INTERNET OF THINGS

UNIT-1

M.KAIVALYA, M.Tech
Assistant Professor
Department of Electronics and Communication Engineering
Aditya College of Engineering & Technology
Email: *kaivalya.mathamsetti@acet.ac.in*

CONTENTS

- Introduction to IoT
- Architectural Overview
- Design principles and needed capabilities
- Basics of Networking
- M2M and IoT Technology Fundamentals
- Devices and gateways
- Data management
- Business processes in IoT
- Everything as a Service (XaaS)
- Role of Cloud in IoT,
- Security aspects in IoT.

Introduction

Internet of Things : Definition
IoT Vision
Examples

"Internet" Definition

Internet

- A vast global network of connected servers, clouds, computers, tablets, mobiles, devices and systems
- Uses the Internationally used protocols and connecting systems.

"Internet" Usages

- Enables sending, receiving, or communicating the information, messages, alerts, ……
- Between devices, sensors, servers Cloud services, applications, business processes……

“Things” Definition

- Thing refers to a physical object, an action, idea, situation or activity, in case when we need not be precise.

Internet of Things- Wikipedia Definition

- The network of physical objects or "things" embedded with electronics, software, sensors.
- Connected so as to enable achieving greater value and offer service by exchanging data with the manufacturer, operator and/or other connected devices
- Each thing uniquely identifiable
- Things embedded with sensors and computing system
- Able to interoperate within the existing Internet infrastructure

“Internet of Things” extends Internet uses

- Internet of Things (IoT) extends the uses of Internet by providing the communication, and thus inter-network of the physical objects, devices, machines,vehicles; all referred as “things”.

Start of "Internet of Things" Concept Development

- Concept of IoT started with things with the communicating devices for the identity, called RFIDs
- RFIDs connect to Internet
- RFID- Radio Frequency Identification

“Internet of Things” Devices Concept

- Connected devices could be tracked, controlled or monitored using remote computers, Applications, Business Processes,…….

Smart Devices

- Embedded devices with computing and communicating capabilities

A Smart Umbrella

Flashing LED

Weather Website

Internet

Smart Hyper-connected Devices

Hyper connectivity:

- ‘use of multiple systems and devices to remain constantly connected to networks, social networks and streams of information’.
- Smart devices constantly connect to networks
- For example, a streetlights network constantly connected to a central controlling station/server.

IoTs Vision

- A vision where things (wearable, watch, alarm clock, home devices, surrounding objects with) become smart and behave alive through sensing, computing and communicating systems

- A vision where embedded devices interact with remote objects or persons through connectivity, for examples, using Internet or Near Field Communication or other technologies.

Origin of Terminology:

In the 2000's, we are heading into a new era of ubiquity, where the "users" of the Internet will be Counted in billions and where humans may become the minority as generators and receivers of traffic. Instead, most of the traffic will flow between devices and all kinds of "things", thereby creating a much wider and more complex Internet of Things

- The title of the report was “Internet of Things”
- Discussed the possibility of Internet connected M2M connectivity networks, extending to common household devices
- Some areas identified as IoT enablers:
  - RFID,
  - Nanotechnology
  - Sensors
  - Smart Networks

➢Business/Manufacturing

•Real-time analytics of supply chains and equipment, robotic machinery.

➢Healthcare

• portable health monitoring, electronic record keeping, pharmaceutical safeguards.

➢Retail

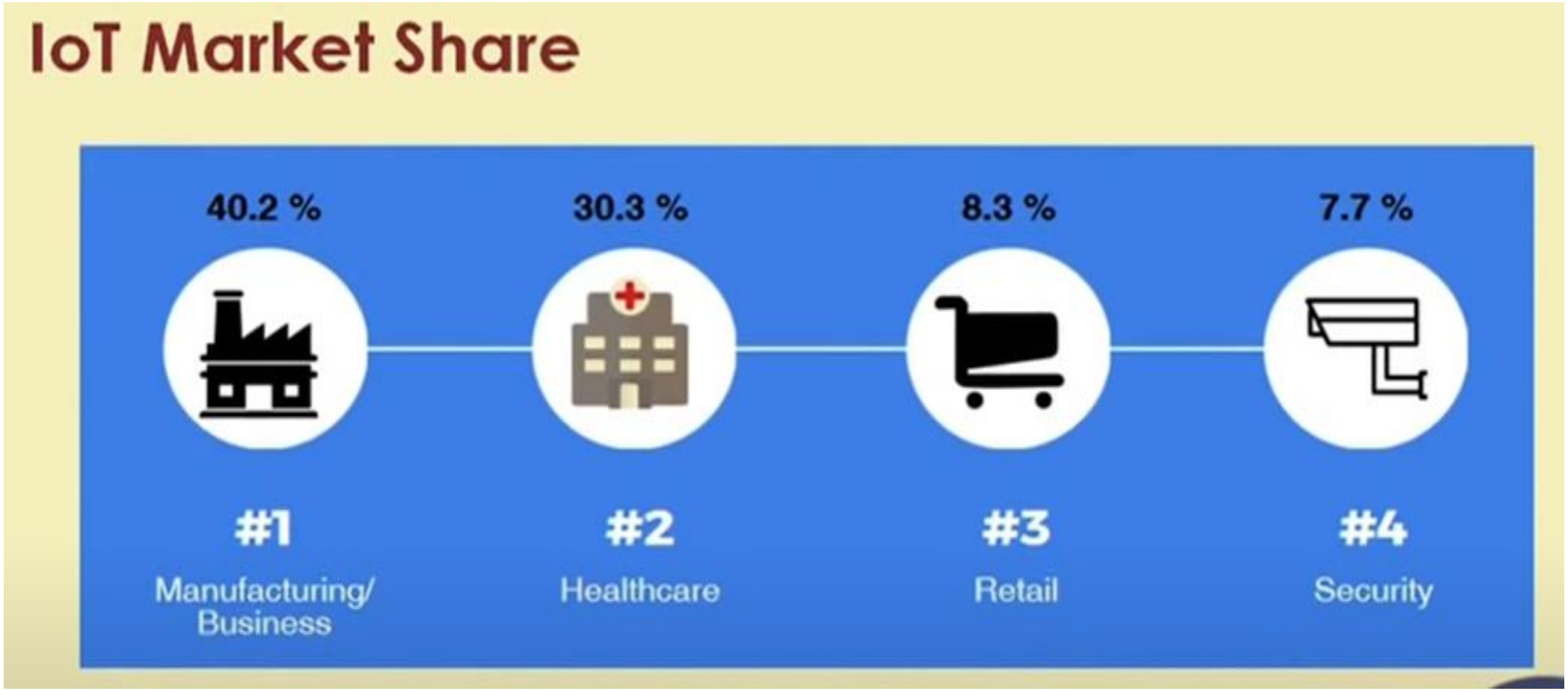
• Inventory tracking, smart phone purchasing, anonymous analytics of consumer choices.

