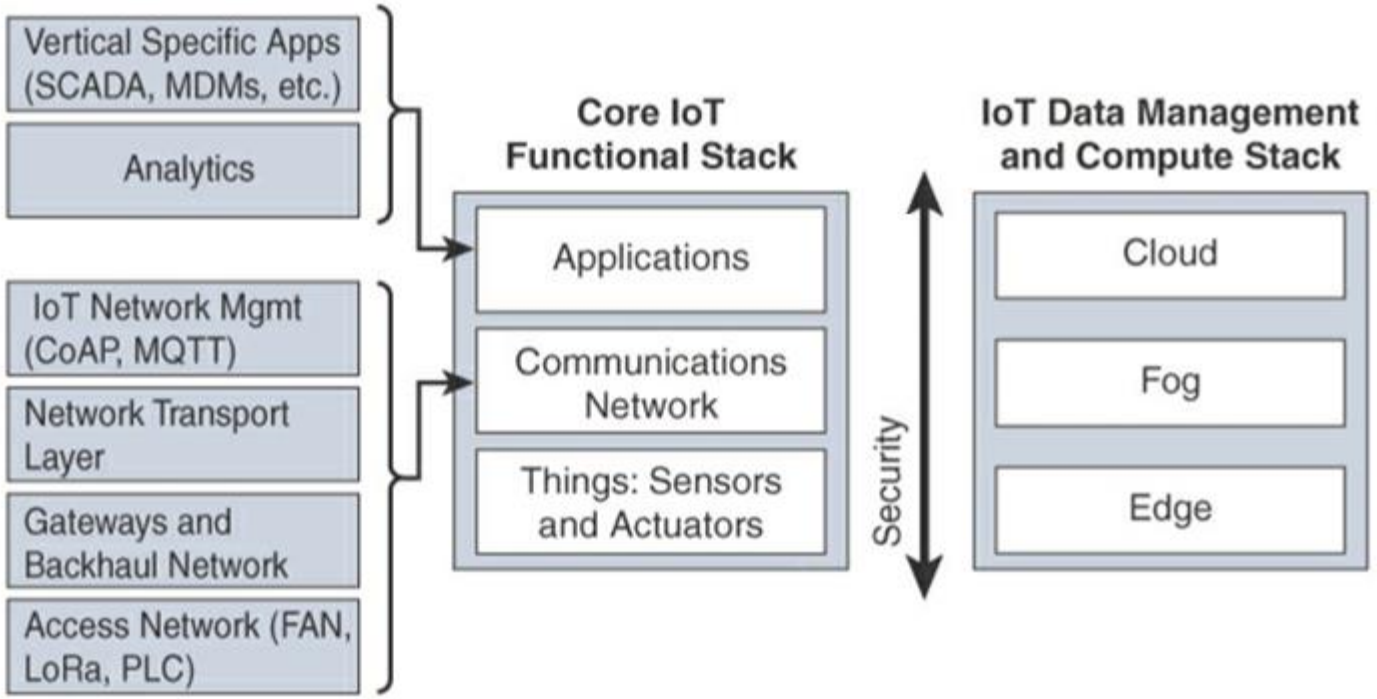


Figure 2-7 Expanded View of the Simplified IoT Architecture

The architectural framework presented in Figure 2-7 reflects the flow of the topics in this Subject

A Simplified IoT Architecture

- Core IoT Functional Stack can be expanded into sublayers
  - **Network functions:**
- **The communications layer** is broken down into four separate sublayers:
  - the access network,
  - gateways and backhaul,
  - IP transport,
  - operations and management sublayers.
- **The applications layer** of IoT networks
  - IoT often involves a strong big data analytics component
  - Thus, the applications layer typically has both analytics and industry-specific IoT control system components
- **Security** is central to the entire architecture, both from network connectivity and data management perspectives

The Core IoT Functional Stack

- IoT networks are built around the concept of **"things," or smart objects.**
- These objects are "smart" because they use a combination of contextual information and configured goals to perform actions.
  - These actions can be **self-contained** (that is, the smart object does not rely on external systems for its actions);
  - however, in most cases, **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 behavior of the smart object.

The Core IoT Functional Stack

- The components of an IoT network:
  - Things Layer
  - Communications network layer:
    - Access network sublayer
    - Gateways and backhaul network sublayer
    - Network transport sublayer
    - IoT network management sublayer
  - Application and analytics layer

- **"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.

The Core IoT Functional Stack

- **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:
  - **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.
  - **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.
  - **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.
  - **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

The Core IoT Functional Stack

- **Application and analytics layer:**
- At the upper layer, an application needs 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 analyzed conditions and change their behaviors or parameters.

The Core IoT Functional Stack
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 architectural classification could be:
  - Battery-powered or power-connected
  - Mobile or static
  - Low or high reporting frequency
  - Simple or rich data
  - Report range
  - Object density per cell

The Core IoT Functional Stack
Layer 1: Things: Sensors and Actuators Layer

- **Battery-powered or power-connected:**
  - 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.

The Core IoT Functional Stack
Layer 1: Things: Sensors and Actuators Layer

- **Mobile or static:**
  - "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 drives the possible power source.

The Core IoT Functional Stack
Layer 1: Things: Sensors and Actuators Layer

- **Low or high reporting frequency:**
  - 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.

The Core IoT Functional Stack
Layer 1: Things: Sensors and Actuators Layer

- **Simple or rich data:**
  - 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).
  - 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 case the flow structure looks bursty).

The Core IoT Functional Stack
Layer 1: Things: Sensors and Actuators Layer

- **Report range:**
  - 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.
    - The assumption is that your phone needs to be at visual distance for you to consult the reported data on the phone screen.
    - If the phone is far away, you typically do not use it, and reporting data from the band to the phone is not necessary.
    - A moisture sensor in the asphalt of a road may need to communicate with its reader several hundred meters or even kilometers away.

The Core IoT Functional Stack
Layer 1: Things: Sensors and Actuators Layer

- **Object density per cell:**
- the number of smart objects (with a similar need to communicate) over a given area, connected to the same gateway.
  - An oil pipeline may utilize a single sensor at key locations every few miles.
  - telescope at the Whipple Observatory deploy hundreds, and sometimes thousands, of mirrors over a small area, each with multiple gyroscopes, gravity, and vibration sensors.

