CS6014 – Internet of Things and Smart Appliances

MODULE I
IoT fundamentals

Evolution of Internet of Things - Enabling Technologies – IoT Architectures: oneM2M, IoT World Forum (IoTWF) and Alternative IoT models – Simplified IoT Architecture and Core IoT Functional Stack -– Fog,Edge and Cloud in IoT

History of IoT

Evolution of IoT

- 1970 – Idea on connecting things were proposed
- 1990 – John Romkey created a toaster which could be turned on/off over Internet
- 1995 – Siemens introduced first cellular module built for M2M
- 1999 – “Internet of Things” term was proposed by **Kevin Ashton**
- 2005 – UN Telecommunication Union used term in publications
- 2008 – Internet of Things was born
- 2011 – Gartner, market research company included IoT in their research report

Internet of Things

- Basic Goal – “Connect the Unconnected”
- IoT - sense and control the physical world by making objects smarter and connecting them through an intelligent network.
- Objects and machines - sensed and controlled remotely across a network, a tighter integration between physical world and computers is enabled.
- Improvements in areas of efficiency, accuracy, automation and enablement of advanced applications.
- Umbrella of different concepts – Protocols, Technology, Concepts.

Evolutionary Phases of Internet

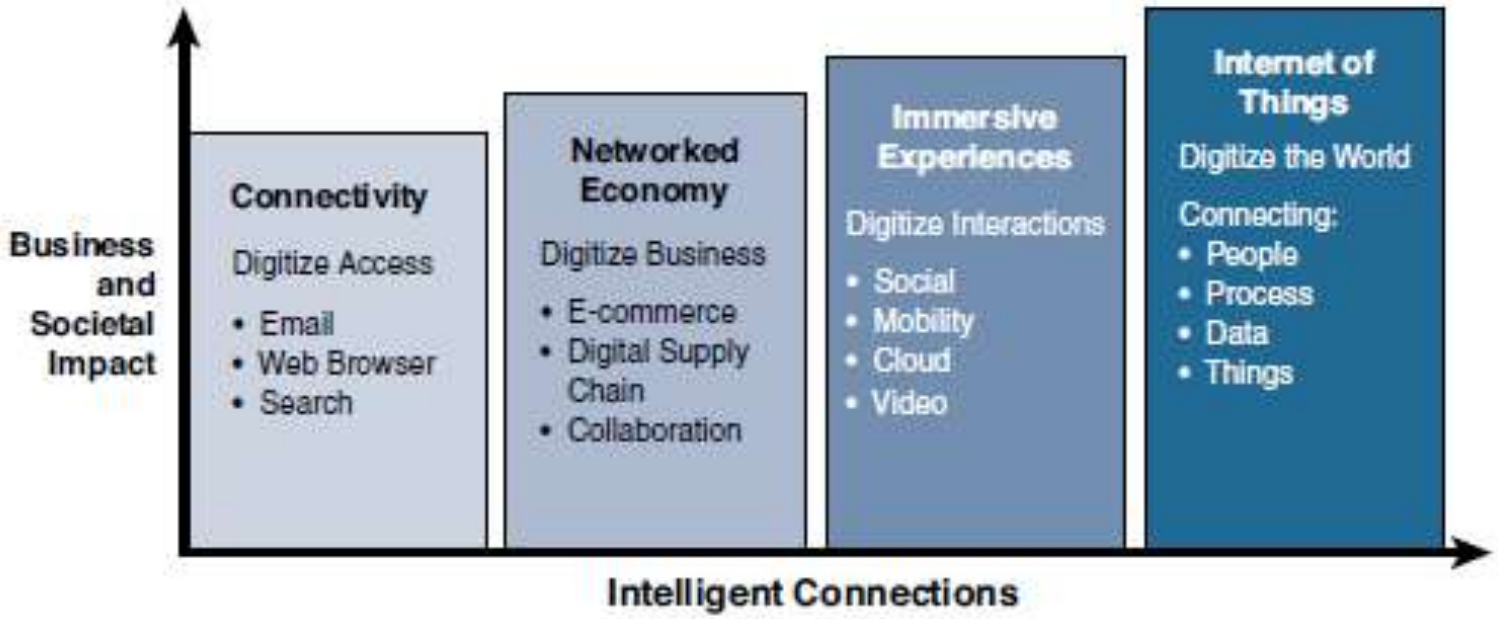


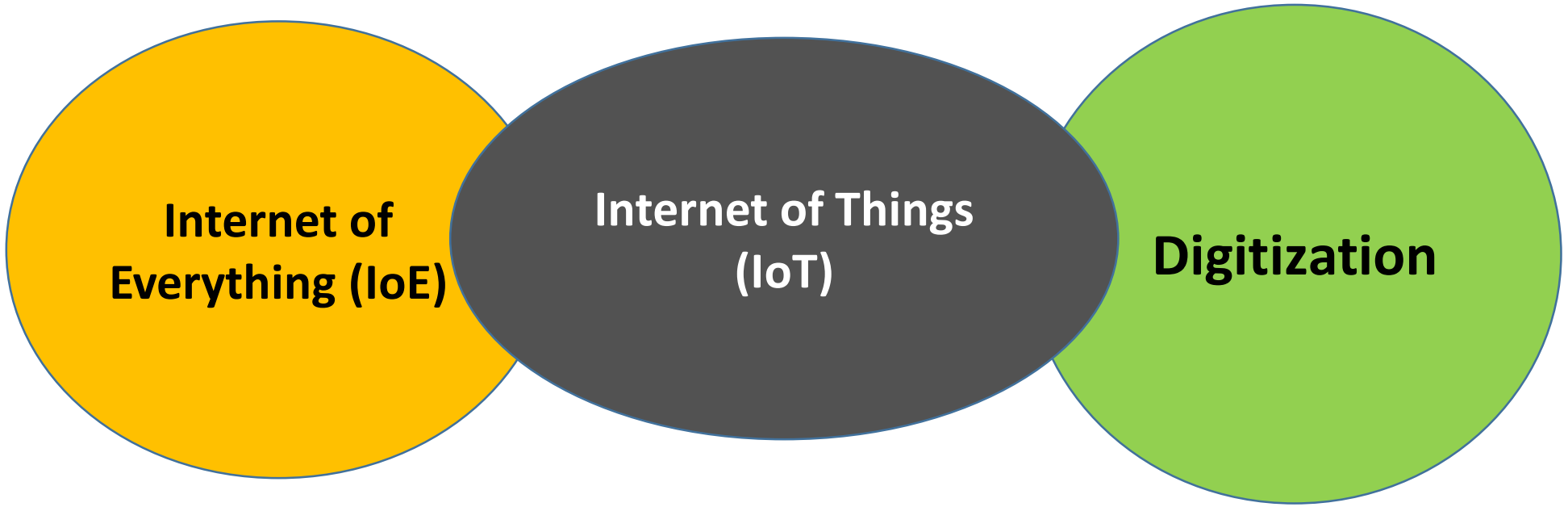
Figure 1-1 *Evolutionary Phases of the Internet*

Evolutionary Phases of Internet

Table 1-1 *Evolutionary Phases of the Internet*

Internet Phase	Definition
Connectivity (Digitize access)	This phase connected people to email, web services, and search so that information is easily accessed.
Networked Economy (Digitize business)	This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.
Immersive Experiences (Digitize interactions)	This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud.
Internet of Things (Digitize the world)	This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences. It is connecting the unconnected.

IoT and Digitization



What are the areas you can see digitization?

- Photography Industry
- Video Rental Industry
- Transportation (Uber and Lyft)
- Company's perspective - digitization - differentiator for businesses

IoT – Prime enabler of digitization

IoT Impact

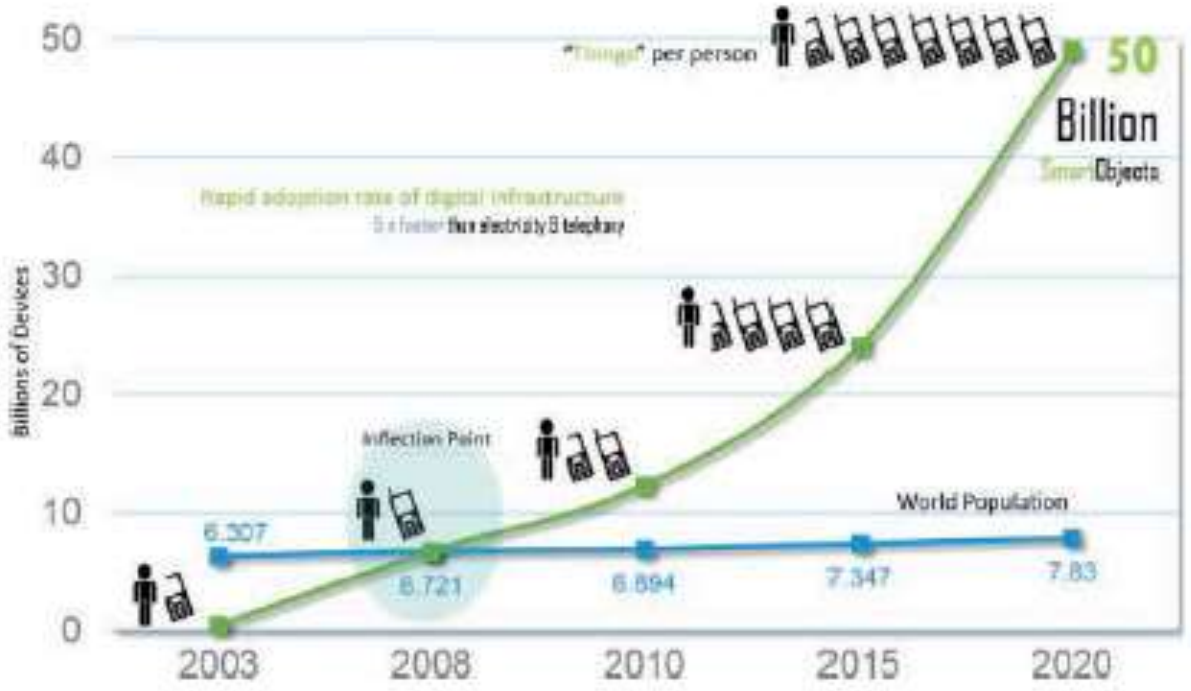


Figure 1-2 *The Rapid Growth in the Number of Devices Connected to the Internet*

Connected Roadways

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

Current Challenges

Table 1-2 *Current Challenges Being Addressed by 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.