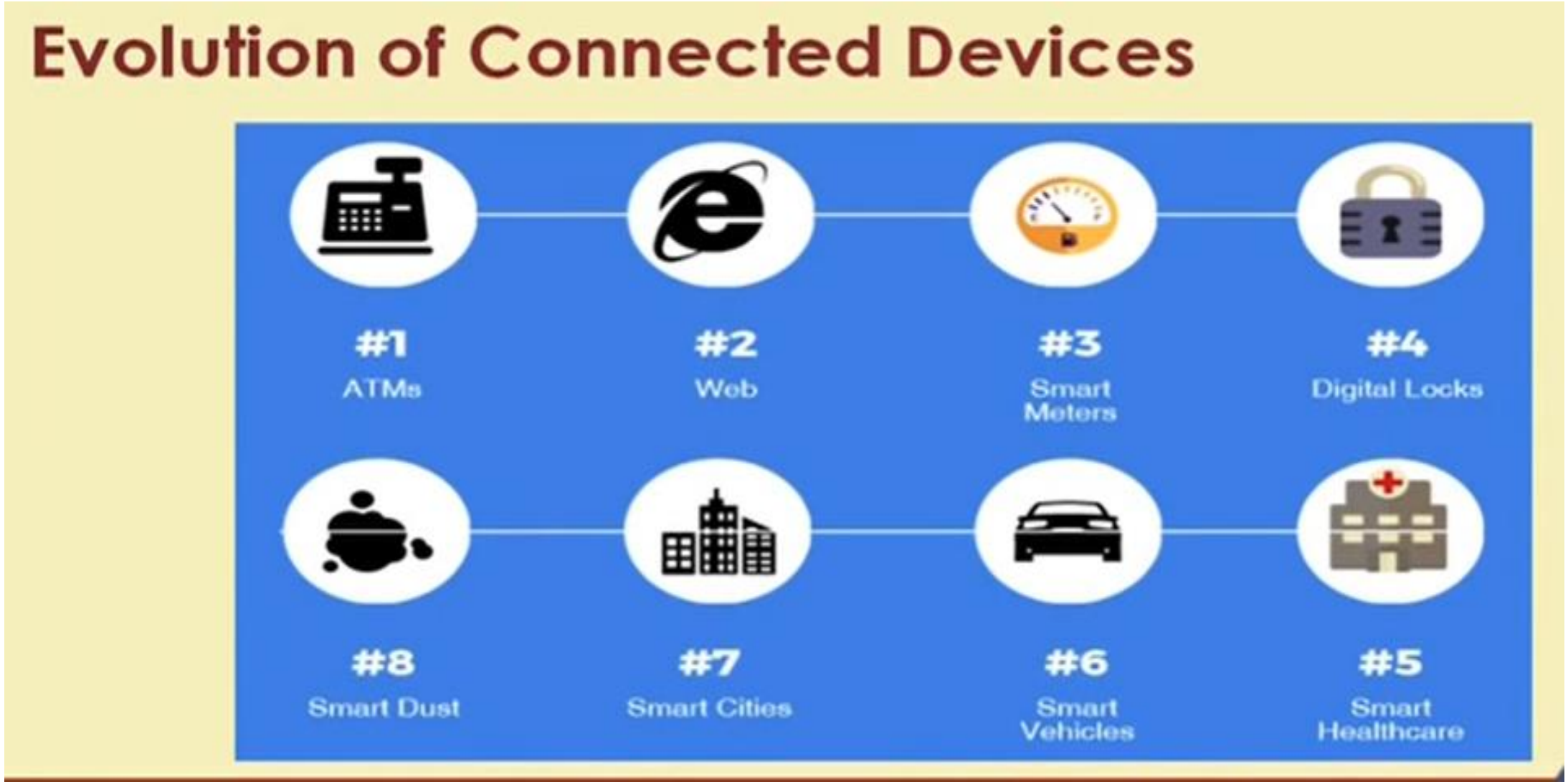
➢Security

•Biometric and facial recognition locks, remote sensors

Characteristics:

- Efficient, scalable and associated architecture
- Unambiguous naming and addressing
- Abundance of sleeping nodes, mobile and non –IP devices
- Intermittent connectivity

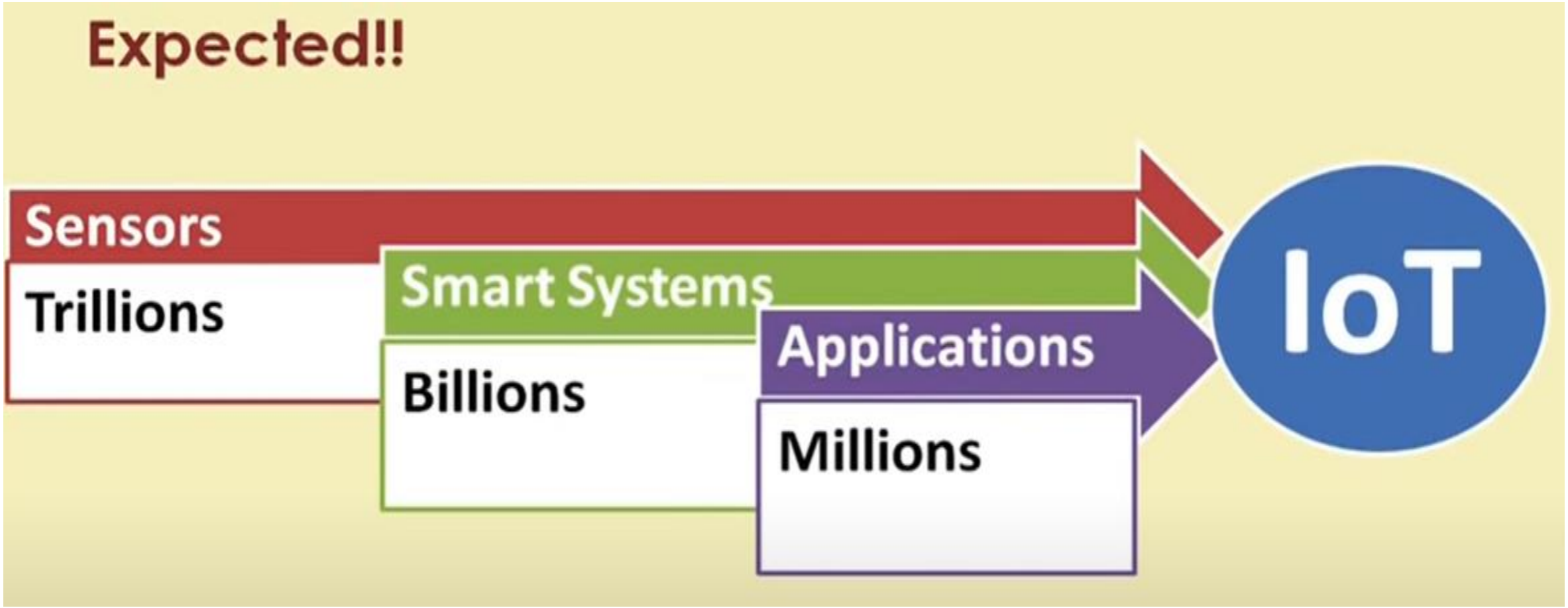

IoT Market Share
40.2 %
30.3 %
8.3 %
7.7 %
#1
Manufacturing/
Business
#2
Healthcare
#3
Retail
#4
Security


Evolution of Connected Devices
#1
ATMs
#2
Web
#3
Smart Meters
#4
Digital Locks
#8
Smart Dust
#7
Smart Cities
#6
Smart Vehicles
#5
Smart Healthcare

- ✓ ATM
  - These ubiquitous money dispensers went online for the first time way back in 1974.
- ✓ WEB
  - World Wide Web made its debut in 1991 to revolutionize computing and communications.
- ✓ SMART METERS
  - The first power meters to communicate remotely with the grid were installed in the early 2000s.
- ✓ DIGITAL LOCKS
  - Smartphones can be used to lock and unlock doors remotely, and business owners can change key codes rapidly to grant or restrict access to employees and guests.

Modern Day IoT Applications

- ✓ Smart Parking
- ✓ Structural health
- ✓ Noise Urban Maps
- ✓ Smartphone Detection
- ✓ Traffic Congestion
- ✓ Smart Lighting
- ✓ Waste Management
- ✓ Smart Roads
- ✓ River Floods
- ✓ Smart Grid
- ✓ Tank level
- ✓ Photovoltaic Installations
- ✓ Water Flow
- ✓ Silos Stock Calculation
- ✓ Perimeter Access Control
- ✓ Liquid Presence


Expected!!
Sensors
Trillions
Smart Systems
Billions
Applications
Millions
IoT


IoT Enablers
IMPLEMENTATION
ZigBee
RFID
LoWPAN
LoRa
INSTEON
CONNECTIVITY
ENABLING TECHNOLOGIES
BIG DATA
AI
DEEP LEARNING

Baseline Technologies

- ✓ A number of technologies that are very closely related to IoT include
  - Machine-to-Machine (M2M) communications,
  - Cyber-Physical-Systems (CPS)
  - Web-of-Things (WoT).