The Core IoT Functional Stack
Layer 1: Things: Sensors and Actuators Layer

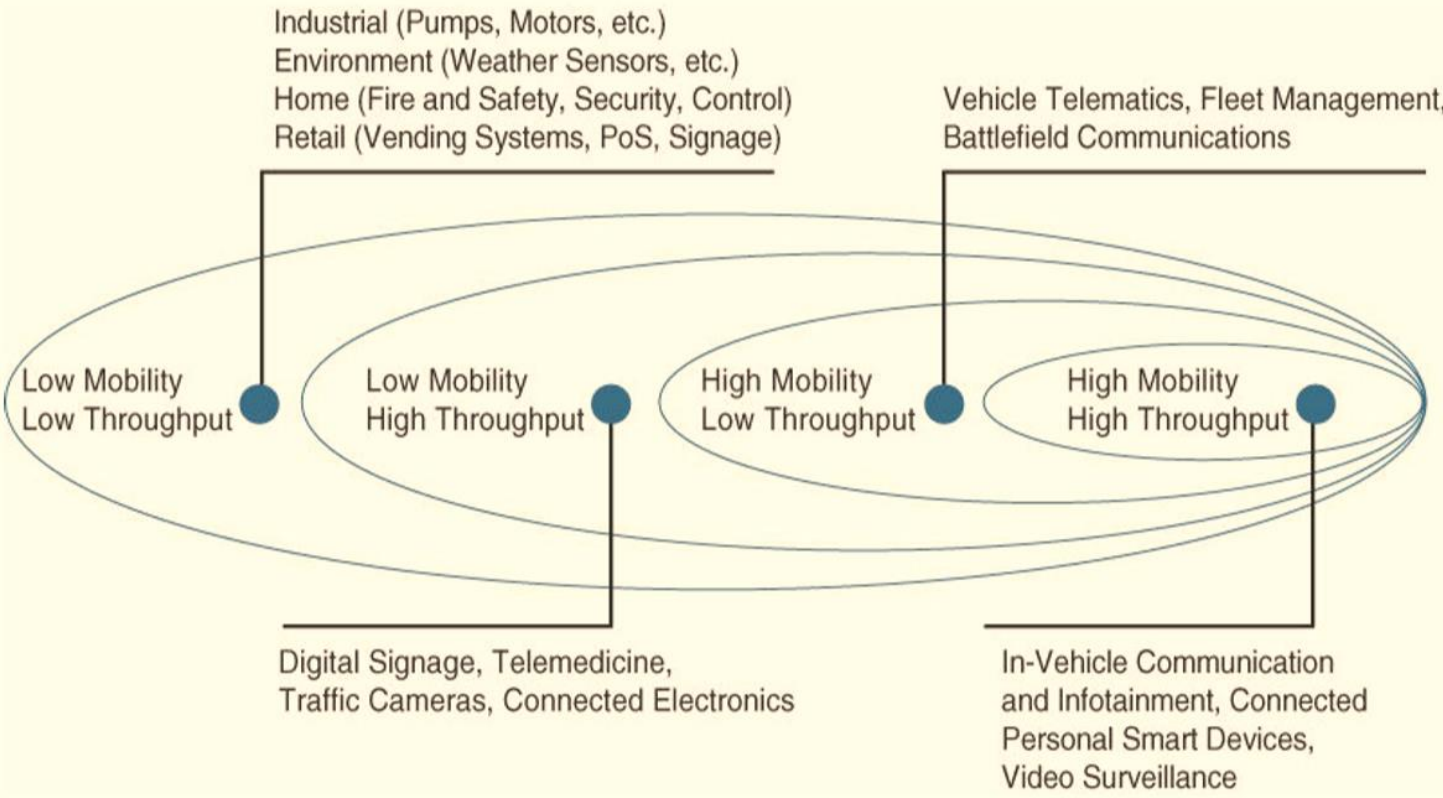


Figure 2-8 Example of Sensor Applications Based on Mobility and Throughput

The categories used to classify things can influence other parameters and can also

The Core IoT Functional Stack
Layer 1: Things: Sensors and Actuators Layer

- These sensors either need to have a constant source of power (resulting in limited mobility) or need to be easily accessible for battery replacement (resulting in limited transmission range).
- A first step in designing an IoT network is to examine the requirements in terms of mobility and data transmission (how much data, how often).

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Once you have determined the influence of the smart object form factor over its transmission capabilities (transmission range, data volume and frequency, sensor density and mobility), you are ready to connect the object and communicate.
- Compute and network assets used in IoT can be very different from those in IT environments.
- The difference in the physical form factors between devices used by IT and OT is obvious even to the most casual of observers.
  - What typically drives this is the physical environment in which the devices are deployed.
  - What may not be as inherently obvious, however, is their operational differences.
  - The operational differences must be understood in order to apply the correct handling to secure the target assets.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Temperature sensor variance
  - The cause for the variance is easily attributed to external weather forces and internal operating conditions.
- Humidity fluctuations can impact the long-term success of a system as well.
- In some conditions, the systems could be exposed to direct liquid contact such as may be found with outdoor wireless devices or marine condition deployments.
- Kinetic forces.
- Shock and vibration needs vary based on the deployment scenario.
- In some cases, the focus is on low amplitude but constant vibrations, as may be expected on a bushing-mounted manufacturing system.
- In other cases, it could be a sudden acceleration or deceleration

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Solid particulates can also impact the gear.
- Hazardous location design may also cause corrosive impact to the equipment.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **Access Network Sublayer:**
- There is a direct relationship between the IoT network technology you choose and the type of connectivity topology this technology allows.
  - Each technology was designed with a certain number of use cases in mind (what to connect, where to connect, how much data to transport at what interval and over what distance).
  - These use cases determined 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.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- An access technology will be required.
  - IoT sometimes reuses existing access technologies
  - Whereas some access technologies were developed specifically for IoT use cases.