Figure 1-4 *Application of Intersection Movement Assist*

Connected Car

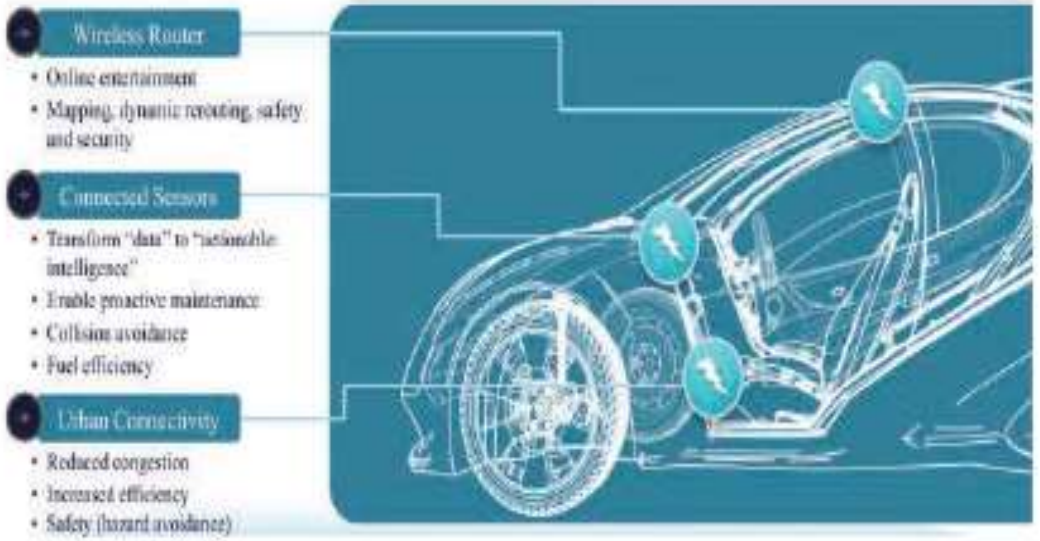


Figure 1-5 *The Connected Car*

- How the data can be handled?
- To whom the data can be useful?
- **IoT data broker**

Connected Factory = Factory-based Operational Technologies + Global IT networks

- Traditional factories are “flying blind” and lack visibility into their operations.
- What will be the main challenges faced by manufacturing in a factory environment?
  - Accelerating new product and service introduction to meet customer and market opportunities.
  - Increasing plant production, quality and uptime
  - Mitigating unplanned downtime
  - Securing factories from cyber threats
  - Decreasing high cabling and re-cabling costs
  - Improving worker productivity and safety

Four Industrial Revolutions

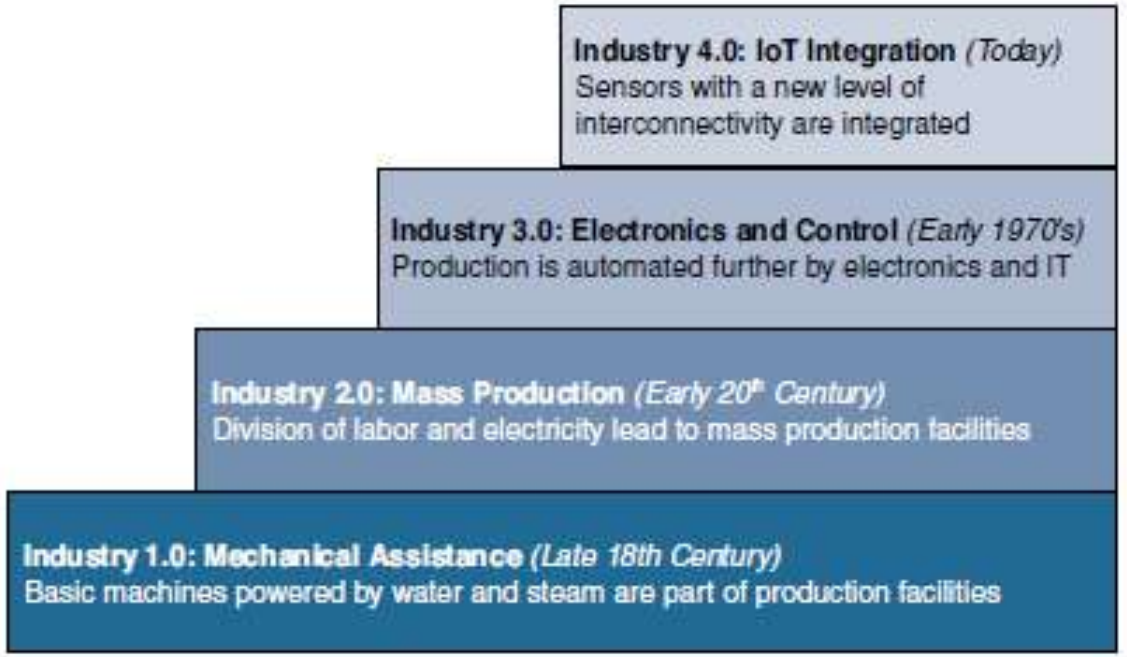


Figure 1-6 *The Four Industrial Revolutions*

Smart Connected Buildings

- Intersections of structural, mechanical, electrical, and IT components.
- HVAC (heating, ventilation, and air conditioning)
- Building Management System (BMS)
- Heterogeneity of IoT systems
- BACNet, BACNet/IP

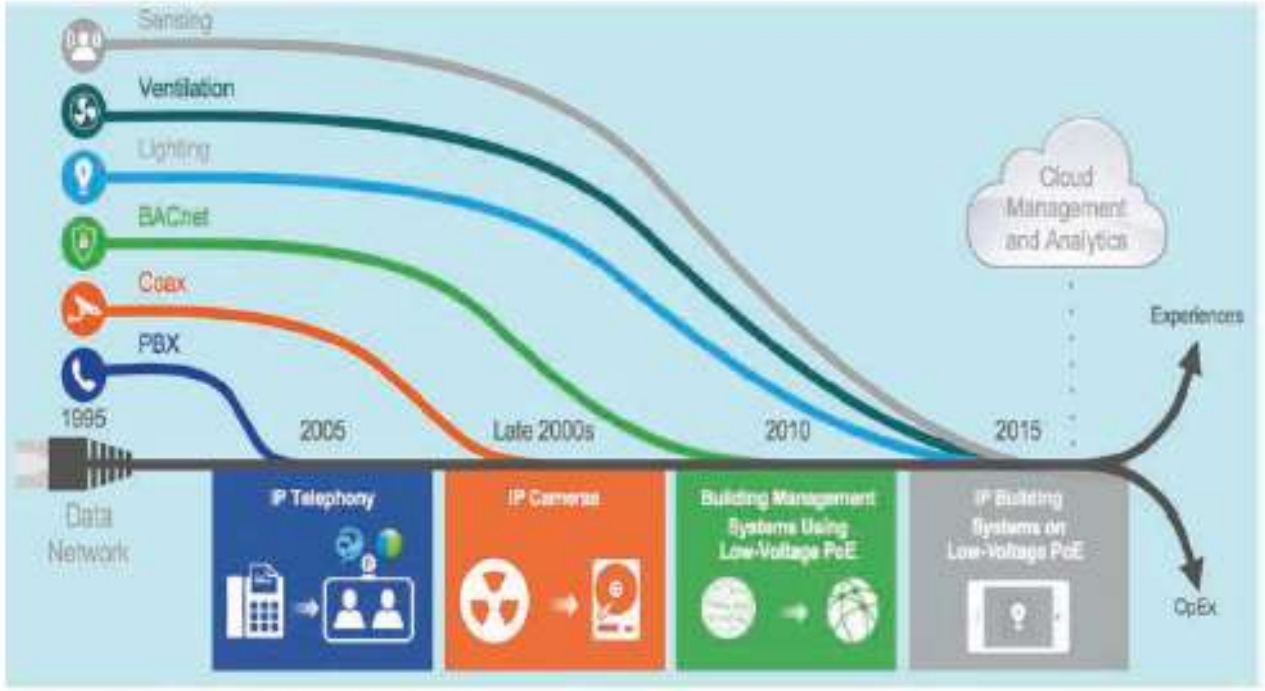


Figure 1-7 *Convergence of Building Technologies to IP*

Framework for Digital Ceiling

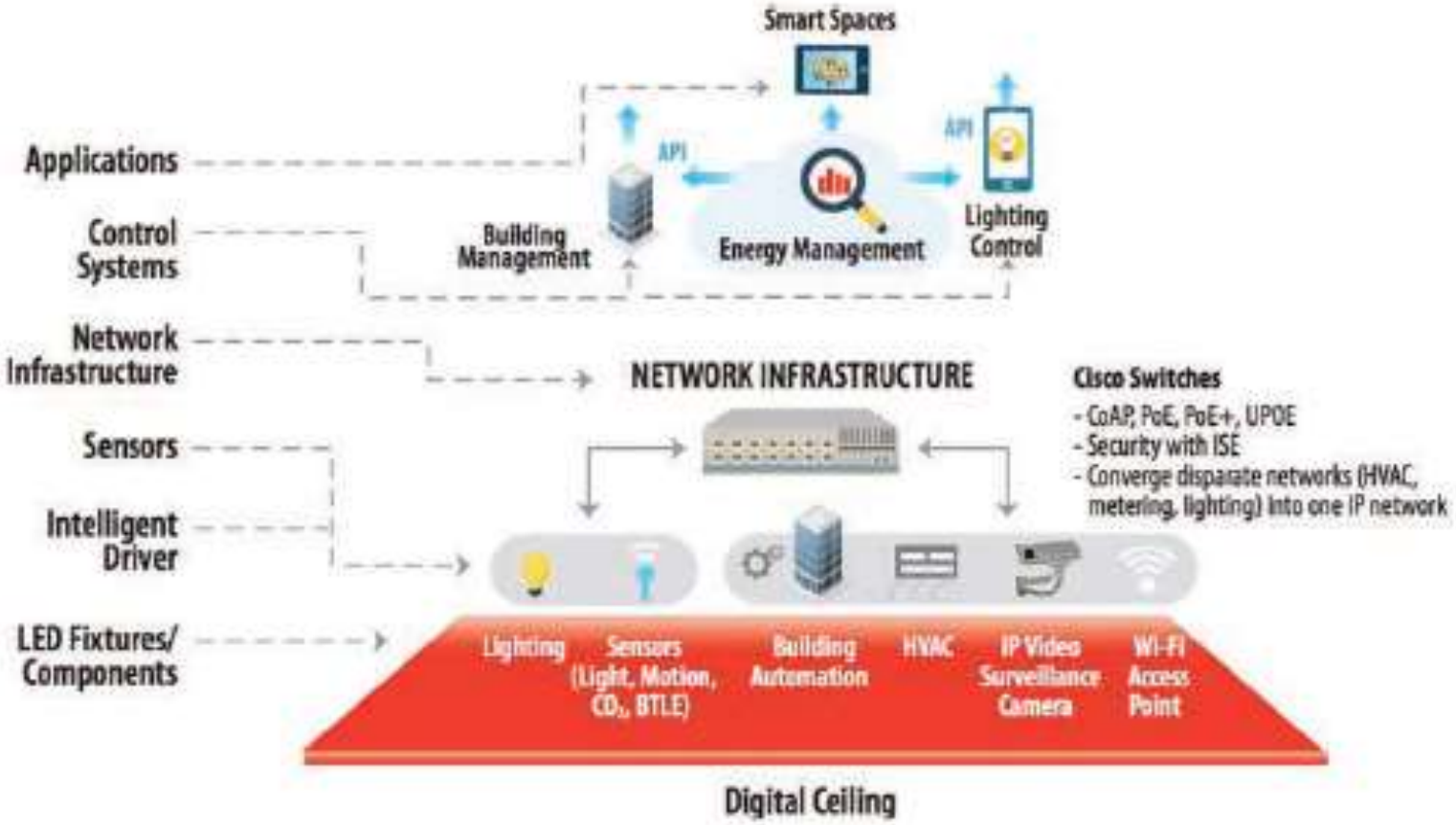


Figure 1-8 *A Framework for the Digital Ceiling*

Figure 1-9 *An LED Digital Ceiling Light with Occupancy Sensor*
(Photo by Bill MacGowan)

SMART CREATURE

- Well-known applications of IoT with respect to animals focuses on what is often referred to as the “connected cow.”
- Another application of IoT to organisms involves the placement of sensors on roaches.
- This backpack communicates with the roach through parts of its body.
- Low-level electrical pulses to an antenna on one side makes the roach turn to the opposite side because it believes it is encountering an obstacle.
- The cerci(**one of a pair of sensory appendages at the tip of the abdomen of some insects**)of the roach are sensory organs on the abdomen that detect danger through changing air currents. When the backpack stimulates the cerci, the roach moves forward because it thinks a predator is approaching.
- These examples show that IoT often goes beyond just adding sensors and more intelligence to nonliving “things.”
- Living “things” can also be connected to the Internet and this connection can provide important results.