IoT vs. M2M

- ✓ **M2M is part of the IoT, while M2M standards have a prominent place in the IoT standards landscape.**
- ✓ However, IoT has a broader scope than M2M, since it comprises a broader range of interactions, including interactions between devices/things, things and people, things with applications and people with applications.
- ✓ It also enables the composition of workflows comprising all of the above interactions.
- ✓ IoT includes the notion of internet connectivity (which is provided in most of the networks outlined above), but is not necessarily focused on the use of telcom networks.

IoT vs. WoT

- ✓ From a developer's perspective, the WoT enables access and control over IoT resources and applications using mainstream web technologies (such as HTML 5.0, JavaScript, Ajax, PHP, Ruby n' Rails etc.).
  - The approach to building WoT is therefore based on RESTful principles and REST APIs, which enable both developers and deployers to benefit from the popularity and maturity of web technologies.
  - Still, building the WoT has various scalability, security etc. challenges, especially as part of a roadmap towards a global WoT.

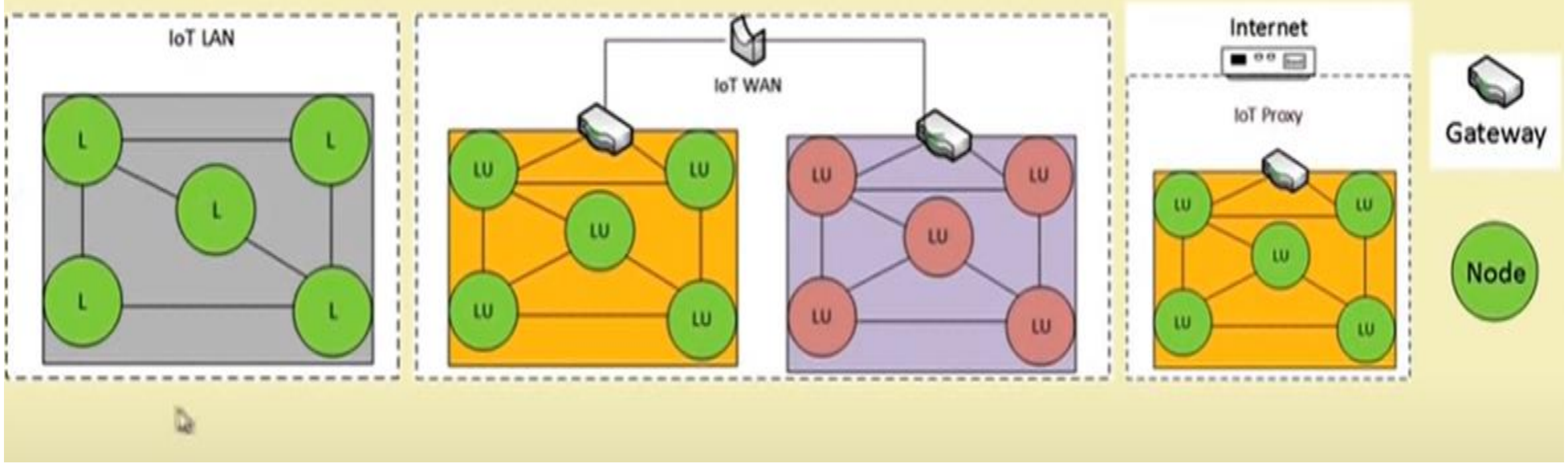
IoT Resulting in Address Crunch

- Estimated 20-50 billion devices by 2024
- Reason is the integration of existing devices, smart devices as well as constrained nodes in a singular framework.
- Integration of various connectivity features such as cellular, Wi-Fi, Ethernet with upcoming ones such as Bluetooth Low Energy (BLE), DASH7, Insteon, IEEE 802.15.4, etc.

Connectivity Terminologies

IoT LAN	•Local, Short range Comm, May or may not connect to Internet, Building or Organization wide
IoT WAN	•Connection of various network segments, Organizationally and geographically wide, Connects to the internet
IoT Node	•Connected to other nodes inside a LAN via the IoT LAN, May be sometimes connected to the internet through a WAN directly
IoT Gateway	•A router connecting the IoT LAN to a WAN to the Internet, Can implement several LAN and WAN, Forwards packets between LAN and WAN on the IP layer
IoT Proxy	•Performs active application layer functions between IoT nodes and other entities

IoT Network Configurations



Internet of Things– Conceptual Frameworks and Architecture

- Physical Object + Controller, Sensor and Actuators + Internet = Internet of Things … (1.1)
- Source: An equation given by Adrian McEwen and Hakim Cassimally, ‘Designing Internet of things’, Wiley, 2014

Another IoT Conceptual Architecture

- Gather + Enrich + Stream + Manage + Acquire + organize and Analyze = Internet of Things Enterprise & Business Applications, Integration … (1.2)
  [An Equation based on Oracle IoT Architecture in Fig. 1.5 of book]