The Core IoT Functional Stack Layer 2: Communications Network Layer

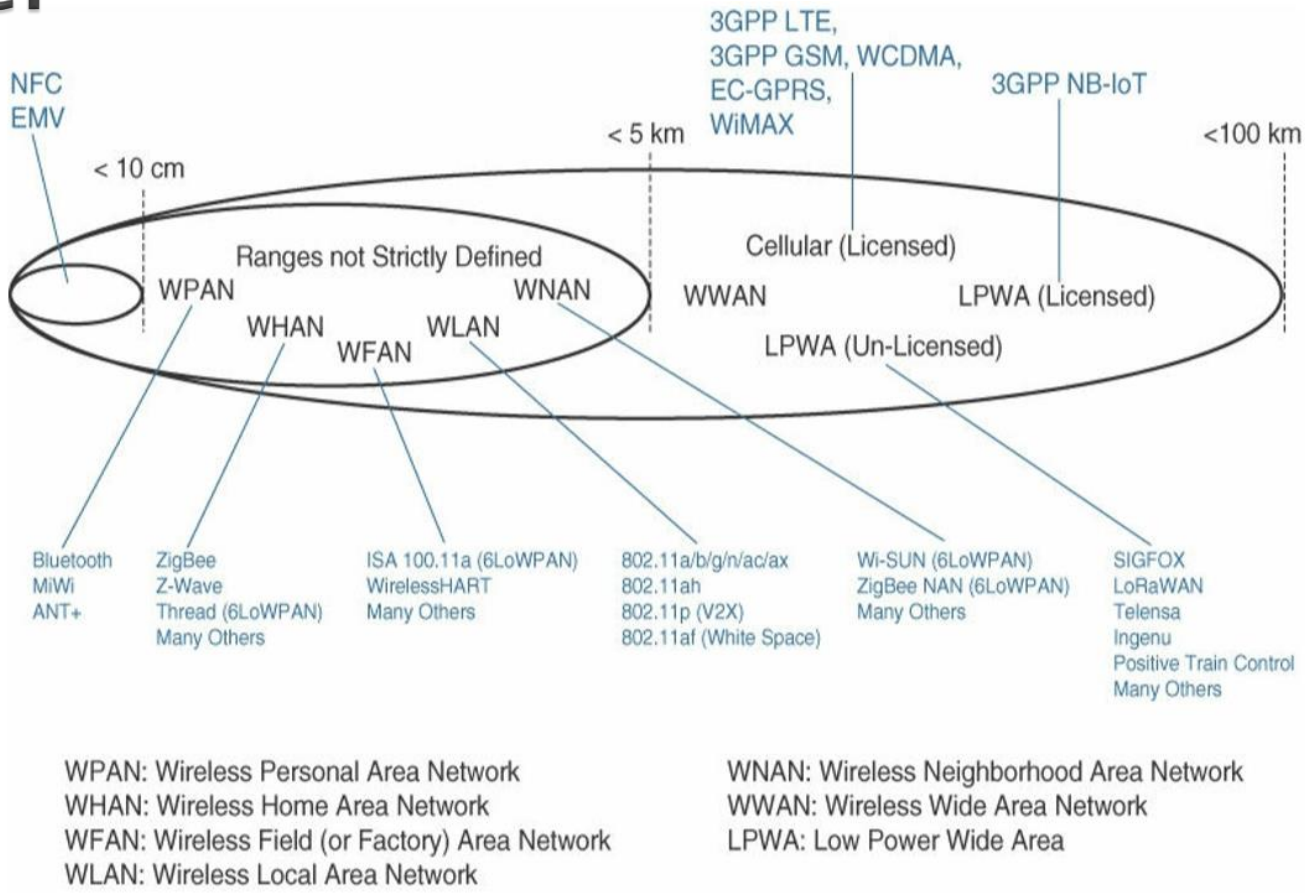


Figure 2-9 Access Technologies and Distances

The Core IoT Functional Stack Layer 2: Communications Network Layer

- For example,
  - Cellular is indicated for transmissions beyond 5 km, but you could achieve a successful cellular transmission at shorter range (for example, 100 m).
  - ZigBee is expected to be efficient over a range of a few tens of meters, but you would not expect a successful ZigBee transmission over a range of 10 km.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- 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 (neighborhood 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.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **FAN (field area network)**: Scale of several tens of meters to several hundred meters.
  - FAN typically refers to an outdoor area larger than a single 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,
    - FAN can be as a group of HANs or a group of smaller outdoor cells.
    - As you can see, FAN and NAN may sometimes be used interchangeably.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- LAN (local area network):
  - Scale of up to 100 m.
    - 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.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Similar achievable distances do not mean similar protocols and similar characteristics.
- Each protocol uses a specific frame format and transmission technique over a specific frequency (or band).
- These characteristics introduce additional differences.

The Core IoT Functional Stack Layer 2: Communications Network Layer

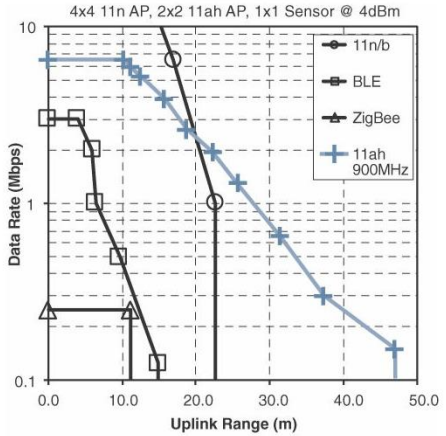


Figure 2-10 Range Versus Throughput for Four WHAN to WLAN Technologies

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Increasing the throughput and achievable distance typically comes with an increase in power consumption.
- First, 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.

The Core IoT Functional Stack Layer 2: Communications Network Layer

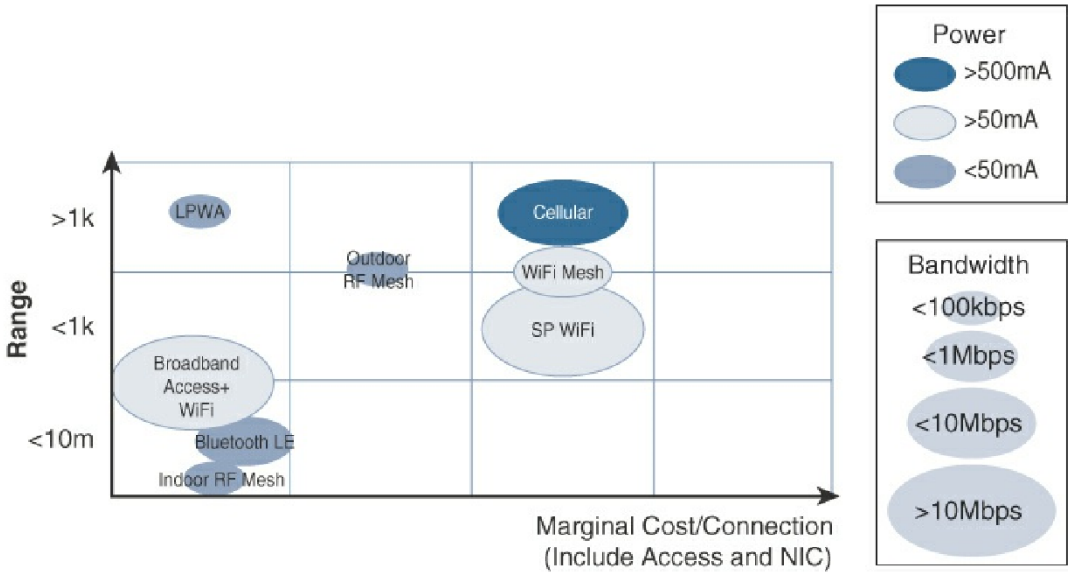


Figure 2-11 Comparison Between Common Last-Mile Technologies in Terms of Range Versus Cost, Power, and Bandwidth

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Some technologies offer flexible connectivity structure to extend communication possibilities:
  - Point-to-point topologies
  - Point-to-multipoint topologies

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **Point-to-point topologies:**
  - These topologies allow one point to communicate with another point. This topology in its strictest sense is uncommon for IoT access, as it would imply that a single object can communicate only with a single gateway.
- **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. However, depending on the features available on each communicating mode, several subtypes need to be considered.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Technology that categorizes nodes based on their function is
  - E.g IEEE 802.15.4
- To form a network, a device needs to connect with another device. When both devices fully implement the protocol stack functions, they can form a peer-to-peer network. However, in many cases, one of the devices collects data from the others.
  - For example, in a house, temperature sensors

The Core IoT Functional Stack Layer 2: Communications Network Layer

- IEEE 802.15.4 standard,
  - The central point is called a coordinator for the network.
  - 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).**
    - An RFD cannot be a coordinator.
    - An RFD also cannot implement direct communications to another RFD.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- 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, forming multiple peer-to-peer connections.
- Topologies where each FFD has a unique path to another FFD are called cluster tree topologies.
- FFDs in the cluster tree may have RFDs, resulting in a cluster star topology.