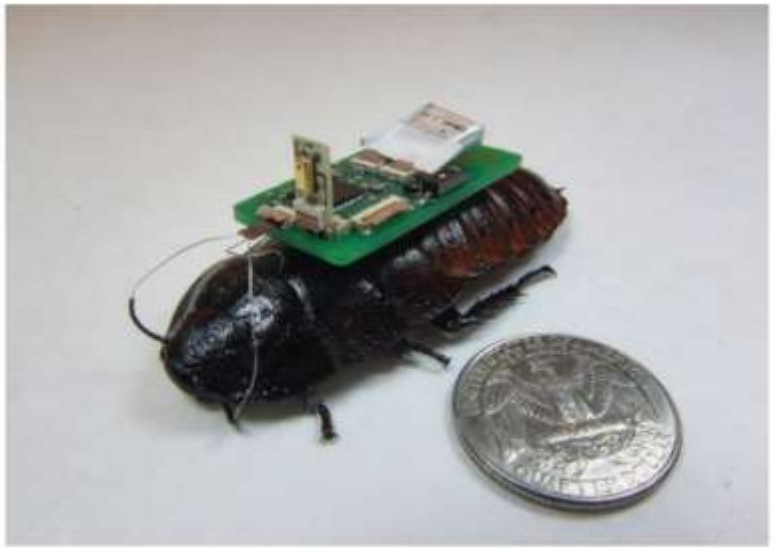


Figure 1-10 *IoT-Enabled Roach Can Assist in Finding Survivors After a Disaster (Photo courtesy of Alper Bozkurt, NC State University)*

Convergence of IT and OT

Table 1-3 *Comparing Operational Technology (OT) and Information Technology (IT)*

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 protection

IoT Challenges

- Scale (IT and OT Network) “IP as the IoT Network Layer” with IPv6
- Security (“things” becoming connected with other “things”)
  ie., Securing IOT
- Privacy (Specific to individuals)
- Big Data and Data Analytics (Large no of sensors triggered and datas should be maintained)
- Interoperability

IoT Enabling Technologies

Wireless Sensor Networks (WSN)

- Distributed devices with sensors which can monitor environmental and physical conditions
- End-nodes, Routers, Co-ordinators
- End-nodes as routers, Co-ordinators as gateways
- Eg: Weather monitoring, Air quality monitoring
- Communication protocol – Zig Bee (250KB/s,2.4GHz frequency)
- Self-organizing in nature

Cloud Computing

- Provisioning of networking, storage and computing resources as metered service
- Pay-as-you-go
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Big Data Analytics

- Volume, Velocity, Variety

- Eg: Weather monitoring stations
  Fitness Bands
  Vehicle-Tracking data
  Inventory monitoring

Communication Protocols

- Backbone of IoT applications
- Enable network connectivity and coupling to applications
- Link, Network, Transport and Application Layer protocols
- Data exchange formats, data encoding and addressing schemes, routing of packets
- Sequence control, flow control and retransmission of lost packets

Embedded Systems

- Consists of computer hardware and software embedded to perform specific tasks

- Key components:

  - Microprocessor or microcontroller

  - Networking units
  - Input/output units
  - Storage
  - Digital Signal Processors (DSP)
  - Graphic Processors
  - Application Specific Processors
  - Embedded Operating System – RTOS(A **Real Time Operating System** is a software component that rapidly switches between tasks, giving the impression that multiple programs are being executed at the same time on a single processing core.)

ASSIGNMENT 1

1. Find out some of the open source IoT Platforms
2. List out the real-world IoT applications

DRIVERS BEHIND NEW NETWORK ARCHITECTURES

S.NO	CRITERIA	IT	IoT
1.	Framework	Simple	Complex
2.	Focus	Business	Data
3.	Processing of Data	Batch-Level Processing	Real-Time Processing

IoT Architectural Drivers

- Scale – Address Spacing
- Security – Zero-touch deployment model
- Device and Constrained Networks – Last-mile wireless technology
- Volume of Data - Data Analytics
- Support for Legacy Devices – Tunneling mechanism
- Need for data to be analyzed in real time – Real-Time streaming analytics

Comparing IoT Architectures

•The foundational concept in all these architectures is supporting data, process, and the functions that endpoint devices perform.

• Two of the best-known architectures are those supported by,

oneM2M and

the IoT World Forum (IoTWF)

i.) The oneM2M IoT Standardized Architecture

- One machine-to-machine (M2M) communications
- European Telecommunications Standards Institute (ETSI)
- ETSI created the M2M Technical Committee in 2008.
- Goal- to create a common architecture that would help accelerate the adoption of M2M applications and devices.
- Greatest Challenge – LoRaWAN, BACNet
- IEEE 802.15.4

Figure 2-1 illustrates the oneM2M IoT architecture.

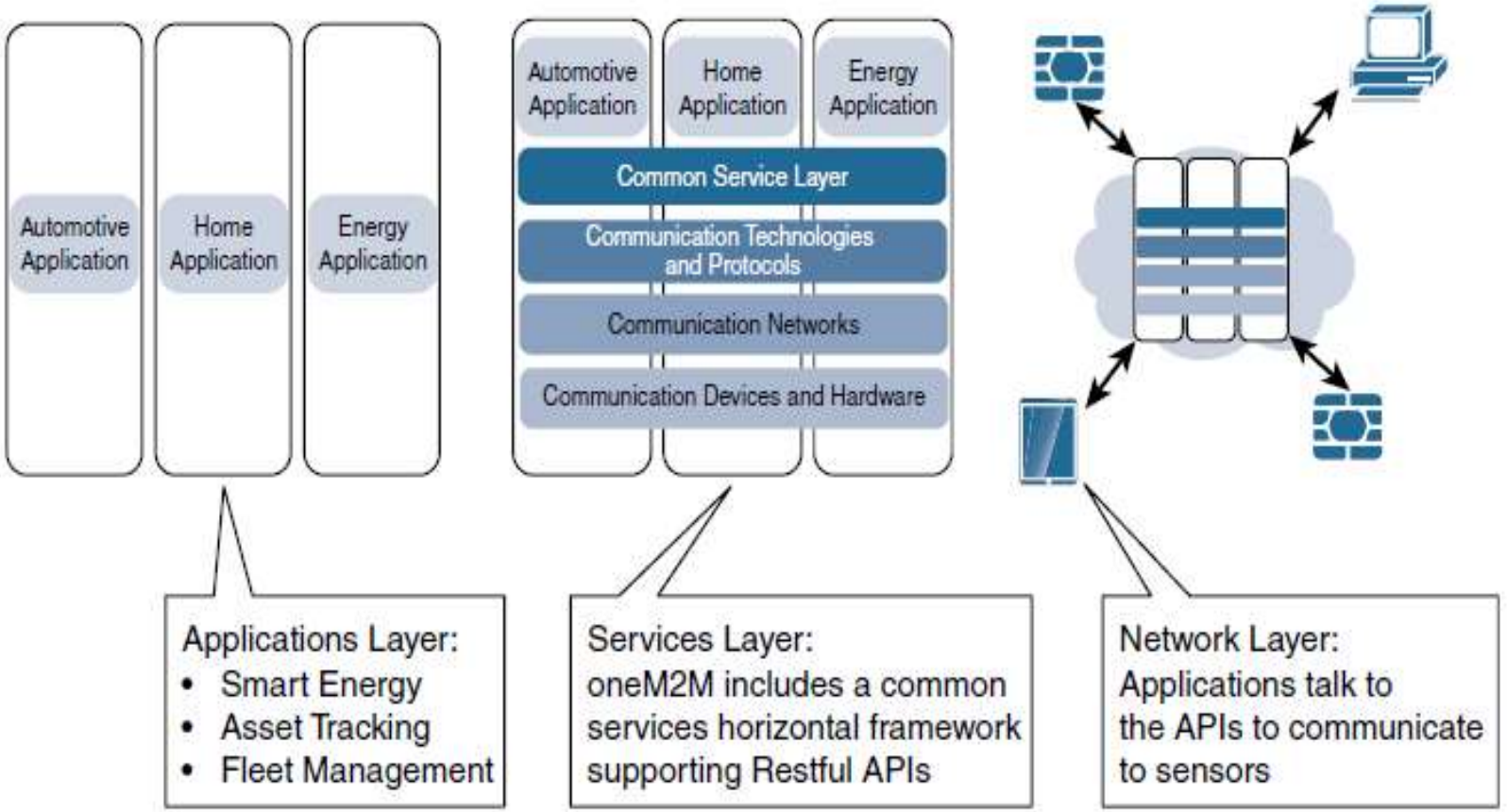
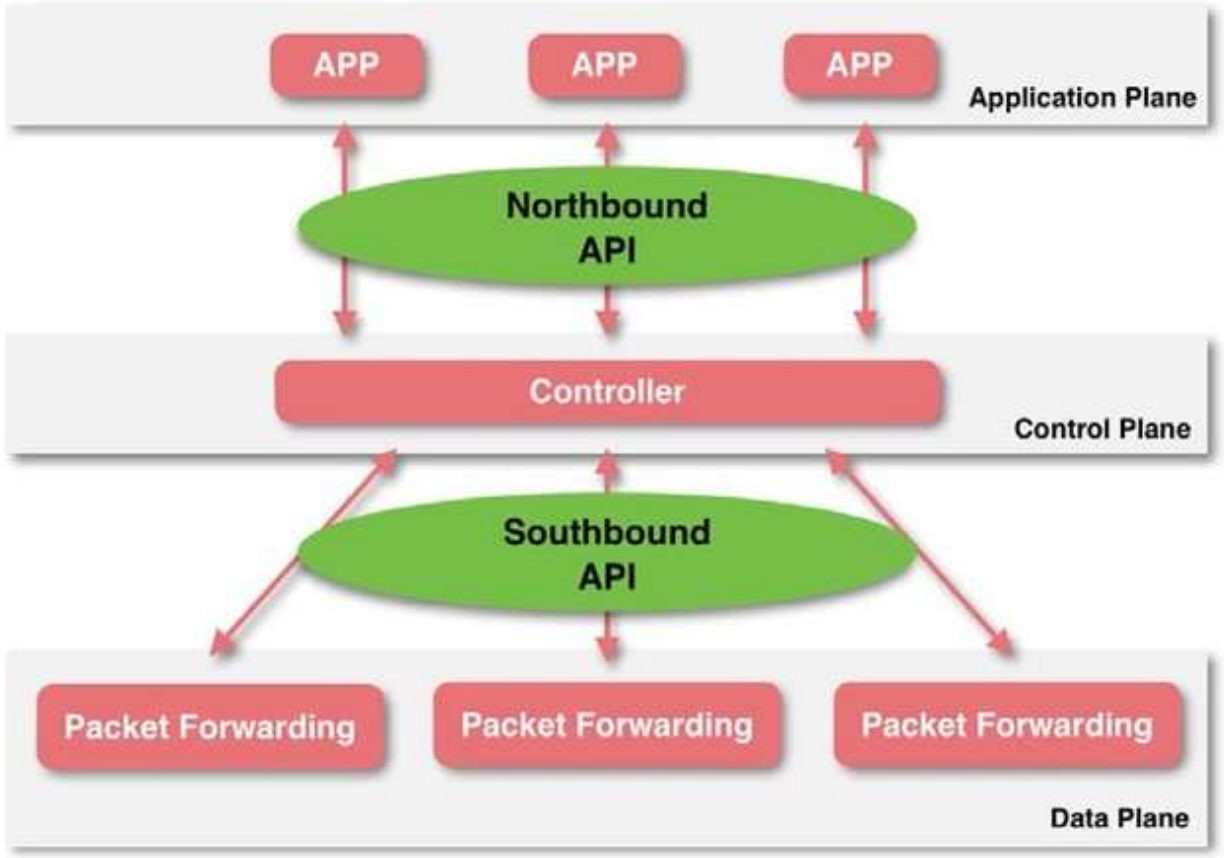