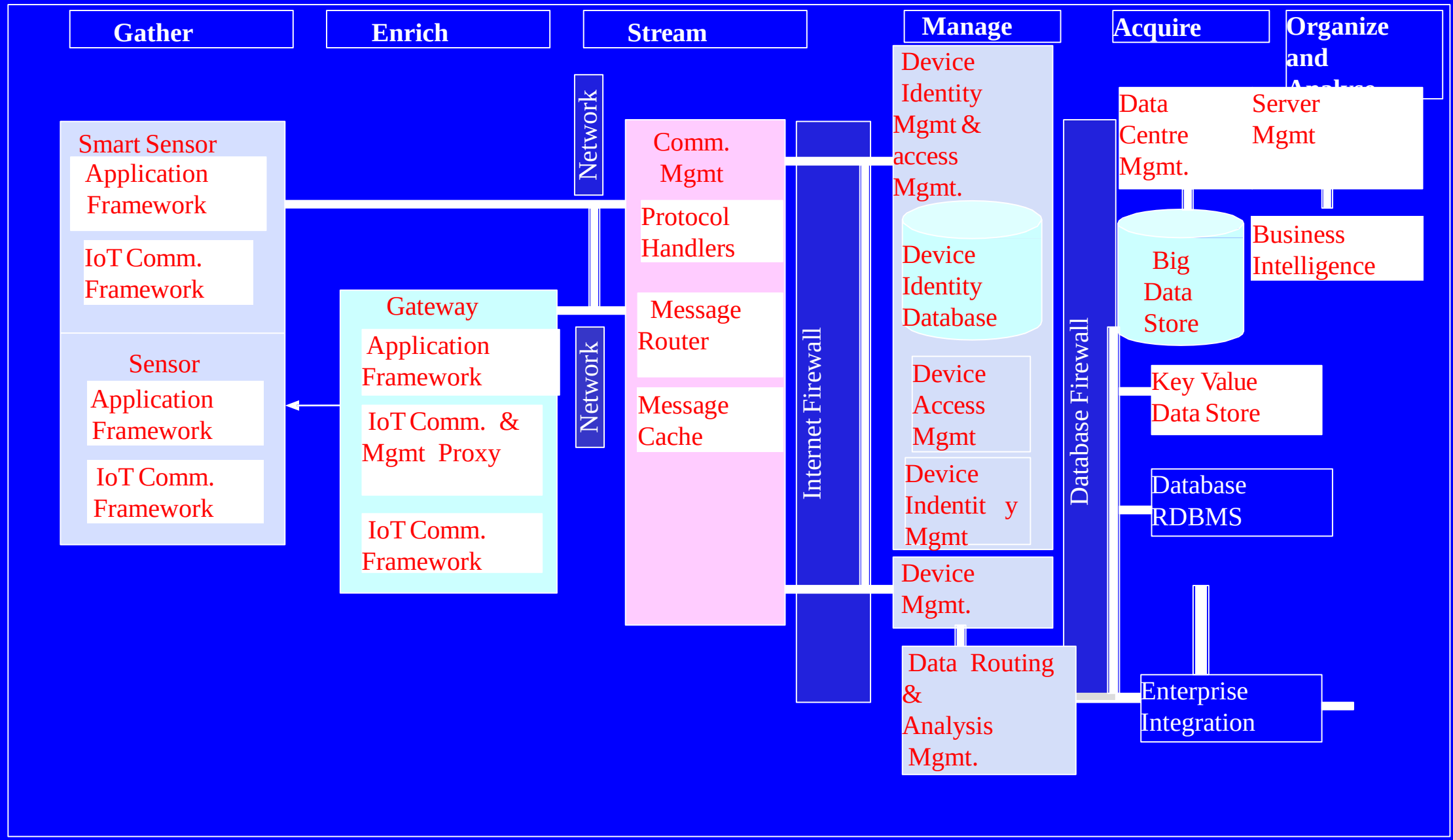
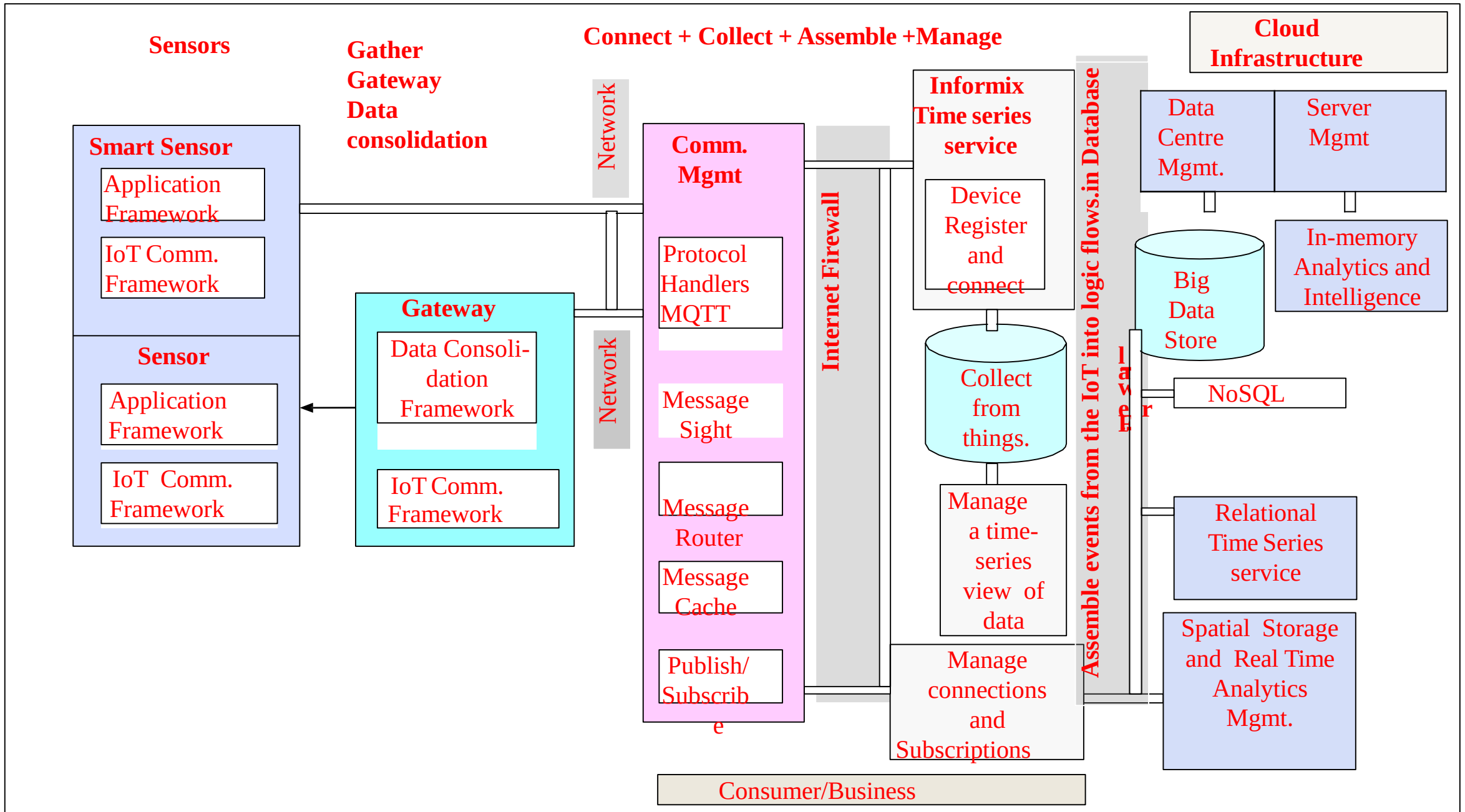
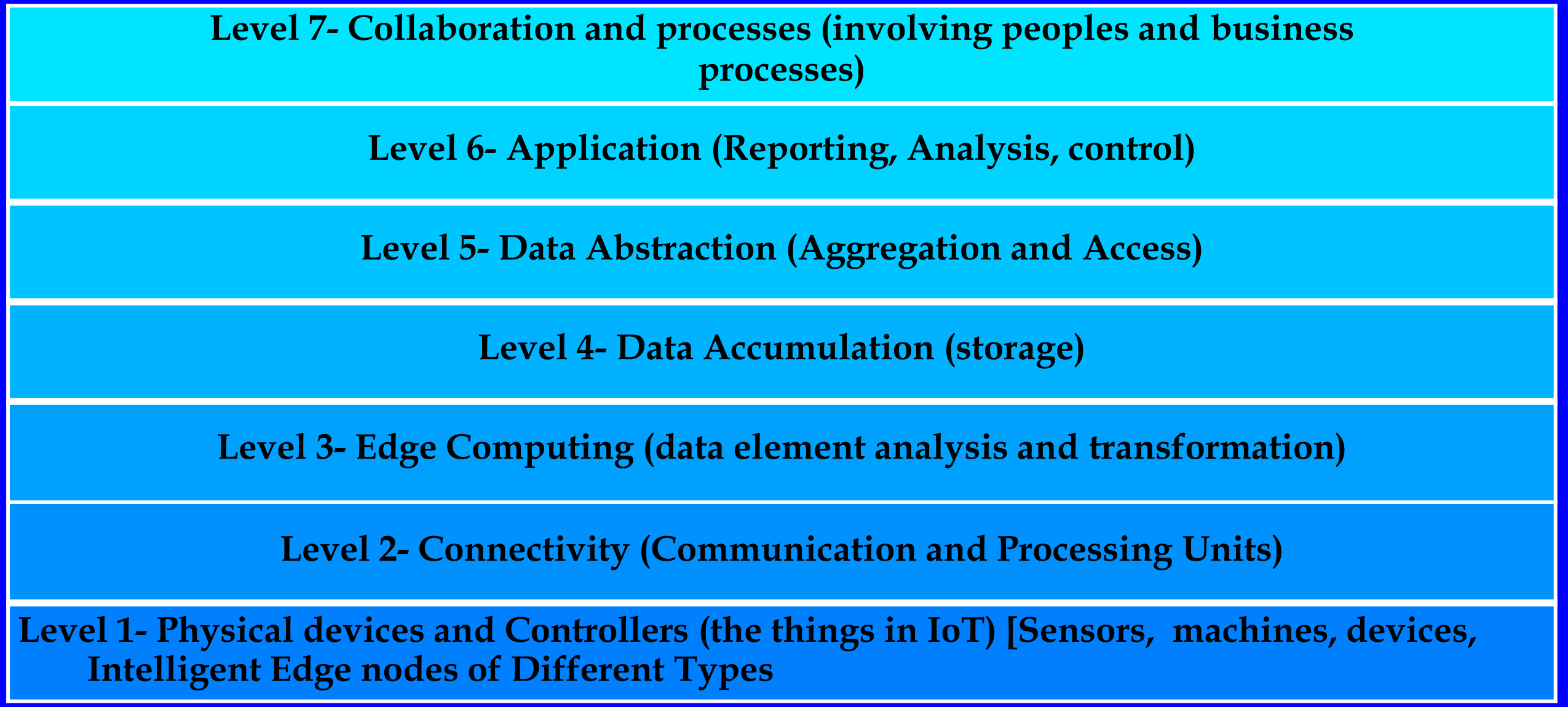


Figure 1.5 Oracle's IoT Architecture

Another IoT Conceptual Framework

- Gather + Consolidate + Connect + Collect + Assemble + Manage and Analyze = Internet of Things connected to Cloud Services … (1.3) [An Equation based on the IBM Framework.