The Core IoT Functional Stack Layer 2: Communications Network Layer

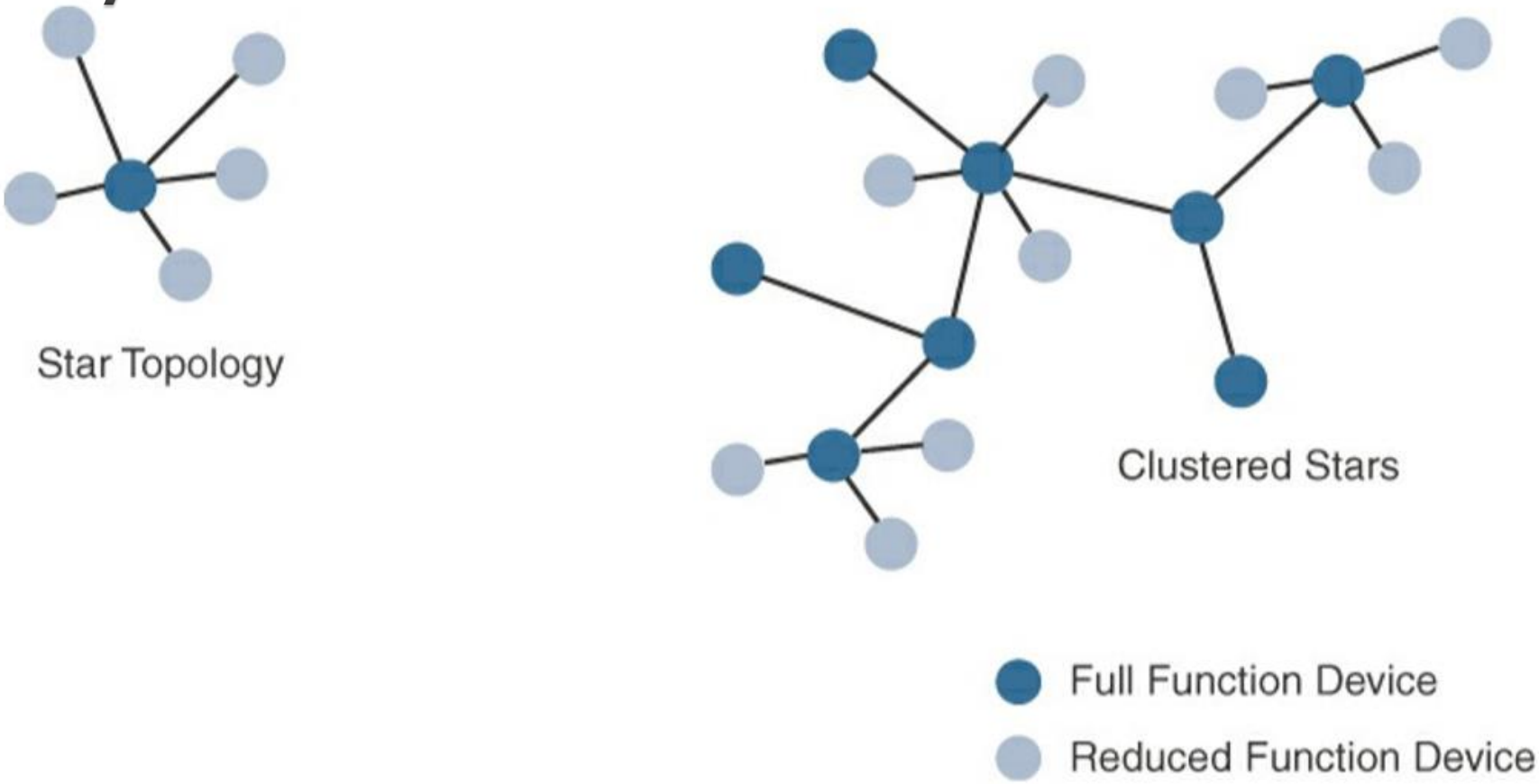


Figure 2-12 Star and Clustered Star Topologies

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **A mesh topology**
  - Other point-to-multipoint technologies allow a node to have more than one path to another node.
  - This redundancy means that each node can communicate with more than just one other node.
  - This communication can extend the range of the communication link.
    - In this case, an intermediate node acts as a relay between two other nodes.
    - Range extension typically comes at the price of slower communications (as intermediate nodes need to spend time relaying other nodes' messages).
  - An example of a technology that implements a mesh topology is Wi-Fi mesh.