Figure 2-1 *The Main Elements of the oneM2M IoT Architecture*

ii.) IoT World Forum (IoTWF) Standardized Architecture



Levels

7 **Collaboration & Processes**
(Involving People & Business Processes)

6 **Application**
(Reporting, Analytics, Control)

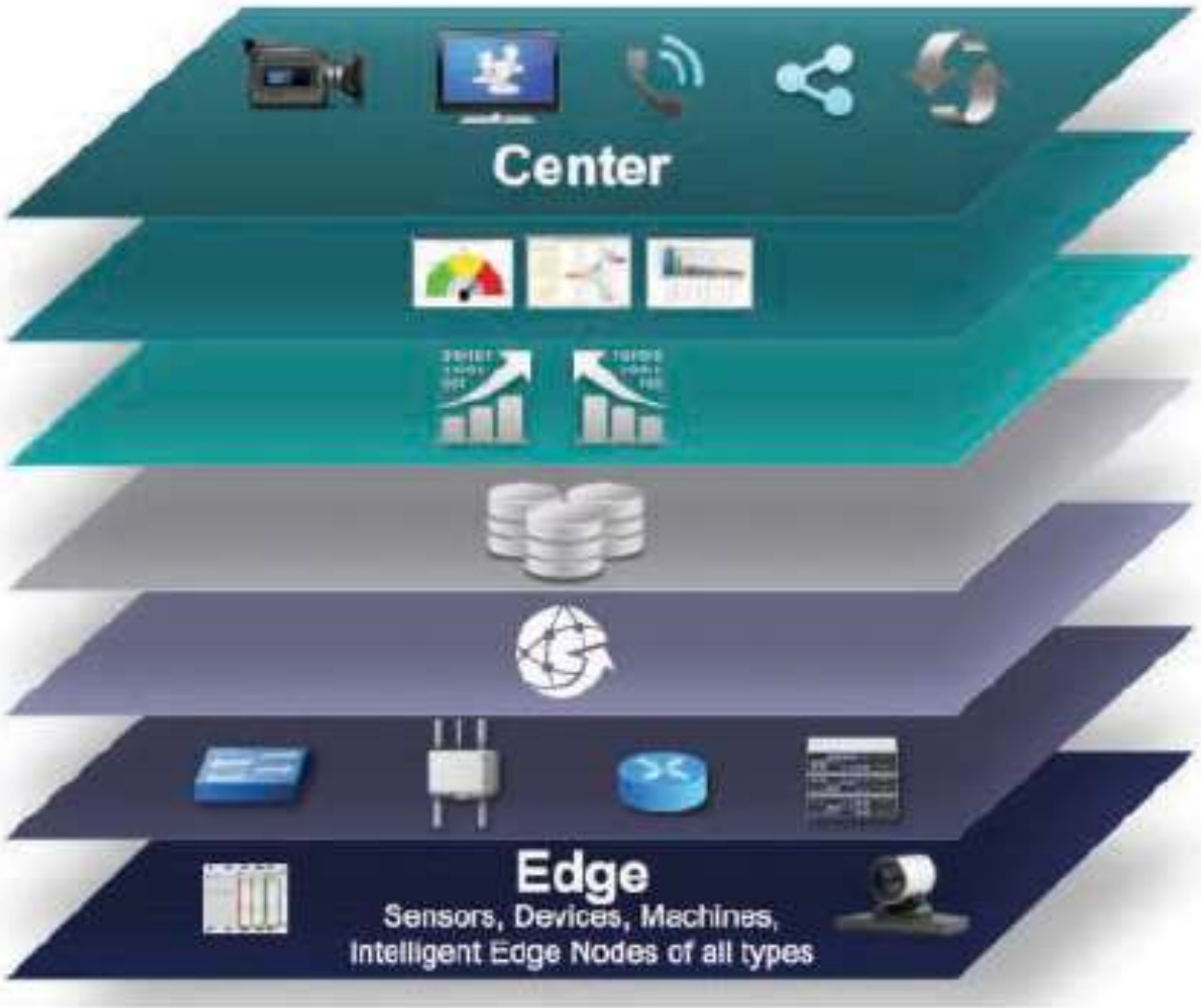
5 **Data Abstraction**
(Aggregation & Access)

4 **Data Accumulation**
(Storage)

3 **Edge Computing**
(Data Element Analysis & Transformation)

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

1 **Physical Devices & Controllers**
(The "Things" in IoT)



We are able to achieve the IoTWF by following,

- Decompose the IoT problem into smaller parts
- Identify different technologies at each layer and how they relate to one another
- Define a system in which different parts can be provided by different vendors
- Have a process of defining interfaces that leads to interoperability
- Define a tiered security model that is enforced at the transition points between levels

Layer 2 and 3

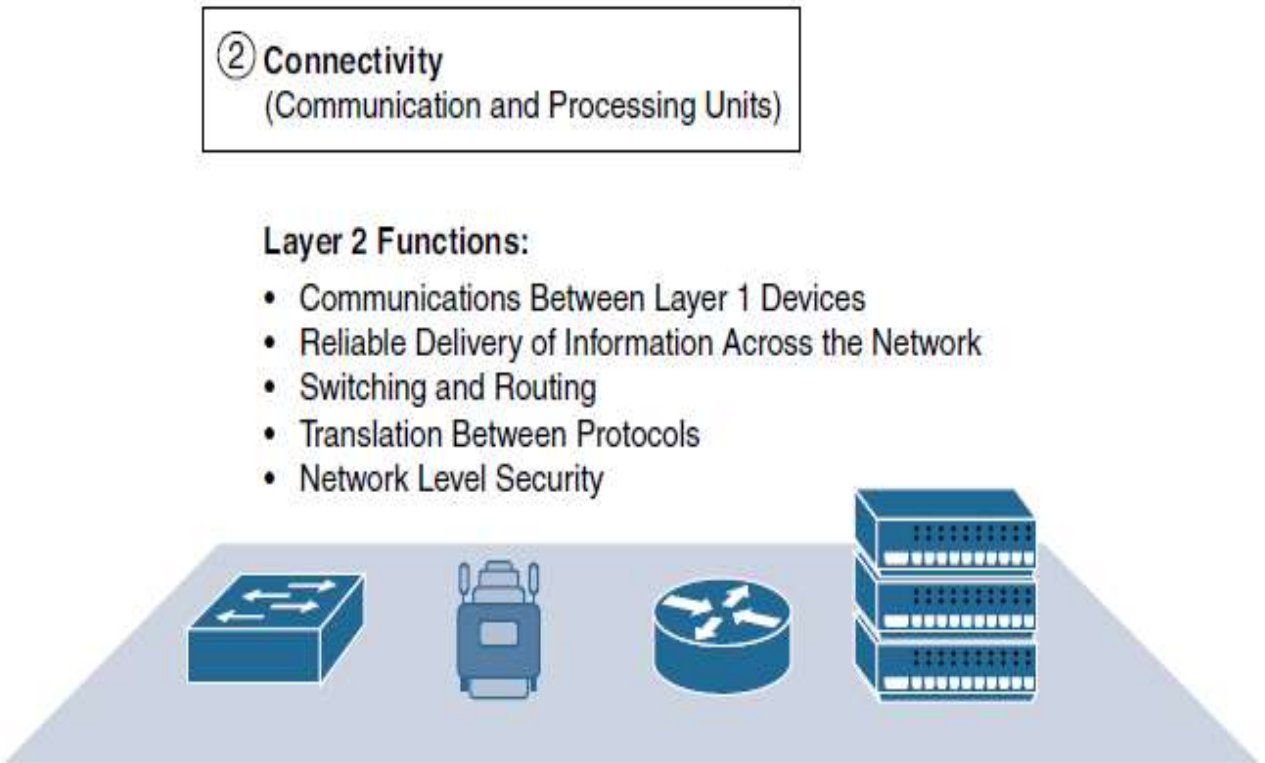


Figure 2-3 *IoT Reference Model Connectivity Layer Functions*

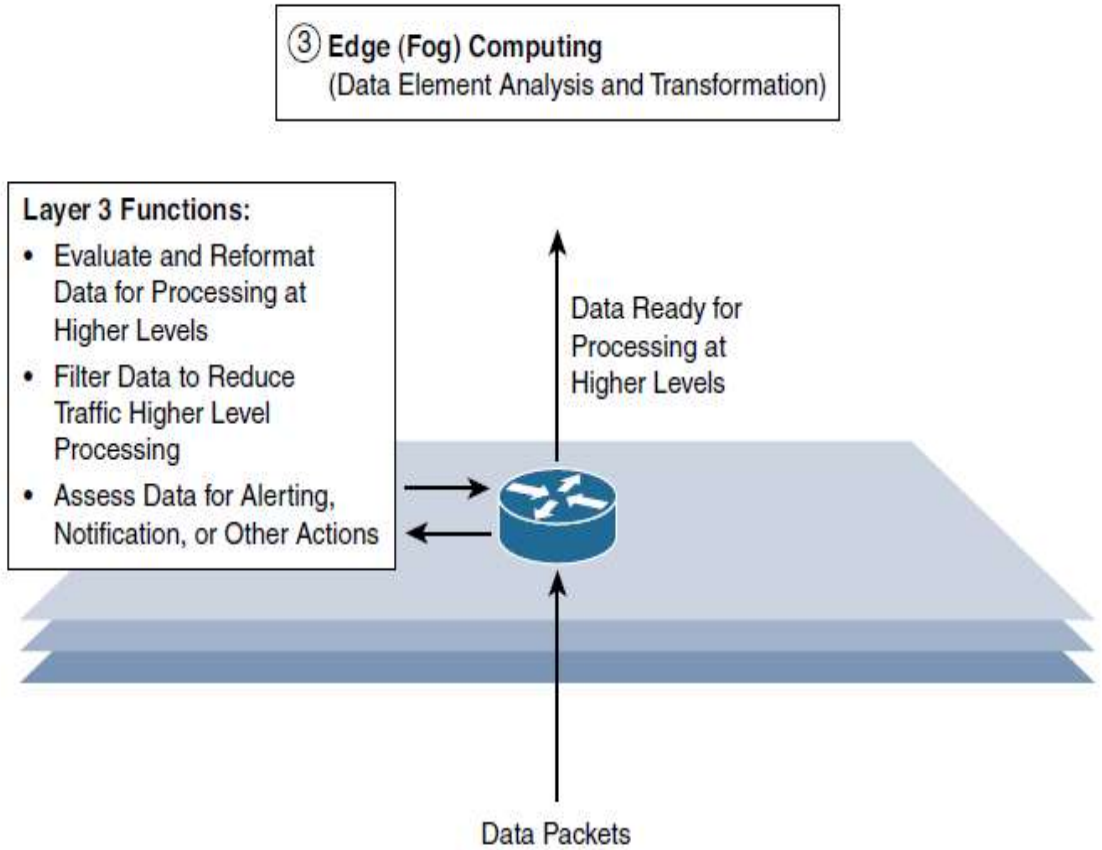


Figure 2-4 *IoT Reference Model Layer 3 Functions*

Upper Layers (4 to 7)

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

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.