Sensors
Gather
Gateway
Data
consolidation
Connect + Collect + Assemble +Manage
Cloud
Infrastructure
Smart Sensor
Application Framework
IoT Comm. Framework
Sensor
Application Framework
IoT Comm. Framework
Gateway
Data Consoli-dation Framework
IoT Comm. Framework
Network
Network
Comm. Mgmt
Protocol Handlers MQTT
Message Sight
Message Router
Message Cache
Publish/ Subscribe
Internet Firewall
Informix Time series service
Device Register and connect
Collect from things.
Manage a time-series view of data
Manage connections and Subscriptions
Assemble events from the IoT into logic flows.in Database
Data Centre Mgmt.
Server Mgmt
In-memory Analytics and Intelligence
Big Data Store
NoSQL
Relational Time Series service
Spatial Storage and Real Time Analytics Mgmt.
Consumer/Business



Ch01Fig. 1.4 An IOT reference model CISCO conceptual framework

Internet of Things Reference Model

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 IoE)

Technology Behind the IoT

1. Hardware
2. Integrated development environment (IDE) and Software
3. a. Embedded Devices/M2M Communication Protocols
   b. Network Protocols
4. Software Platforms
5. a. Analyzing and Visualizing
   b. Analytics & Machine Learning

1. Hardware

- Embedded Devices
- Embedded hardware/software with Sensors/Actuators
- Hardware (Arduino Raspberry Pi, Intel Edison, mBed, Beagle Bone Black and Wireless SoC, …..)

2.Integrated development environment (IDE) and Software

- Enables developing device software, firmware and APIs
- Eclipse IoT Stack, Sense, ThingWorx, EveryThing,
- Software (RIOT OS, Thingsquare Mist firmware, Eclipse IoT)

3a. Embedded Devices/M2M Communication Protocols

- CoAP, RESTful HTTP, MQTT, XMPP
- Communication (RFID, NFC, 6LowPAN, UWB, ZigBee, Bluetooth LE, Power-line Ethernet, LPWAN)

3b. Network Protocols

- ZigBee, IP, RPL, IPv4, IPv6, UDP
- WiFi, WiMax, 2G/3G/4G/5G)

4. Software Platforms

- Internetwork Cloud Platforms (Xively, Nimbits, TCS Connected Universe Platform, openHAB, AWS IoT, IBM BlueMix, CISCO IoT, IOx and Fog, EveryThng)

5a. Analyzing and Visualizing

- Analyzing data, streaming data, events streaming data
- Descriptive, Prescriptive and Predictive Analytics
- Data Visualization

5b. Analytics & Machine Learning

- Learning ability to learn continuously from data, and the ability to drive actions/Applications/Business Processes
- Machine learning algorithms, for example, GROK from Numenta Inc.

Design Principles and Needed Capabilities

The overall design objective of IoT architecture shall be to target a horizontal system of real-world services that are open, service-oriented, secure, and offer trust.

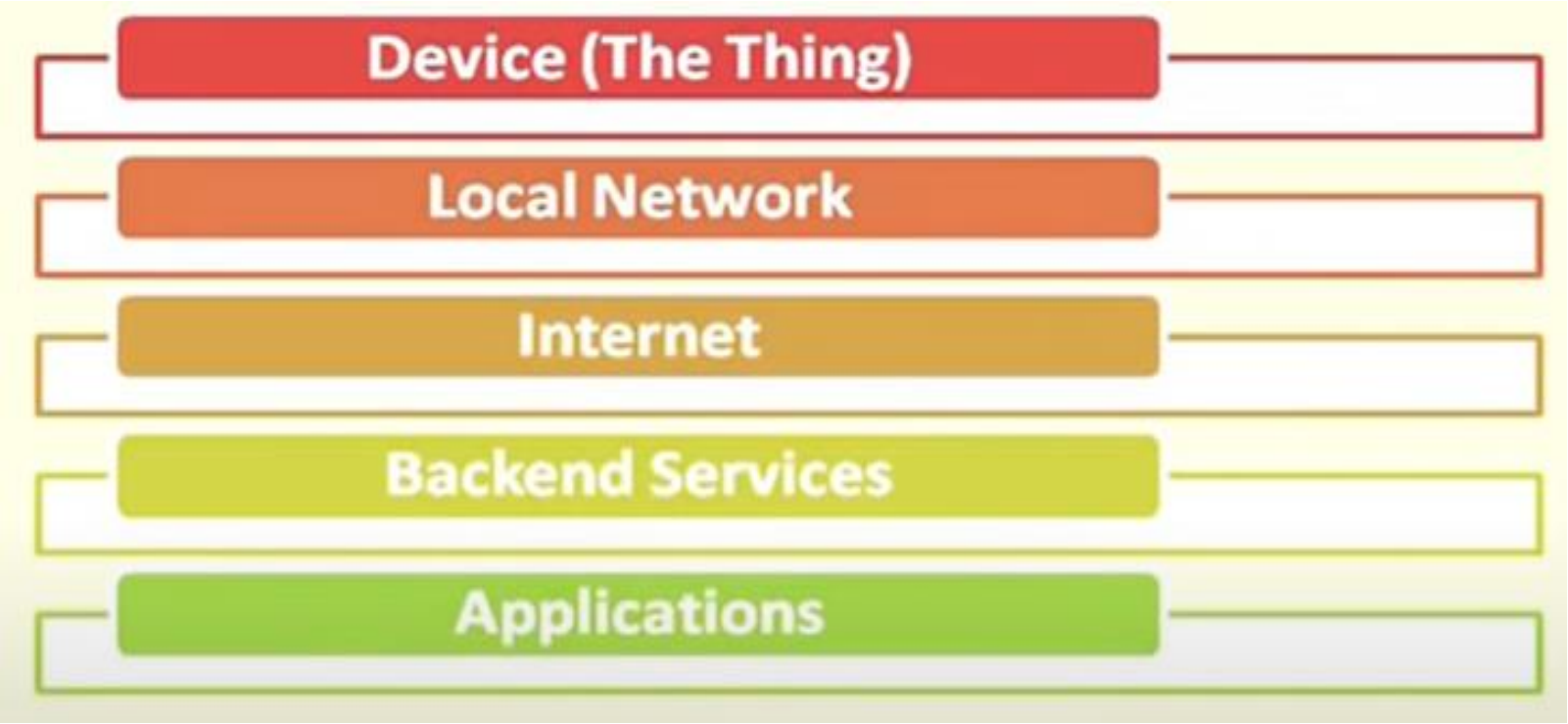
- Design for reuse of deployed IoT resources across application domains.
- Design for a set of support services that provide open service-oriented capabilities and can be used for application development and execution.
- Design for different abstraction levels that hide underlying complexities and heterogeneities.
- Design for sensing and actuators taking on different roles of providing and using services across different business domains and value chains.