The Core IoT Functional Stack Layer 2: Communications Network Layer

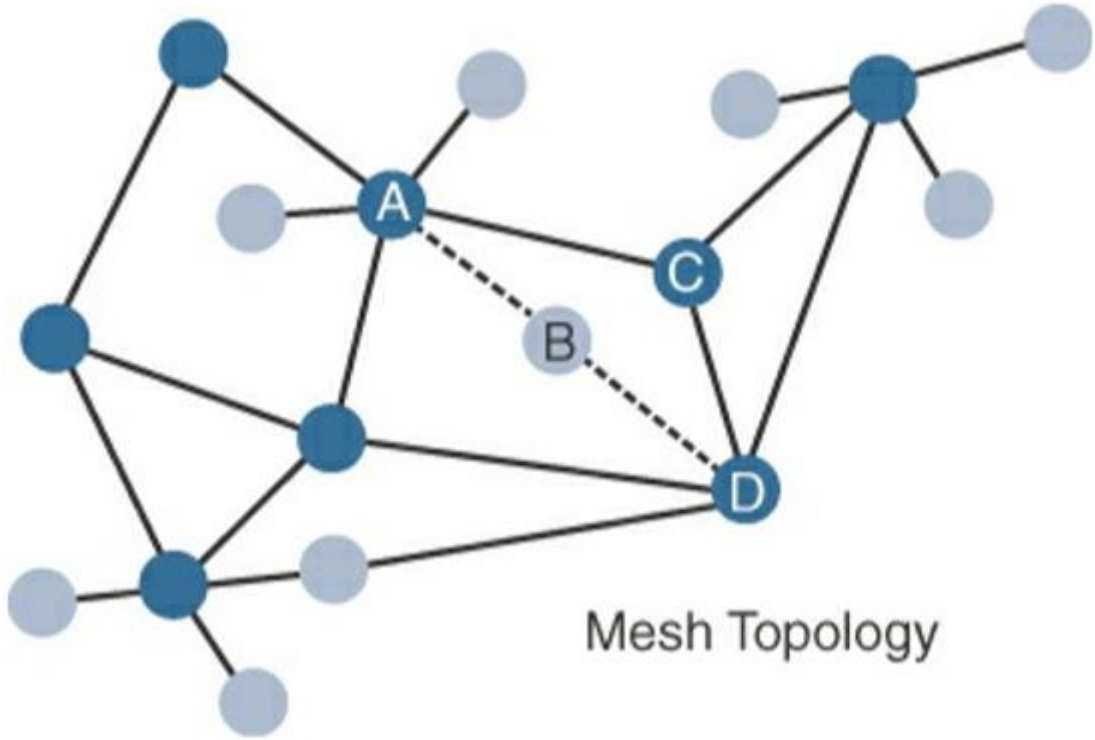


Figure 2-13 Mesh Topology

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **Gateways and Backhaul Sublayer**
  - Data collected from a smart object may need to be forwarded to a central station where data is processed.
  - 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.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- In most cases, the smart objects are static or mobile within a limited area.
- The gateway is often static.
- However, some IoT technologies do not apply this model.
  - For example, dedicated short-range communication (DSRC) allows vehicle-to-vehicle and vehicle-to-infrastructure communication.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **Dedicated short-range communication (DSRC)**
  - Smart object's position relative to the **gateway is static.**
  - The car includes sensors and one gateway.
  - Communication between the sensors and the gateway may involve wired or wireless technologies.
  - Sensors may also be integrated into the road infrastructure and connect over a wired or wireless technology to a gateway on the side of the road.
  - A wireless technology (DSRC operates in the upper 5 GHz range) is used for backhaul communication, peer-to-peer, or mesh communication between vehicles.
  - The range at which DSRC can communicate is limited.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- For IoT architectures, the choice of a backhaul technology depends on the communication distance and also on the amount of data that needs to be forwarded.
  - E.g.
    - Environment is stable (for example, factory or oil and gas field), Ethernet can be used as a backhaul
    - Unstable or changing environments (for example, open mines) where cables cannot safely be run, a wireless technology is used E.g. WiFi
- **Mesh is a common topology to allow communication flexibility in this type of dynamic environment.**

The Core IoT Functional Stack Layer 2: Communications Network Layer

- However, throughput decreases as node-to-node distance increases, and it also decreases as the number of hops increases.
  - In Wi-Fi mesh network, throughput halves for each additional hop.
  - Other technologies are needed to increase beyond the range .
    - E.g. WiMax (802.16d) or cellular technology.

The Core IoT Functional Stack Layer 2: Communications Network Layer

Technology	Type and Range	Architectural Characteristics
Ethernet	Wired, 100 m max	Requires a cable per sensor/sensor group; adapted to static sensor position in a stable environment; range is limited; link is very reliable
Wi-Fi (2.4 GHz, 5 GHz)	Wireless, 100 m (multipoint) to a few kilometers (P2P)	Can connect multiple clients (typically fewer than 200) to a single AP; range is limited; adapted to cases where client power is not an issue (continuous power or client battery recharged easily); large bandwidth available, but interference from other systems likely; AP needs a cable
802.11ah (HaloW, Wi-Fi in sub-1 GHz)	Wireless, 1.5 km (multipoint), 10 km (P2P)	Can connect a large number of clients (up to 6000 per AP); longer range than traditional Wi-Fi; power efficient; limited bandwidth; low adoption; and cost may be an issue
WiMAX (802.16)	Wireless, several kilometers (last mile), up to 50 km (backhaul)	Can connect a large number of clients; large bandwidth available in licensed spectrum (fee-based); reduced bandwidth in license-free spectrum (interferences from other systems likely); adoption varies on location
Cellular (for example, LTE)	Wireless, several kilometers	Can connect a large number of clients; large bandwidth available; licensed spectrum (interference-free; license-based)

Table 2-4 Architectural Considerations for WiMAX and Cellular Technologies

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **Network Transport Sublayer**
  - In a hierarchical communication architecture in which a series of smart objects report to a gateway that conveys the reported data over another medium and up to a central station.
  - However, practical implementations are often flexible, with multiple transversal communication paths.
    - For example, consider the case of IoT for the energy grid. Your house may have a meter that reports the energy consumption to a gateway over a wireless technology.
    - Other houses in your neighbourhood (NAN) make the same report, likely to one or several gateways.
    - If your power consumption becomes unusually high, the utility headend application server may need on-demand reporting from your meter at short intervals to follow the consumption trend.
    - From a standard vertical push model, the transport structure changes and becomes bidirectional (downstream pull model instead of upstream push).

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **Distribution automation (DA)**
  - Allows meter to communicate with neighbouring meters or other devices in the electrical distribution grid. With such communication, consumption load balancing may be optimized.
    - For example, if your air conditioning pulses fresh air at regular intervals.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Your smart meter may communicate with your house appliances to evaluate their type and energy demand.
- Once the system learns your consumption pattern,
- Smart meter may communicate with your house appliances to evaluate their type and energy demand.
  - system learns your consumption pattern
    - E.g. public car charging station

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Communication structure may include
  - 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.
- Communication structure must include, a network protocol with specific characteristics, Scalability, security, Standartd and open protocol, IP protocol .

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **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).
  - UDP is a much lighter and faster protocol than TCP.
    - However, it does not guarantee packet delivery.
  - Both TCP and UDP can be secured with TLS/SSL (TCP) or DTLS (UDP).

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **IoT Network Management Sublayer**
  - IP, TCP, and UDP bring connectivity to IoT networks.
  - Upper-layer protocols need to take care of data transmission between the smart objects and other systems.
  - Multiple protocols have been leveraged or created to solve IoT data communication problems.
  - Some networks rely on a
    - **push model**
      - that is, a sensor reports at a regular interval or based on a local trigger
    - **pull model**
      - that is, an application queries the sensor over the network
    - **Multiple hybrid approaches** are also possible.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Web-based protocols
  - HTTP
  - WebSocket
  - Extensible Messaging and Presence Protocol (XMPP)

The Core IoT Functional Stack Layer 2: Communications Network Layer

- Some IoT implementers have suggested **HTTP** for the data transfer phase.
  - 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),
    - but HTTP is something of a fat protocol and was not designed to operate in constrained environments with low memory, low power, low bandwidth, and a high rate of packet failure.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **WebSocket** (Small compared to HTTP)
  - is part of the HTML5 specification, and provides a simple bidirectional connection over a single connection.
  - WebSocket to manage the connection between the smart object and an external application.
  - WebSocket is often combined with other protocols, such as MQTT (Message Queue Telemetry Transport).

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **Extensible Messaging and Presence Protocol (XMPP)**
  - 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,
    - which may force subscribers to maintain open sessions to other systems and may be a limitation for memory-constrained objects.

The Core IoT Functional Stack Layer 2: Communications Network Layer

- IoT protocol
  - IETF Constrained Restful Environments (CoRE)
  - Constrained Application Protocol (CoAP).
  - MQTT

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **IETF Constrained Restful Environments (CoRE)**
- Working group: **Constrained Application Protocol (CoAP).**
  - CoAP uses some methods similar to those of HTTP (such as Get, Post, Put, and Delete) but implements a shorter list, thus limiting the size of the header.
  - CoAP also runs on UDP (whereas HTTP typically uses TCP).
  - CoAP observation: Observation allows the streaming of state changes as they occur,

The Core IoT Functional Stack Layer 2: Communications Network Layer

- **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**,
  - 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 holds a connection open to the broker at all times.
  - This may be a limiting factor in environments where loss is high or where computing resources are limited.