IoT Reference Model Separation of IT and OT

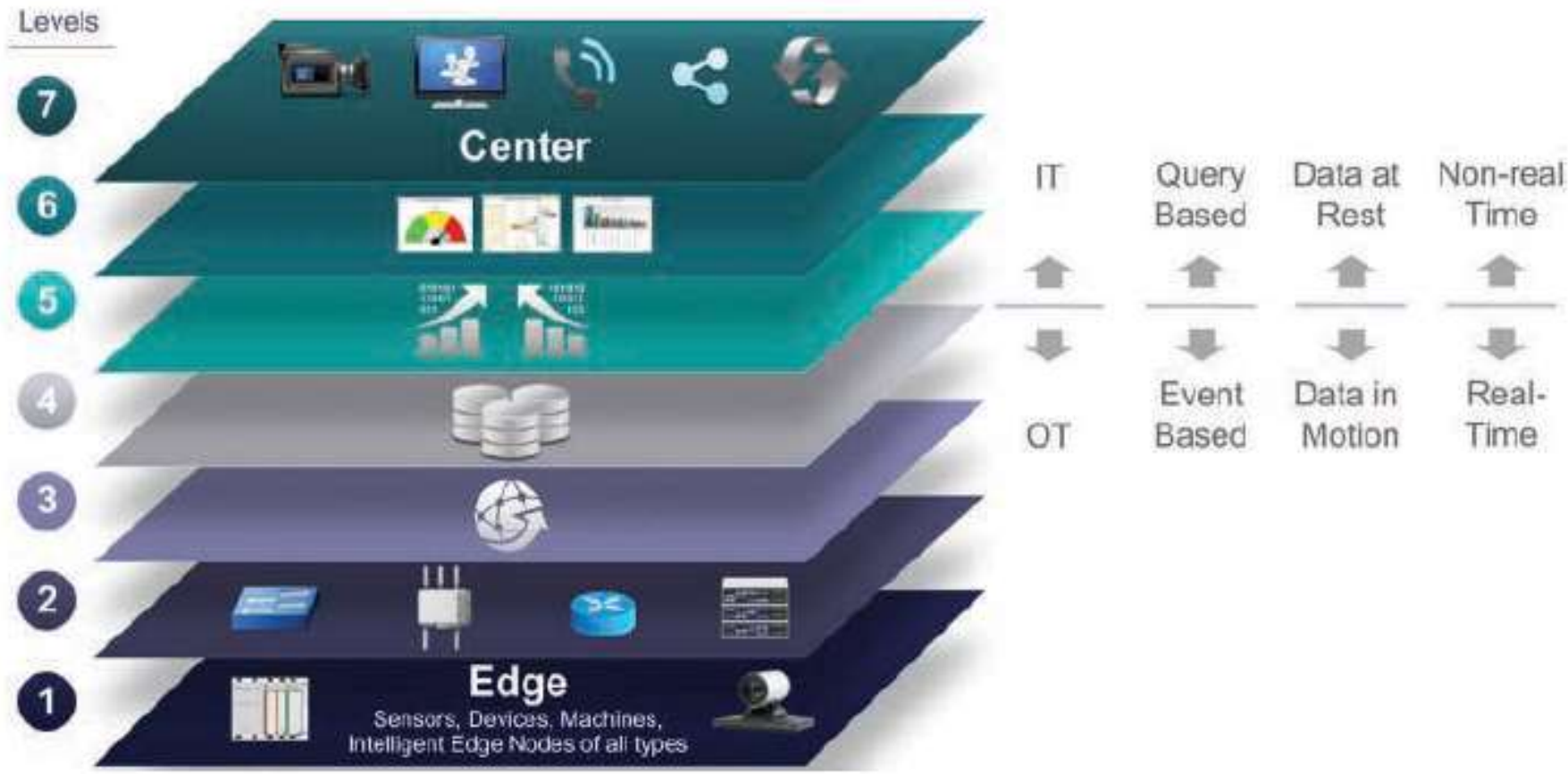


Figure 2-5 *IoT Reference Model Separation of IT and OT*

Alternative IoT Reference Models

- Purdue Model for Control Hierarchy - CISCO
- Industrial Internet Reference Architecture (IIRA) by Industrial Internet Consortium (IIC)
- Internet of Things Architecture (IoT-A) –Emerging Domains

Simplified IoT Architecture

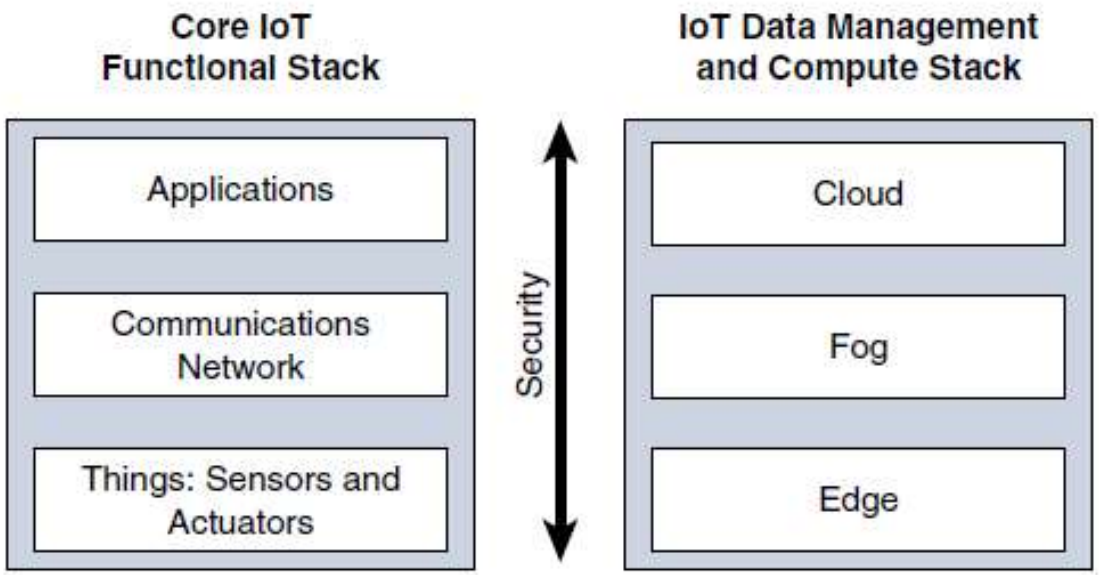


Figure 2-6 *Simplified IoT Architecture*

- Communication Network
  - Access Network Sublayer
  - Gateway and Backhaul Network
  - Network Transport Sublayer
  - IoT Network Management Sublayer

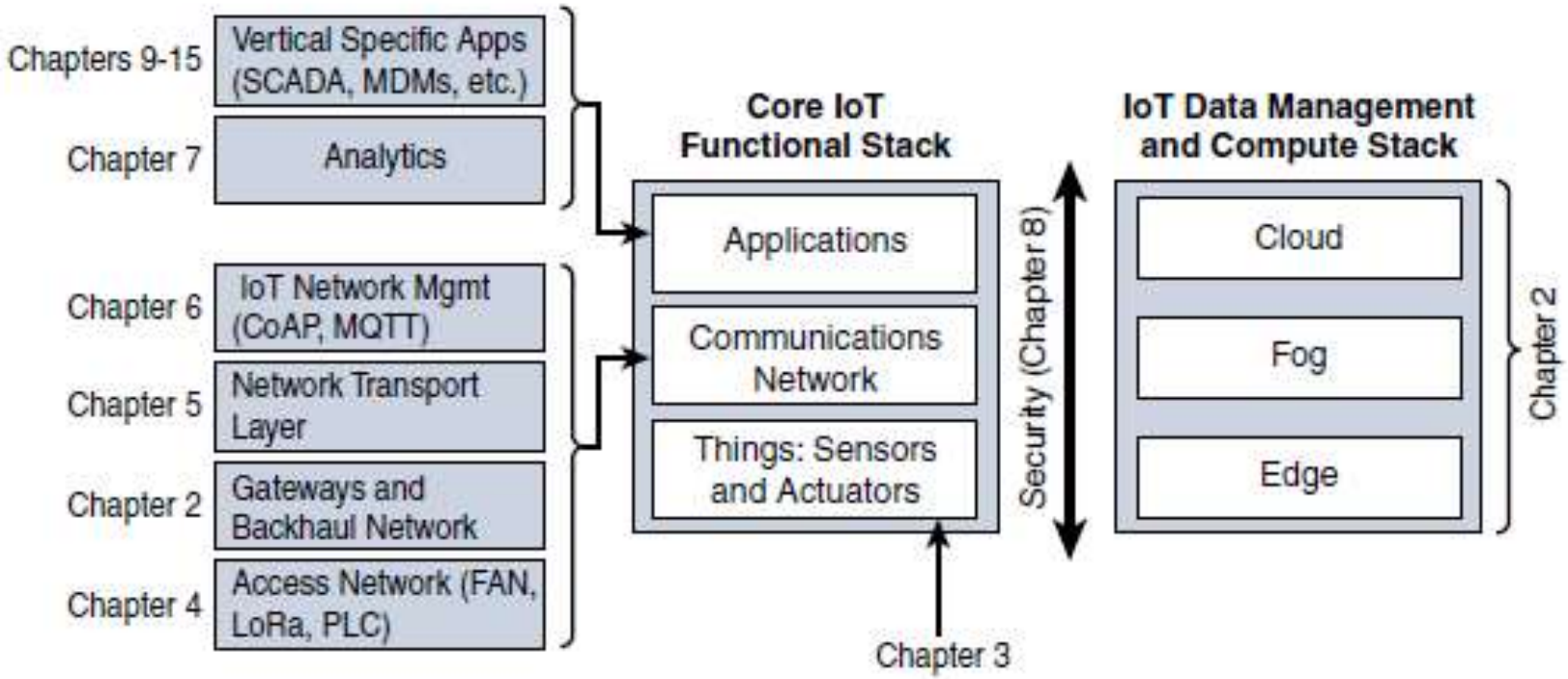


Figure 2-7 *Expanded View of the Simplified IoT Architecture*

The Core IoT Functional Stack

Layer 1:

"Things"

Layer 2:

Communications network layer

- Access network sublayer
- Gateways and backhaul network sublayer
- Network transport sublayer
- IoT network management sublayer

Layer 3:

Application and analytics layer

Layer 1
Things: Sensors and Actuators Layer

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

Sensor Applications Based on Mobility and Throughput

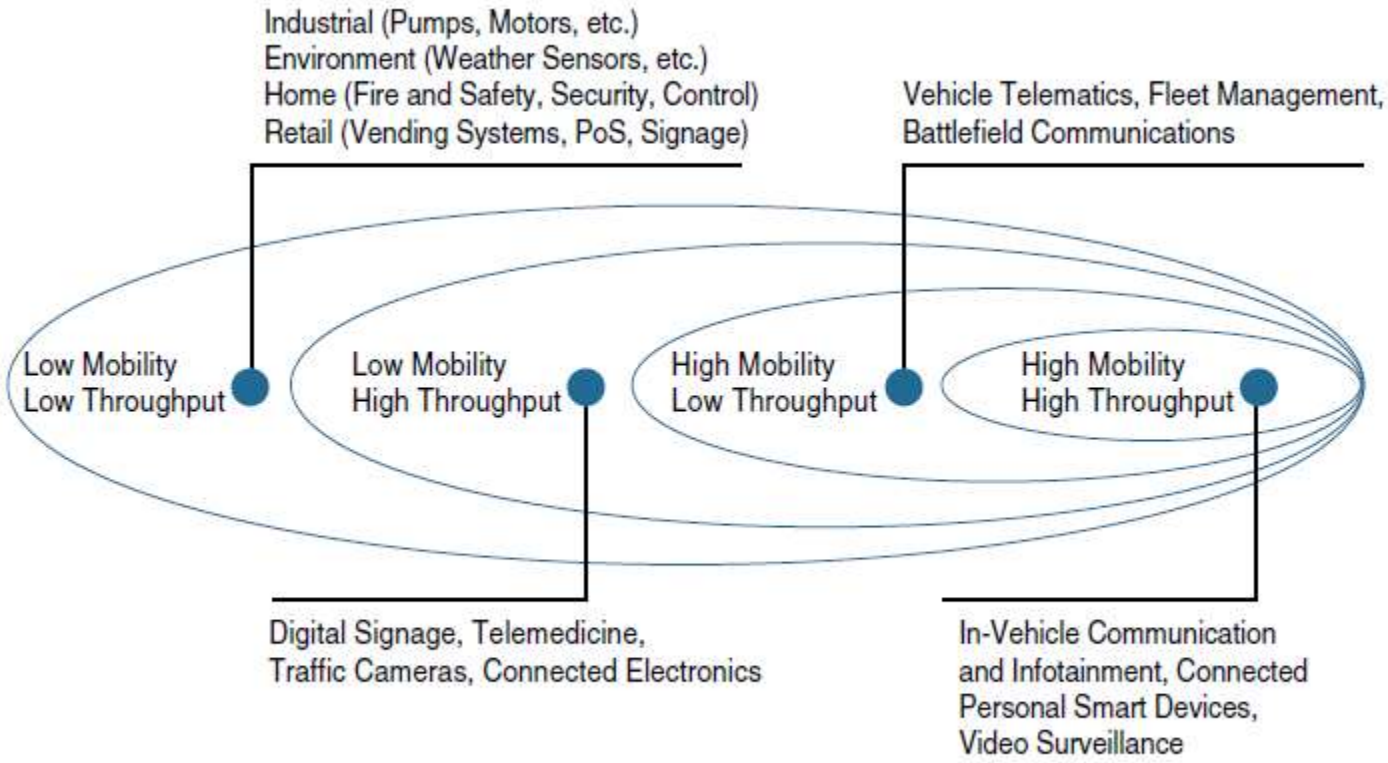


Figure 2-8 *Example of Sensor Applications Based on Mobility and Throughput*

Layer 2
COMMUNICATIONS NETWORK LAYER

- Transmission Capabilities (transmission range, data volume and frequency, sensor density and mobility)

- Environment is the main constraint to be considered for deployment

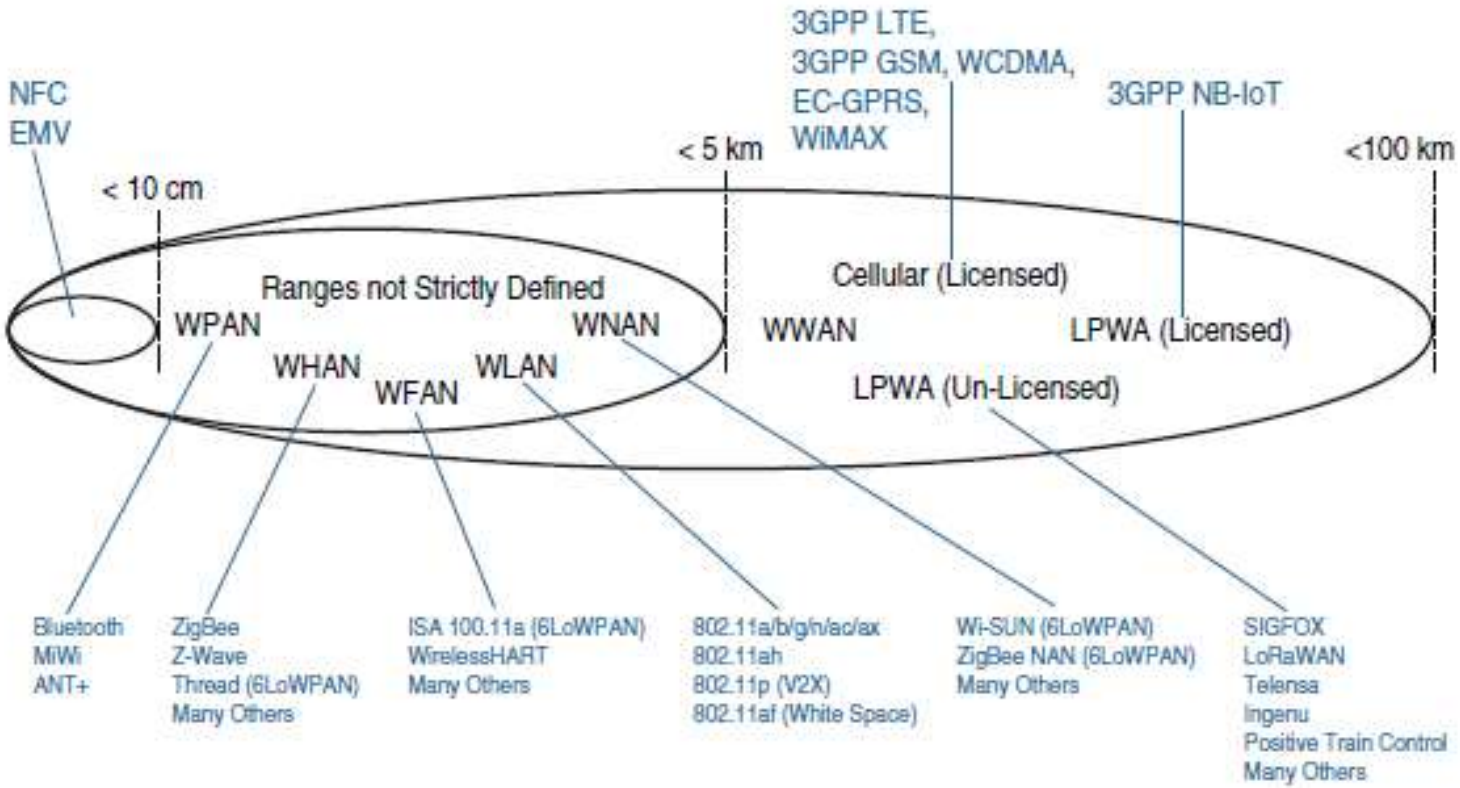
    - Temperature Variances
    - Humidity fluctuations
    - Industrial applications – kinetic forces, extreme vibrations
    - Hazardous location design – caustic materials

    How environment impact the equipment and also how equipment impact the environment

    Power Supplies and placement of sensors in IT and OT

Access Network Sublayer

- IoT network technology has a connection with the topology used.
- Designed with certain use cases in mind
    - What to connect
    - Where to connect
    - How much data to be transported at what interval and over what distance
- One key parameter determining the choice of access technology is the range between the smart object and the information collector.
- 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). By contrast, ZigBee(**Zonal Intercommunication Global-standard**) 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.
- Zigbee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. Zigbee is typically used in **low data rate applications that require long battery life and secure networking**. It is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks.



WPAN: Wireless Personal Area Network
WHAN: Wireless Home Area Network
WFAN: Wireless Field (or Factory) Area Network
WLAN: Wireless Local Area Network

WNAN: Wireless Neighborhood Area Network
WWAN: Wireless Wide Area Network
LPWA: Low Power Wide Area

Figure 2-9 *Access Technologies and Distances*

Common groups are as follows:

- PAN (personal area network)

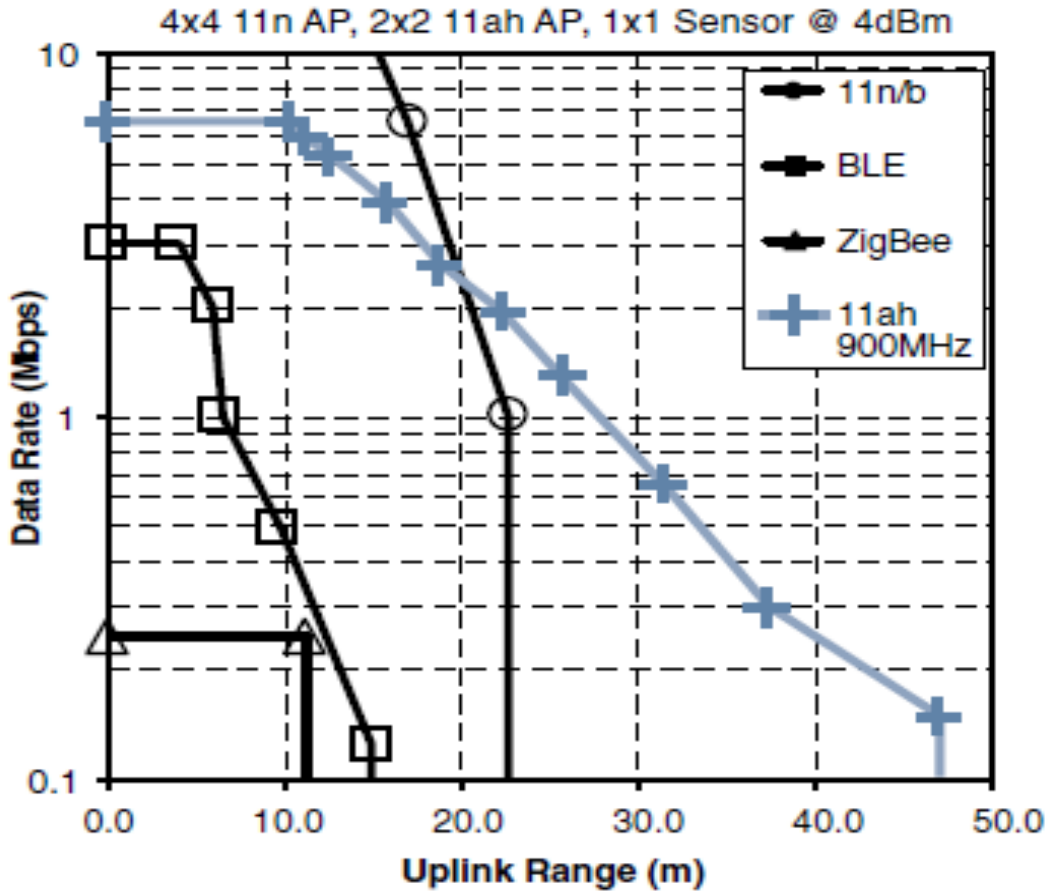
  Scale of a few meters , personal space around a person eg., Bluetooth
- HAN (home area network)