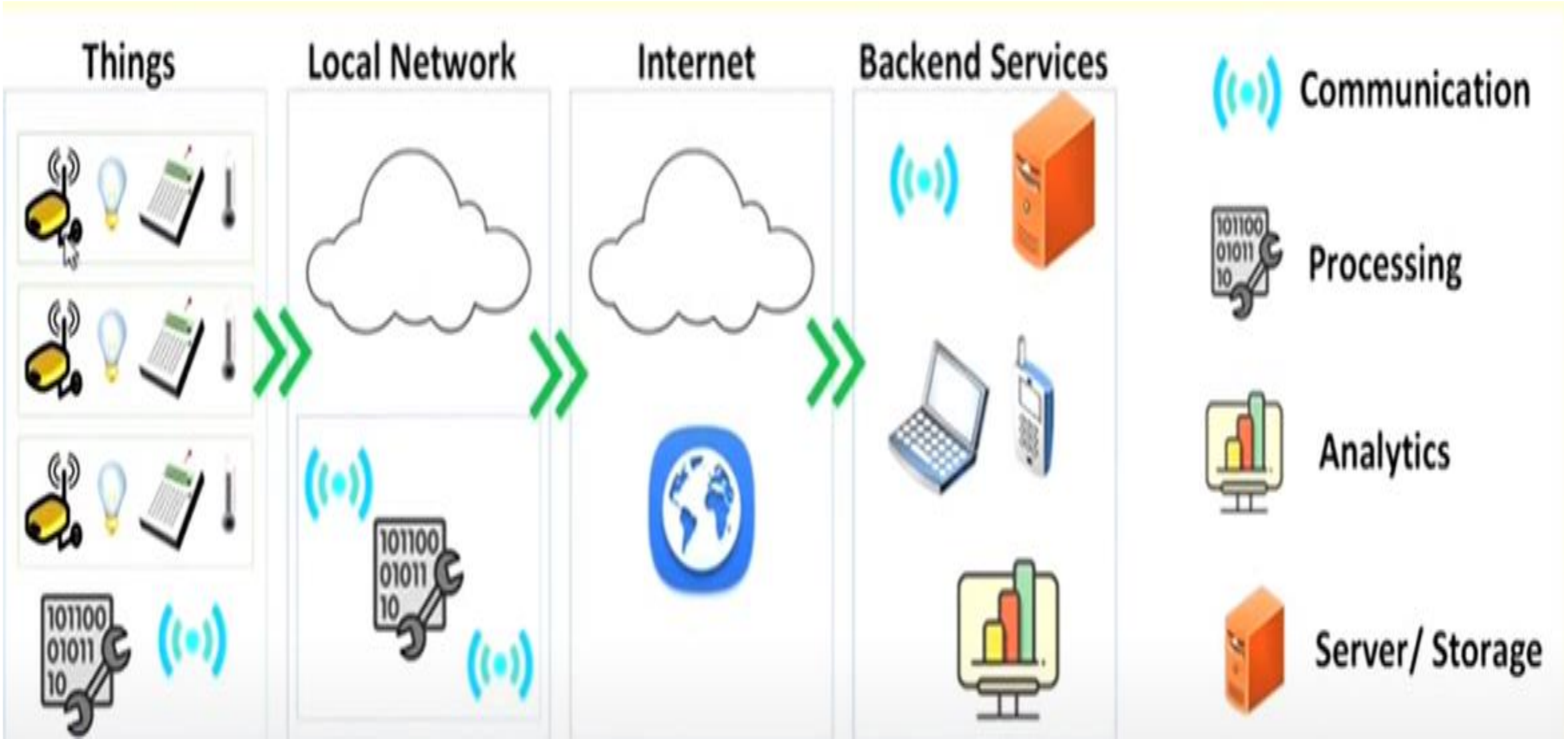
Design Principles and Needed Capabilities cntd…….

- Design for ensuring trust, security, and privacy.
- Design for scalability, performance, and effectiveness.
- Design for evolvability, heterogeneity, and simplicity of integration.
- Design for simplicity of management.
- Design for different service delivery models.
- Design for lifecycle support. The lifecycle phases are: planning, development, deployment, and execution. Management aspects include deployment efficiency, design time tools, and run-time management.

Basics of Networking

IoT Components:

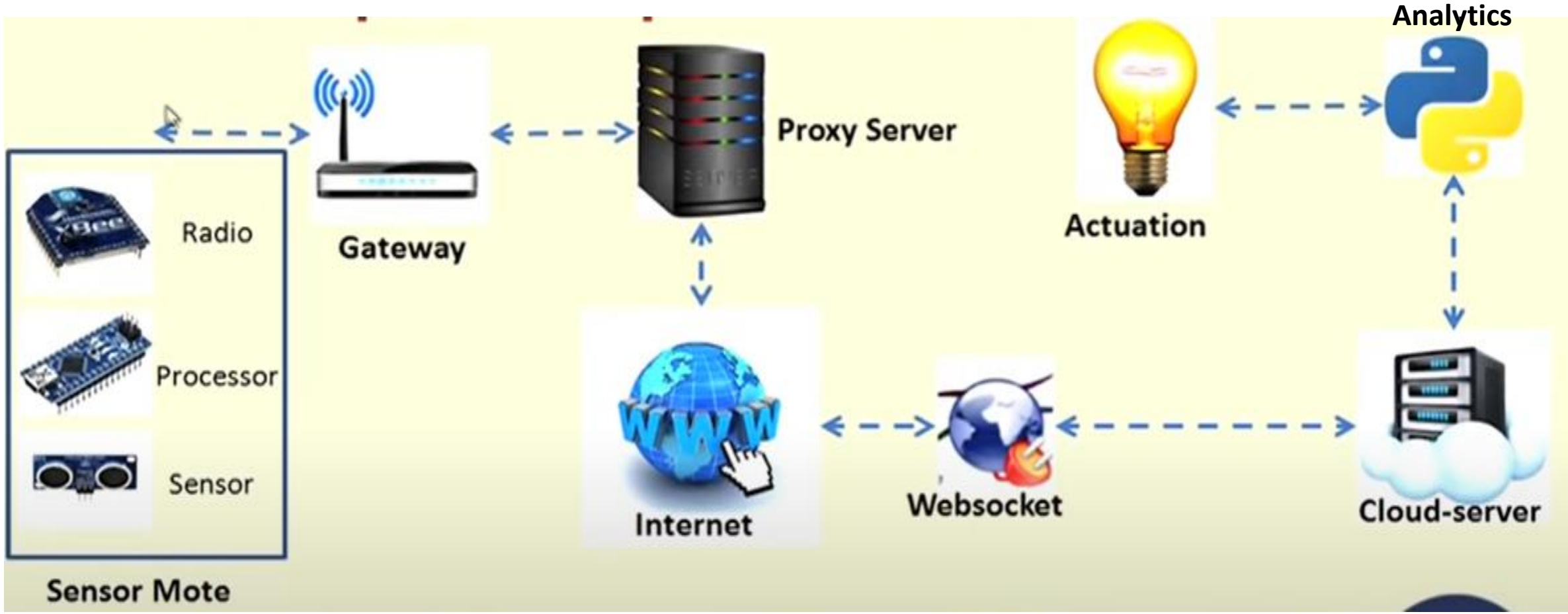



Things
Local Network
Internet
Backend Services
Communication
Processing
Analytics
Server/ Storage