The Core IoT Functional Stack Layer 3: Applications and Analytics Layer

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

The Core IoT Functional Stack Layer 3: Applications and Analytics Layer

- **Analytics Versus Control Applications**
  - Each application collects data and provides a range of functions based on analysing the collected data.
- **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.
- **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.

The Core IoT Functional Stack Layer 3: Applications and Analytics Layer

- **Data Versus Network Analytics**
- **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.
  - E.g.
    - Simple case dashboard can display an alarm when a weight sensor detects that a shelf is empty in a store.
    - Complex case, temperature, pressure, wind, humidity, and light levels collected from thousands of sensors
    - Data analytics can also monitor the IoT system itself.
      - For example, a machine or robot in a factory can report data about its own movements.

The Core IoT Functional Stack Layer 3: Applications and Analytics Layer

- **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.
  - 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.

The Core IoT Functional Stack Layer 3: Applications and Analytics Layer

- **Data Analytics Versus Business Benefits**
  - Collecting and interpreting the data generated by these devices is where the value of IoT is realized.
  - Static IoT networks : Cant be update or add/remove sensors
  - Connect to new sensors.
    - This enhanced data processing and can add value for businesses.
  - E.g. Vending machines deployed throughout a city
    - Sensors can be deployed to report when a machine is in an error state.
    - A repair person can be sent to address.
    - This type of alert is a time saver

The Core IoT Functional Stack Layer 3: Applications and Analytics Layer

- **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.
- Smart services can be integrated into an IoT system.
  - For example, sensors can be integrated in a light bulb.
- Similar efficiency can be extended to larger systems than a house.
  - For example, smart grid

IoT Data Management and Compute Stack

- The data generated by IoT sensors is one of the single biggest challenges in building an IoT system.
  - In IT networks, the data sourced by a computer or server is typically generated by the client/server communications model, and it serves the needs of the application.
- In sensor networks, the vast majority of data generated is unstructured and of very little use on its own.
  - For example, the majority of data generated by a smart meter is nothing more than polling data

IoT Data Management and Compute Stack

- In most cases, the processing location is outside the smart object.
- A natural location for this processing activity is the cloud.
- Smart objects need to connect to the cloud, and data processing is centralized.

IoT Data Management and Compute Stack

- As data volume, the variety of objects connecting to the network, and the need for more efficiency increase, new requirements appear as follows:
  - **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. Analyzing data close to the device that collected the data can make a difference between averting disaster and a cascading system failure.

IoT Data Management and Compute Stack

- **Conserving network bandwidth:** Offshore oil rigs generate 500 GB of data weekly.
  - Commercial jets generate 10TB 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.

IoT Data Management and Compute Stack

- **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.
  - Analyzing both areas in the same cloud system may not be necessary for immediate efficiency.

- Design an IoT network to manage this volume of data in an efficient way such that the data can be quickly (Real time) analyzed and lead to business benefits.

IoT Data Management and Compute Stack

- The volume of data also introduces questions about bandwidth management.
  - funnel into the data center or server ?
  - capacity to sustain this volume of traffic ?
  - server have the ability to ingest, store, and analyze the vast quantity of data ?
- **“impedance mismatch”** of the data generated by the IoT system and the management application’s

IoT Data Management and Compute Stack

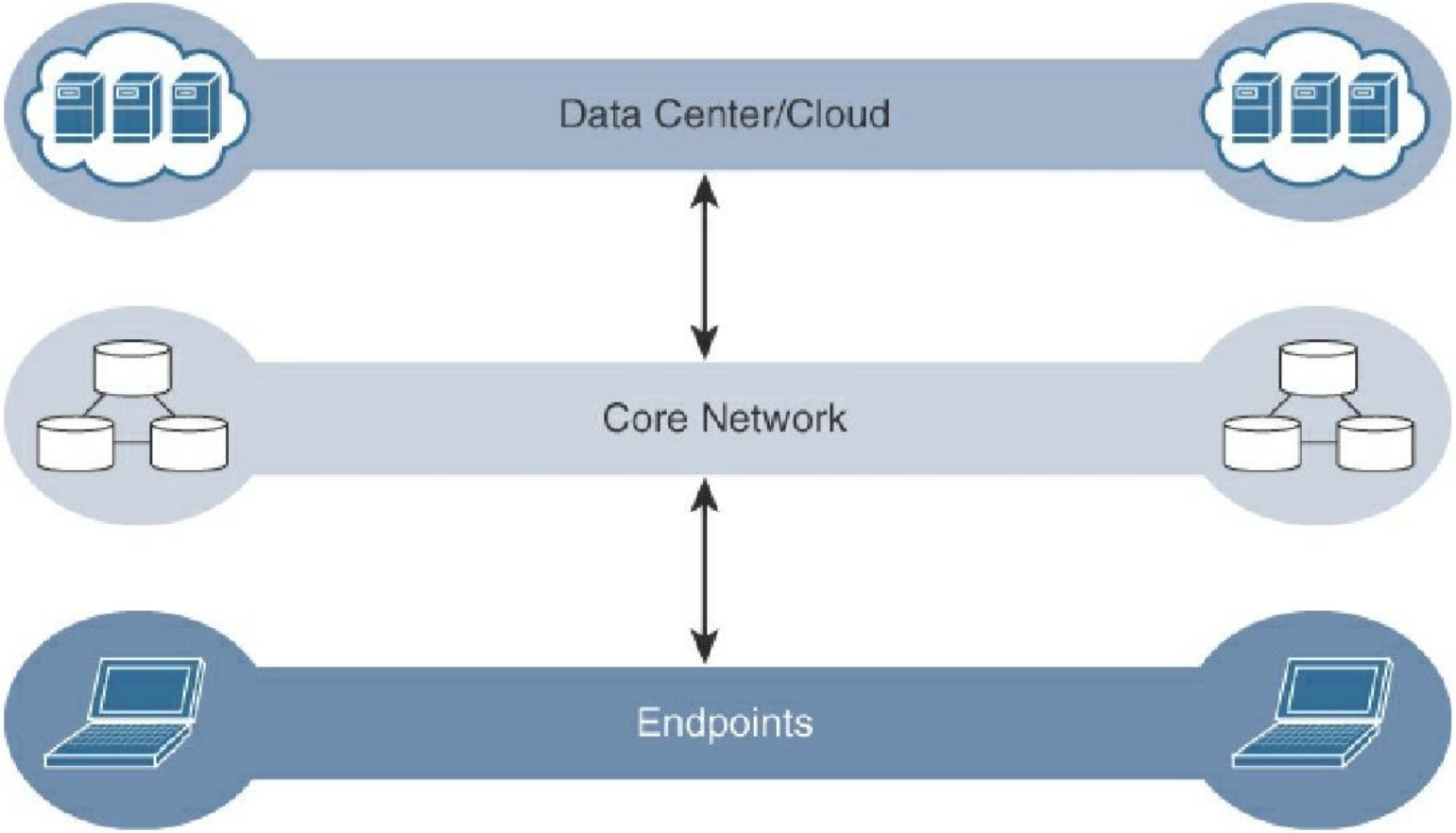


Figure 2-14 The Traditional IT Cloud Computing Model

IoT Data Management and Compute Stack

- 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 of tens 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.
  - 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.