  Scale of a few tens of meters eg., ZigBee and Bluetooth Low Energy (BLE)
- NAN (neighborhood area network)

  Scale of a few hundreds of meters
- FAN (field area network)

  Scale of several tens of meters to several hundred meters.
- LAN (local area network)

  Scale of up to 100 m. eg., Ethernet or IEEE 802.11



Simulation Assumptions: 1% PER, 4dB NF,
32 Bytes, D-NLOS Fading, Indoor-to-Outdoor
PL Model. 900MHz has12dB propagation gain.

Sensor Antenna Gain: 11ah (-6.5dB)
and 11n (-4dB). AP antenna gain = 2dB.
* BT Long Range Adds 125 kbps and 500 kbps Modes

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

Some technologies offer flexible connectivity structure to extend communication possibilities:

- **Point-to-point topologies**

These topologies allow one point to communicate with another point.

- **Point-to-multipoint topologies**

These topologies allow one point to communicate with more than one other point.

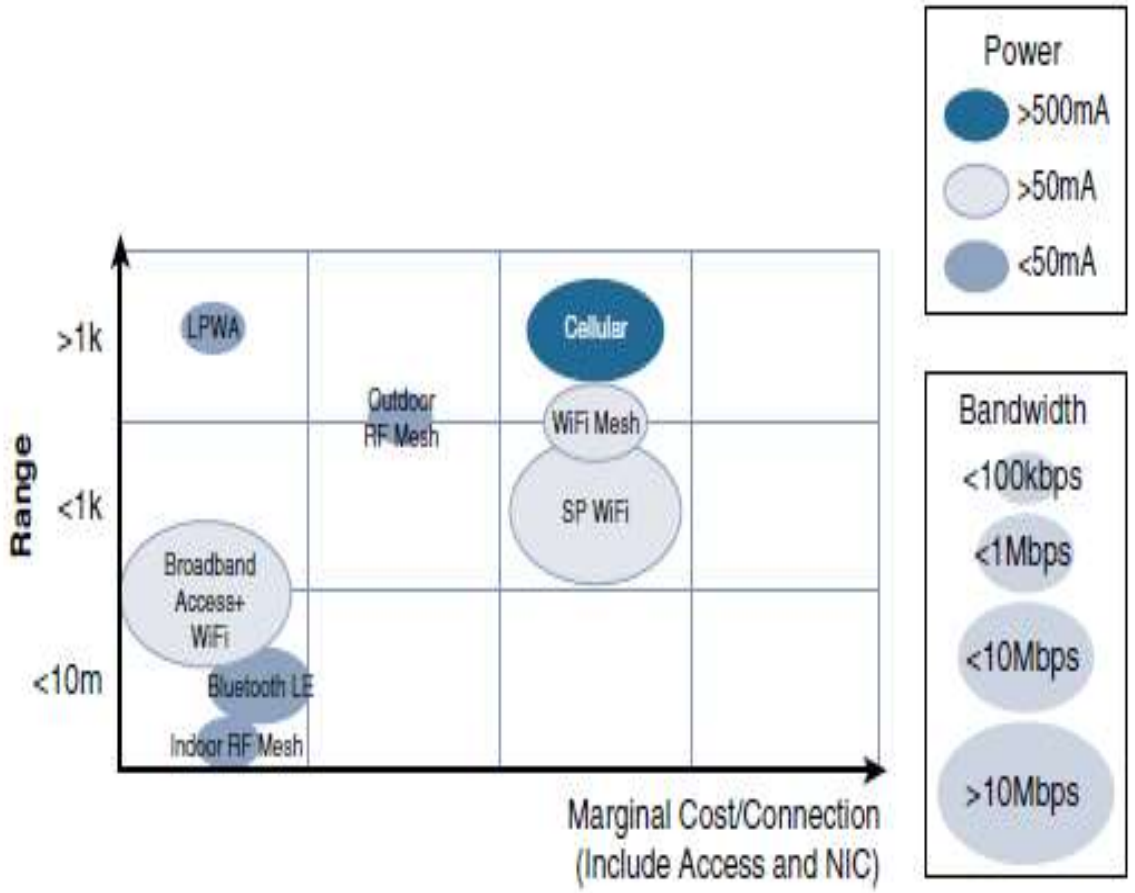


Figure 2-11 *Comparison Between Common Last-Mile Technologies in Terms of Range Versus Cost, Power, and Bandwidth*

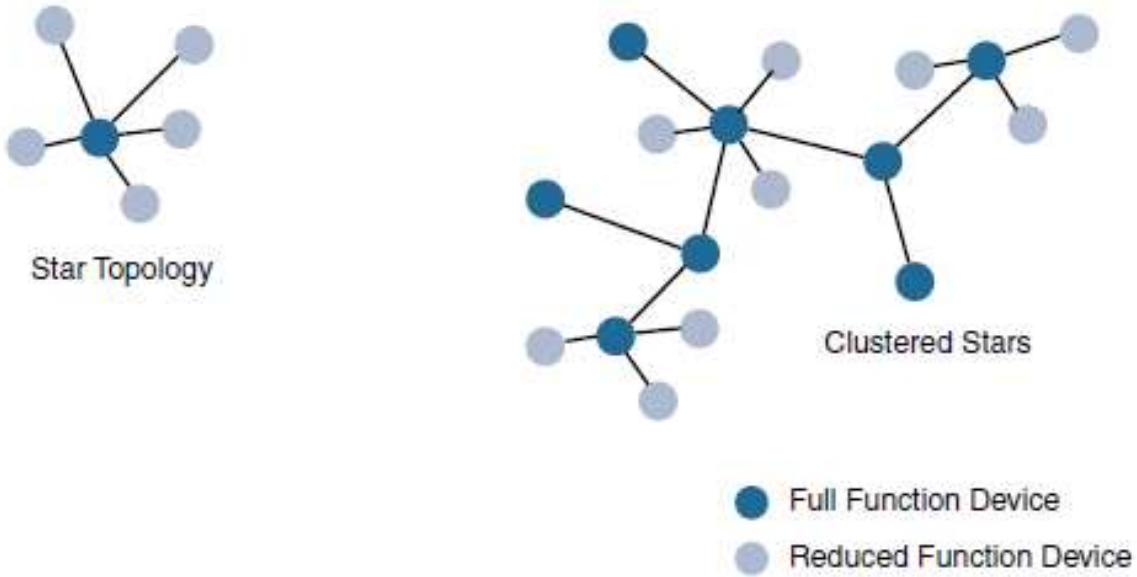


Figure 2-12 *Star and Clustered Star Topologies*

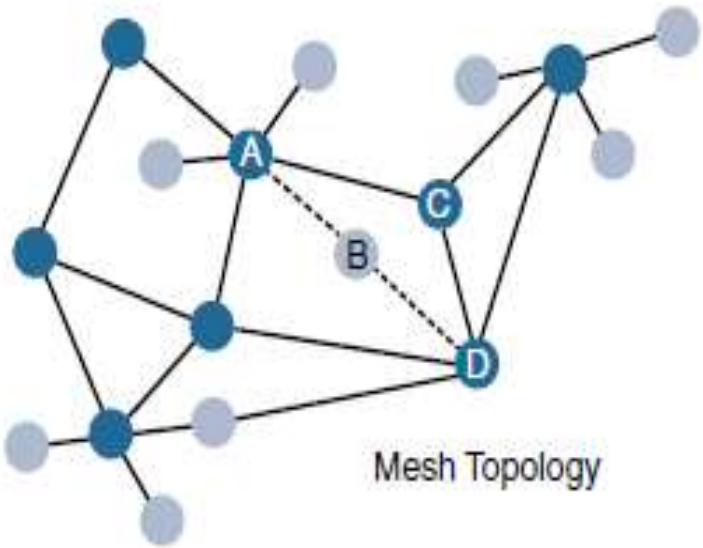


Figure 2-13 *Mesh Topology*

Gateways and Backhaul Sublayer

Table 2-4 *Architectural Considerations for WiMAX and Cellular Technologies*

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)

Network Transport Sublayer

- The previous section describes 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.

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.
- Constrained Application Protocol (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).
- Another common IoT protocol utilized in these middle to upper layers is Message Queue Telemetry Transport (MQTT).
- MQTT uses a broker-based architecture.