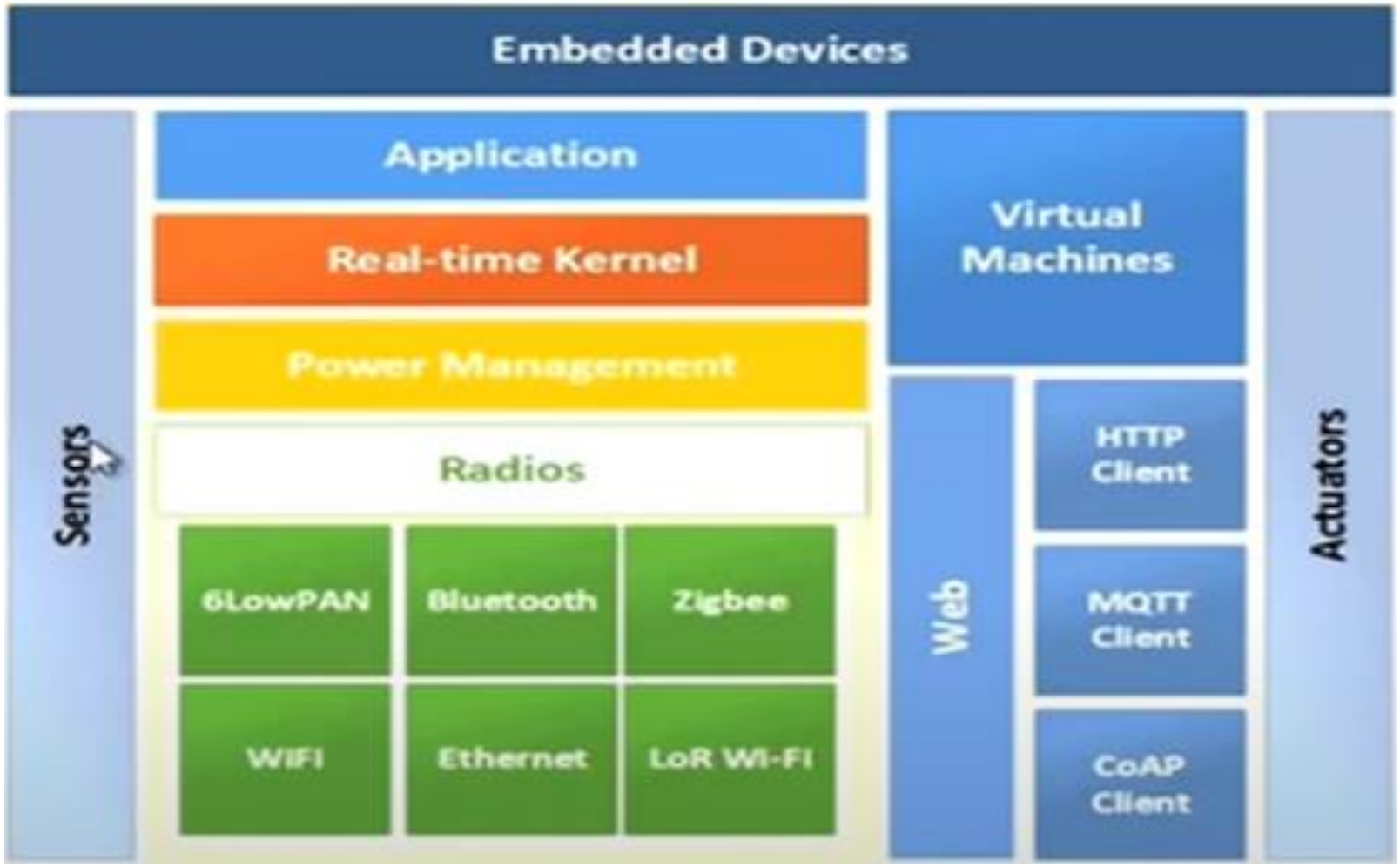
Functional components of IoT:

- Component for interaction and communication with other IoT devices
- Component for processing and analysis of operations.
- Component for internet interaction.
- Components for handling Web services of applications.
- Component to integrate application services.
- User interface to access IoT.

An Example IoT implementation:



IoT Interdependencies



IoT Categories

➢Industrial IoT

•IoT device connects to an IP network and the glot .

•Communication between the nodes done using regular as well as industry specific technologies.

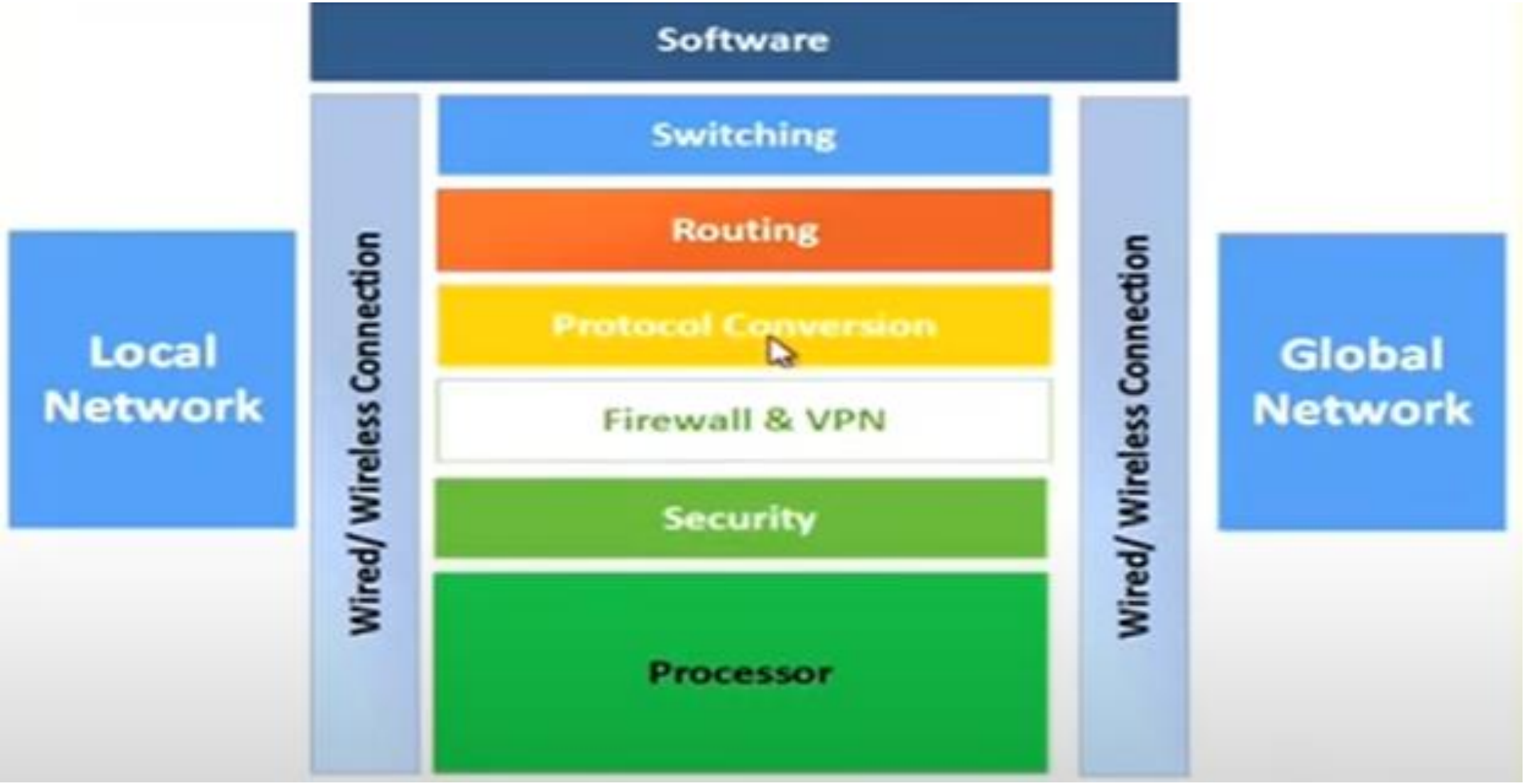
➢Consumer IoT

•IpT device communicates within the locally networked devices.

•Local communication is done mainly bluetooth, Zigbee or wifi.

•Generally limited to local communication by a Gateway.