IoT Data Management and Compute Stack: Fog Computing

- 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.**
- Just as clouds exist in the sky, fog rests near the ground. In the same way, the intention of fog computing is to place resources as close to the ground that is, the IoT devices as possible.
- Any device with computing, storage, and network connectivity can be **a fog node.**
  - Examples include industrial controllers, switches, routers, embedded servers, and IoT gateways.
- Analyzing IoT data close to where it is collected minimizes latency, offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the local network.

IoT Data Management and Compute Stack: Fog Computing

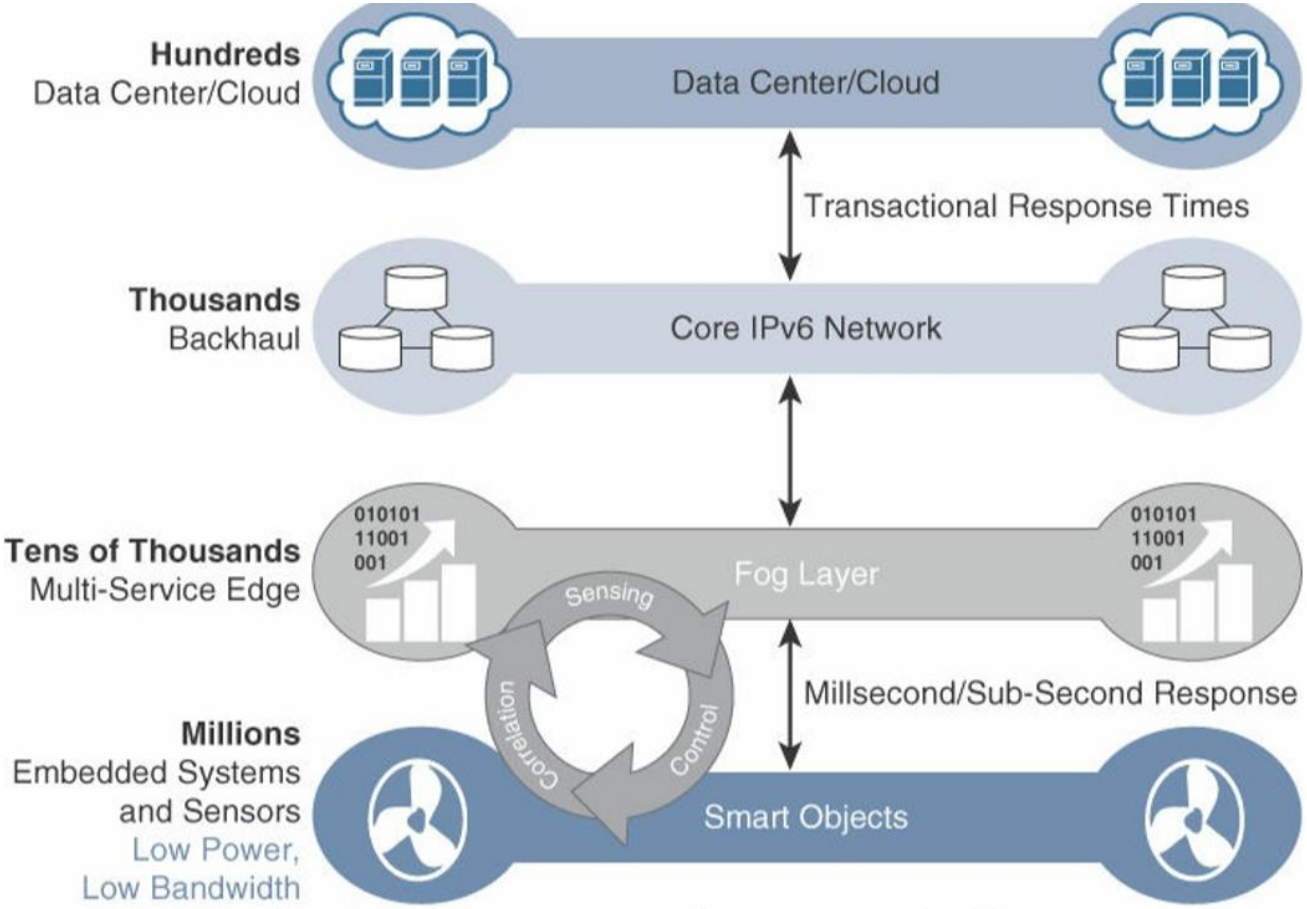


Figure 2-15 The IoT Data Management and Compute Stack with Fog Computing

IoT Data Management and Compute Stack: Fog Computing

- 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.
  - monitoring all the sensor activity
  - analyze information from all the sensors
  - to send back only the relevant information over the backhaul network to the cloud
  - volume of data sent upstream is greatly reduced

IoT Data Management and Compute Stack: Fog Computing

- 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.

IoT Data Management and Compute Stack: Fog Computing

- For example,
  - tire pressure sensors on a large truck in an open-pit mine might continually report measurements all day long.
    - There may be only minor pressure changes that are well within tolerance limits, making continual reporting to the cloud unnecessary.
    - Is it really useful to continually send such data back to the cloud over a potentially expensive backhaul connection?
  - With a fog node on the truck, it is possible to not only measure the pressure of all tires at once but also combine this data with information coming from other sensors in the engine, hydraulics, and so on.
  - With this approach, the fog node sends alert data upstream only if an actual problem is beginning to occur on the truck that affects operational efficiency.

IoT Data Management and Compute Stack: Fog Computing

- IoT fog computing enables data to be preprocessed and correlated with other inputs to produce relevant information.
- This data can then be used as real-time, actionable knowledge by IoT-enabled applications.
- Longer term, this data can understanding of network behavior and systems for the purpose of developing proactive policies, processes, and responses.
- Fog applications and the Internet of Things have in common is data reduction monitoring or analyzing real-time data from network connected things and then initiating an action

IoT Data Management and Compute Stack: Fog Computing

- 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.

IoT Data Management and Compute Stack: Edge Computing

- Edge computing is also sometimes called "mist" computing.
  - **clouds** exist in the sky, and
  - **fog** sits near the ground, then
  - **mist** is what actually sits on the ground.
- Thus, the concept of mist is to extend fog to the furthest point possible, right into the IoT endpoint device itself.