Layer 3: Applications and Analytics Layer

- Analytics Versus Control Applications

  Analytics application

  Control application

- Data Versus Network Analytics

  Data analytics

  Network analytics

- Data Analytics Versus Business Benefits
- Smart Services

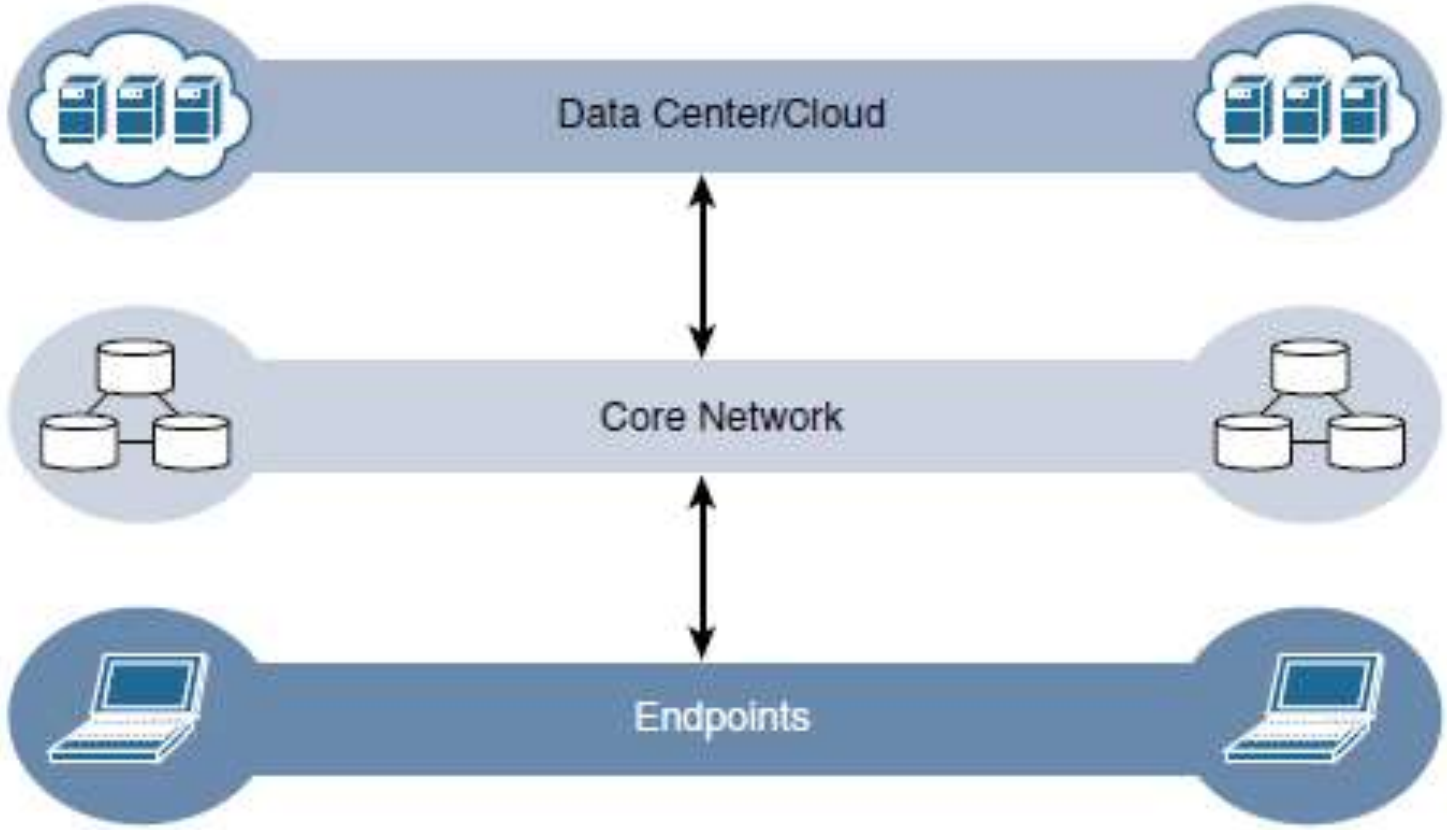
IoT Data Management and Compute Stack

- How can we categorise data generated by IoT sensors?
- Eg: Smart Meter – Real value of data is given by Meter Management System (MMS)
- What happens when there is an interruption of connectivity to meters?
- How the analytics of data helps in this scenario?
- How the data collected from the sensors are processed ?
- Advantage:

Challenges

- Minimizing Latency
- Conserving Network Bandwidth
- Increasing local efficiency
- IMPEDANCE MISMATCH

TRADITIONAL IT Cloud Computing Model



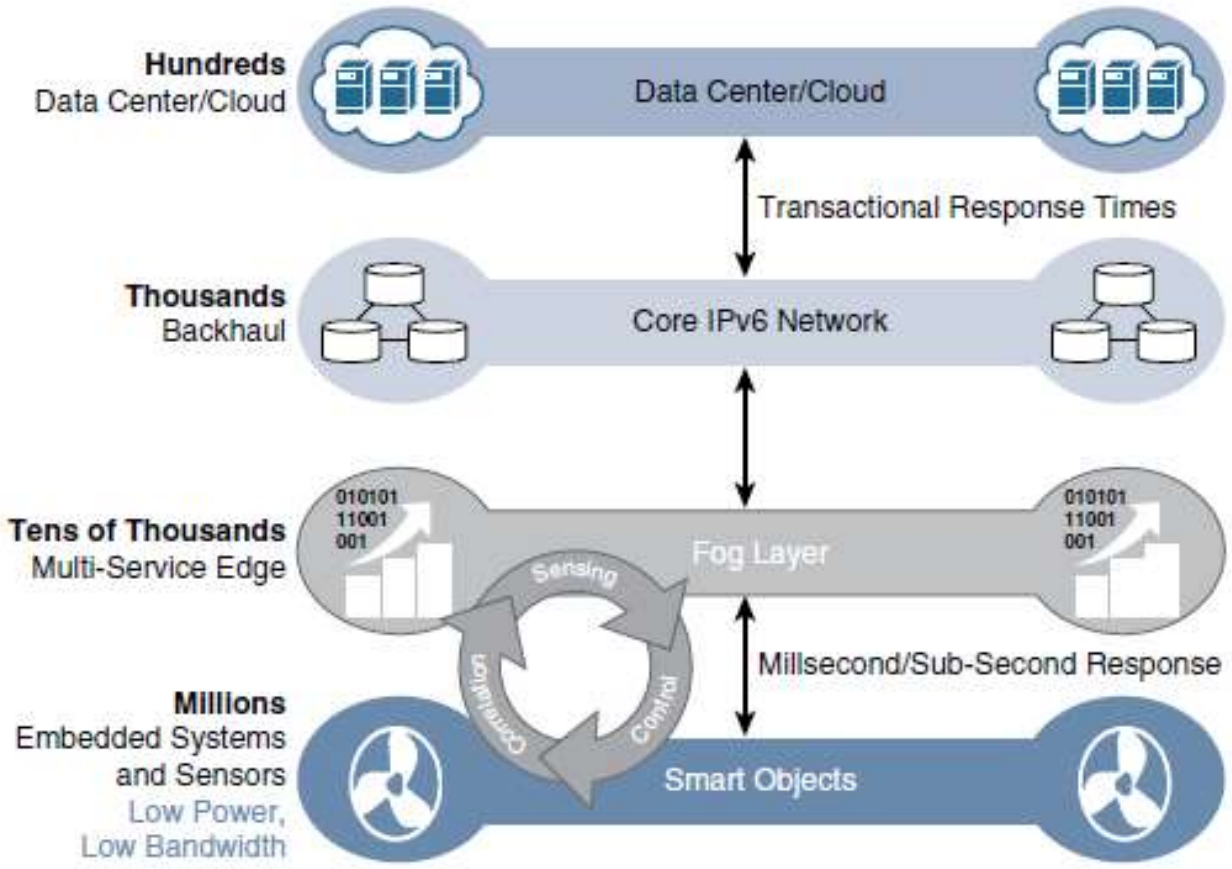
What are the highlighted Data-related problems ?

- Bandwidth in lastmile IoT Network
- Latency
- Network backhaul
- Volume of data
- Big data is getting better

FOG COMPUTING

- Distribute data management throughout IoT system
- Any device with computing, storage, and network connectivity – fog node
- Eg: Industrial controllers, switches, routers, embedded servers and IoT Gateways.
- Minimizes latency, offloads gigabytes of network traffic
- Maintains the sensitive information inside local network

FOG COMPUTING



CHARACTERISTICS OF FOG COMPUTING

- Contextual location awareness and low latency
- Geographic distribution
- Deployment near IoT endpoints
- Wireless communication between Fog and IoT ENDPOINT
- Use for real-time interactions

EDGE COMPUTING

Edge computing can also called as

Hierarchy of Edge, Fog and Cloud

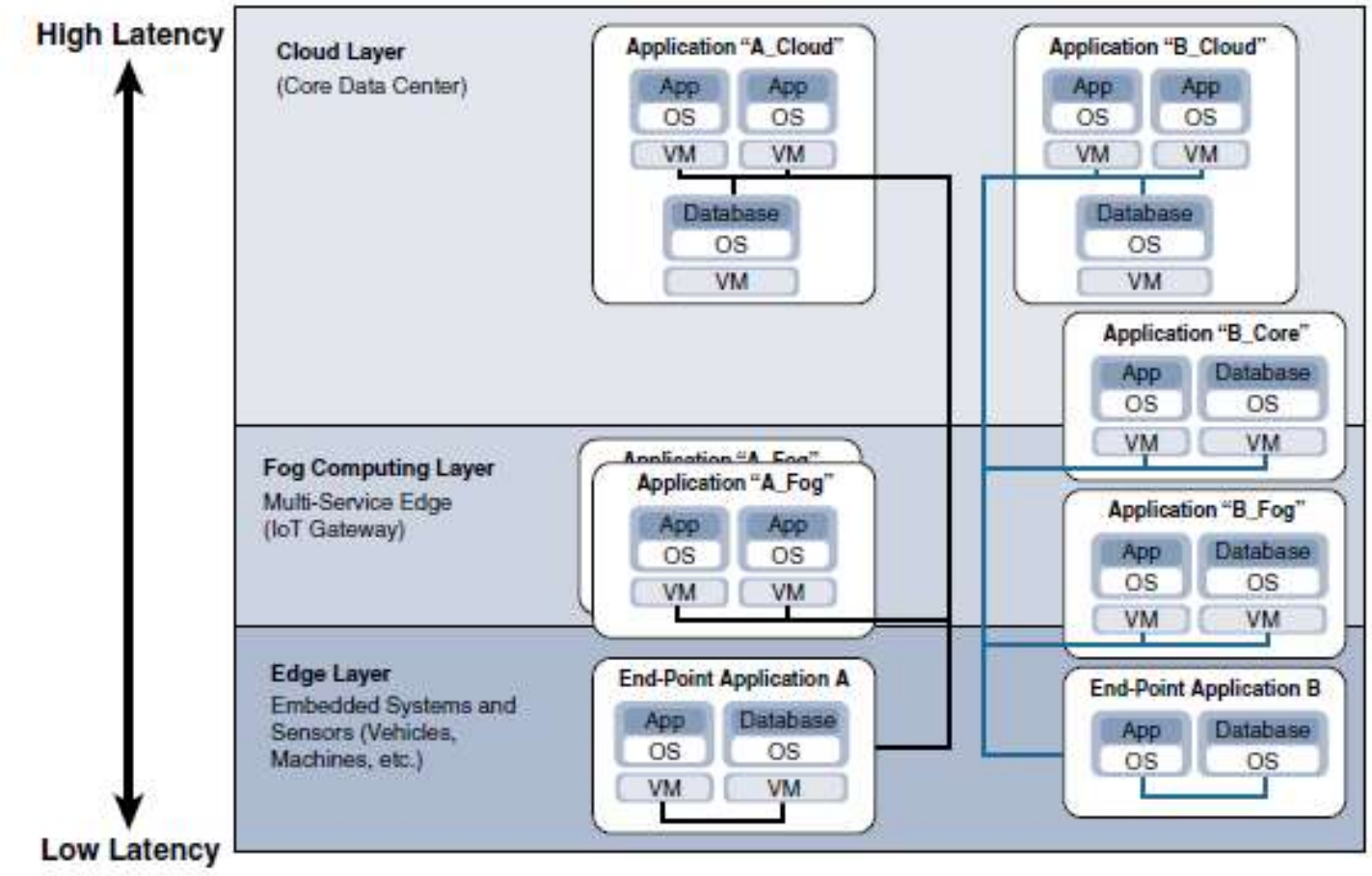


Figure 2-16 *Distributed Compute and Data Management Across an IoT System*

- Amount of data
- Time-sensitivity