IoT Data Management and Compute Stack: Edge Computing

- 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. While a fog node sitting on an electrical pole in the distribution network may have an excellent view of all the fire hydrants in a local neighborhood,
  - 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,

IoT Data Management and Compute Stack:
The Hierarchy of Edge, Fog, and Cloud

- Edge or fog computing in no way replaces the cloud.
- Rather, they complement each other, and many use cases actually require strong cooperation between layers.
- Edge and fog computing layers simply act as a filtering, analyzing, and otherwise managing data endpoints.
- **This saves the cloud from being queried by each and every node for each event.**

IoT Data Management and Compute Stack:
The Hierarchy of Edge, Fog, and Cloud

- At each stage, data is collected, analyzed, and responded to when necessary.
- As data 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.

IoT Data Management and Compute Stack:
The Hierarchy of Edge, Fog, and Cloud

- It is important to note that the heterogeneity of IoT devices also means a heterogeneity of edge and fog computing resources.
  - Different operating systems, have different CPU and data storage capabilities, and have different energy consumption profiles
- While cloud resources are expected to be homogenous
- Common communications services framework between Edge, Fog and Cloud

IoT Data Management and Compute Stack: The Hierarchy of Edge, Fog, and Cloud

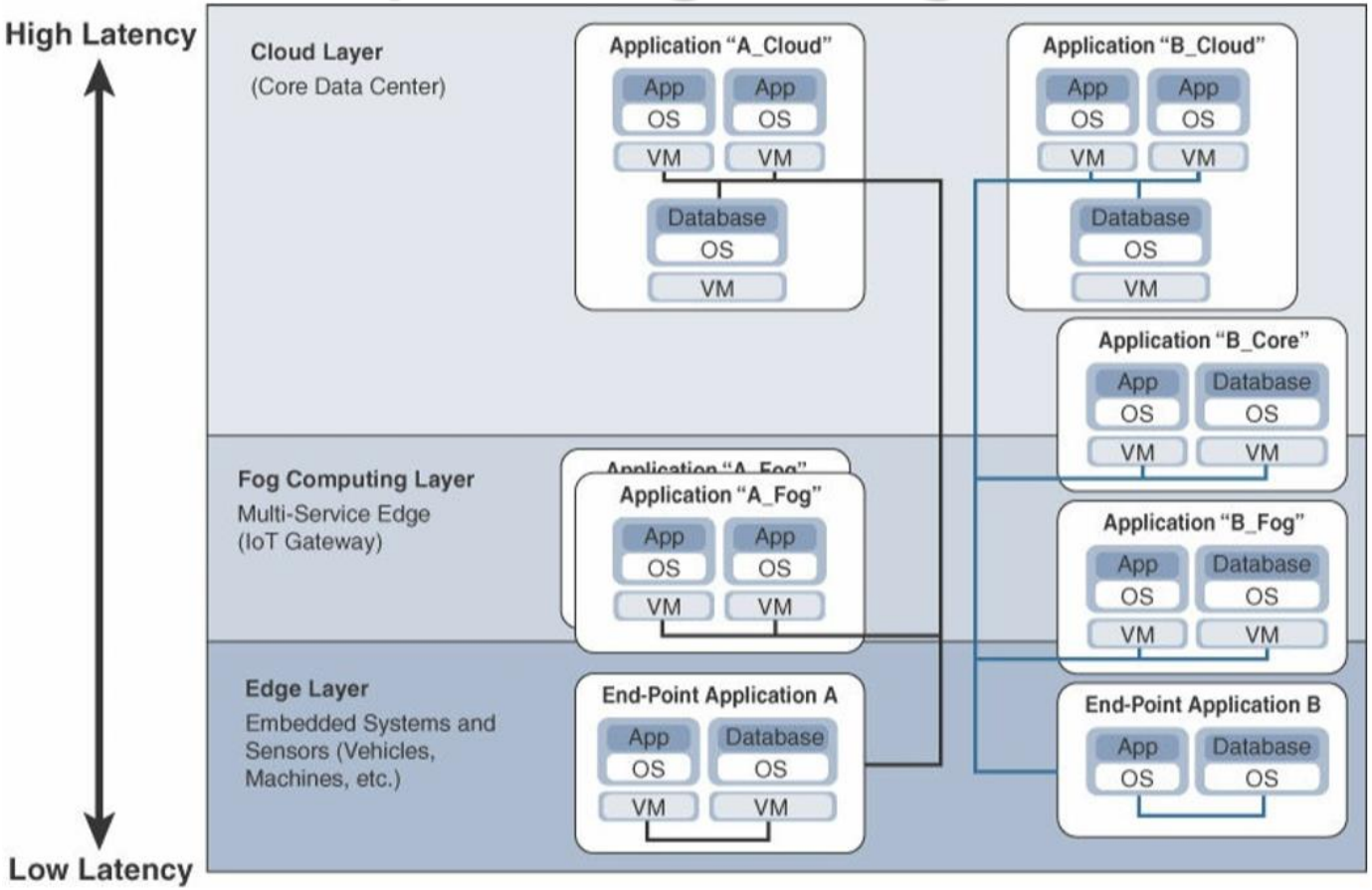


Figure 2-16 Distributed Compute and Data Management Across an IoT System

IoT Data Management and Compute Stack:
The Hierarchy of Edge, Fog, and Cloud

- 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.

IoT Data Management and Compute Stack:
The Hierarchy of Edge, Fog, and Cloud

- Based on amount of data you can decide whether cloud computing is enough or whether edge or fog computing would improve your system efficiency.
- It avoids the need for costly bandwidth additions by offloading gigabytes of network traffic from the core network.

FUTURE VISION BIE

By K B Hemanth Raj

Visit : https://hemanthrajhemu.github.io

Quick Links for Faster Access.

CSE 8th Semester - https://hemanthrajhemu.github.io/CSE8/

ISE 8th Semester - https://hemanthrajhemu.github.io/ISE8/

ECE 8th Semester - https://hemanthrajhemu.github.io/ECE8/

8th Semester CSE - TEXTBOOK - NOTES - QP - SCANNER & MORE

17CS81 IOT - https://hemanthrajhemu.github.io/CSE8/17SCHEME/17CS81/

17CS82 BDA - https://hemanthrajhemu.github.io/CSE8/17SCHEME/17CS82/

17CS832 UID - https://hemanthrajhemu.github.io/CSE8/17SCHEME/17CS832/

17CS834 SMS - https://hemanthrajhemu.github.io/CSE8/17SCHEME/17CS834/

8th Semester Computer Science & Engineering (CSE)

8th Semester CSE Text Books: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Text-Book.html

8th Semester CSE Notes: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Notes.html

8th Semester CSE Question Paper: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Question-Paper.html

8th Semester CSE Scanner: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Scanner.html

8th Semester CSE Question Bank: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Question-Bank.html

8th Semester CSE Answer Script: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Answer-Script.html

Contribution Link:

https://hemanthrajhemu.github.io/Contribution/

Stay Connected... get Updated... ask your queries...

Join Telegram to get Instant Updates:
https://telegram.me/joinchat/AAAAAFTtp8kuvCHALxuMaQ

Contact: MAIL: futurevisionbie@gmail.com

INSTAGRAM: www.instagram.com/futurevisionbie/