IoT Gateways



Considerations:

- Communication between the IoT device(s) and the outside world dictates the network architecture.
- Choice of communication technology dictates the IoT device hardware requirements and costs
- Due to the presence of numerous applications of IoT enabled device, a single networking paradigm not suffiecient to address all the needs of the consumer or the IoT device

Complexity of networks

- Growth of networks
- Interference among devices
- Network management
- Heterogeneity in networks
- Protocol standardization within networks

Wireless networks

- Traffic and load management
- Variations in wireless networks-Wireless body Area networks and other personal area networks
- Interoperability
- Network management
- Overlay networks

Internet of Things– Conceptual Frameworks and Architecture

- Physical Object + Controller, Sensor and Actuators + Internet = Internet of Things … (1.1)
- Source: An equation given by Adrian McEwen and Hakim Cassimally, ‘Designing Internet of things’, Wiley, 2014

Another IoT Conceptual Architecture

- Gather + Enrich + Stream + Manage + Acquire + organize and Analyze = Internet of Things Enterprise & Business Applications, Integration … (1.2)
  [An Equation based on Oracle IoT Architecture in Fig. 1.5 of book]

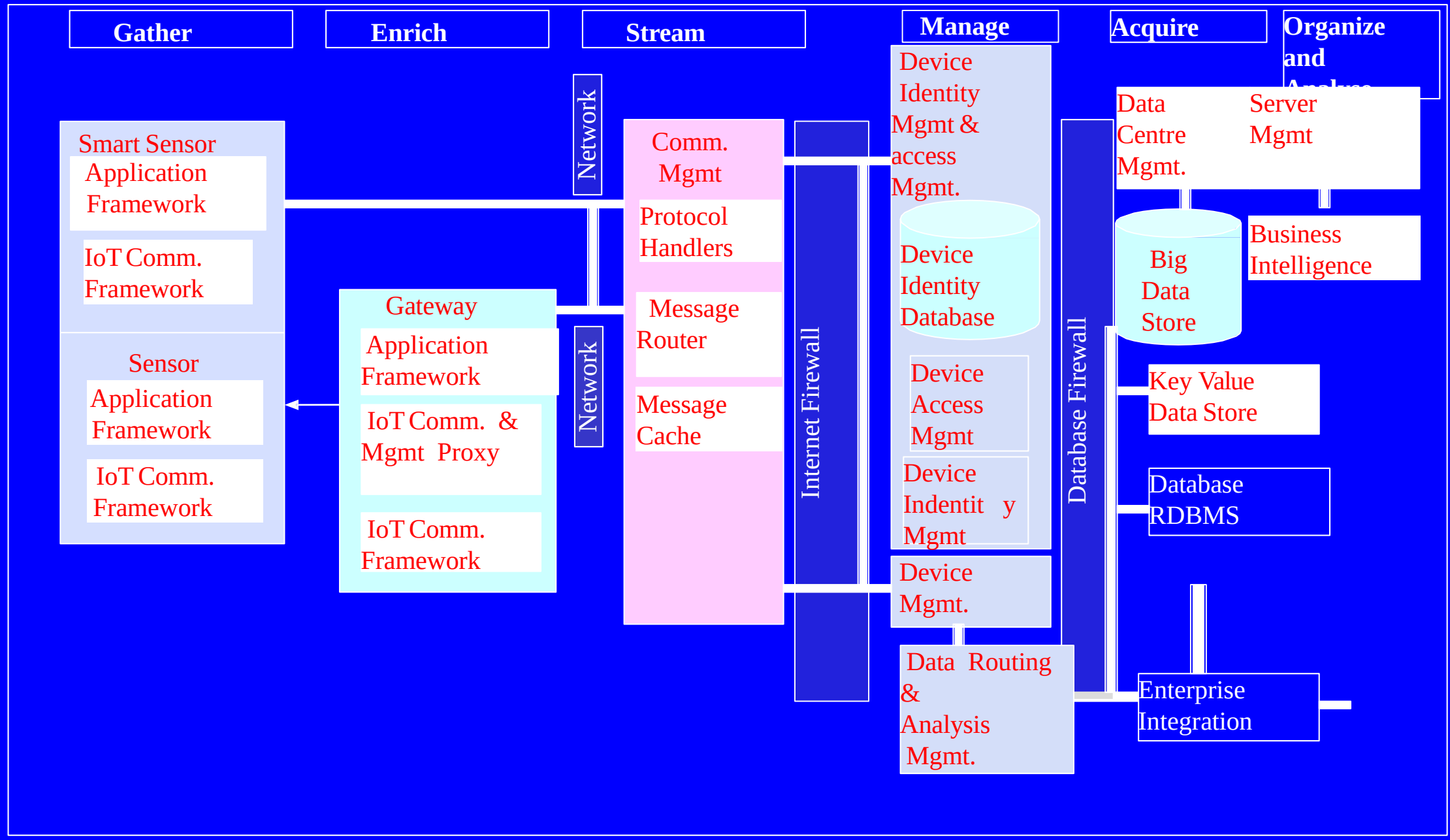
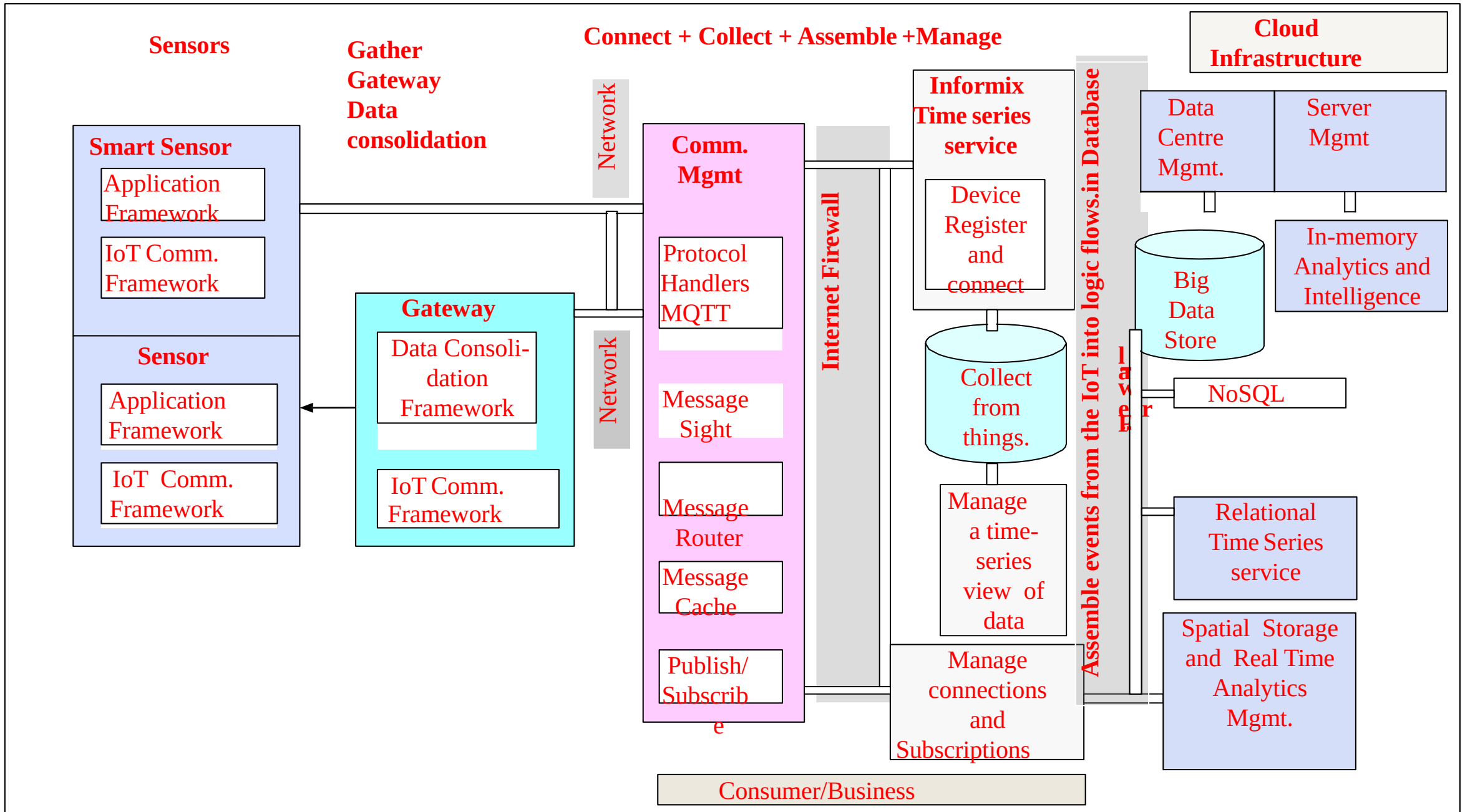
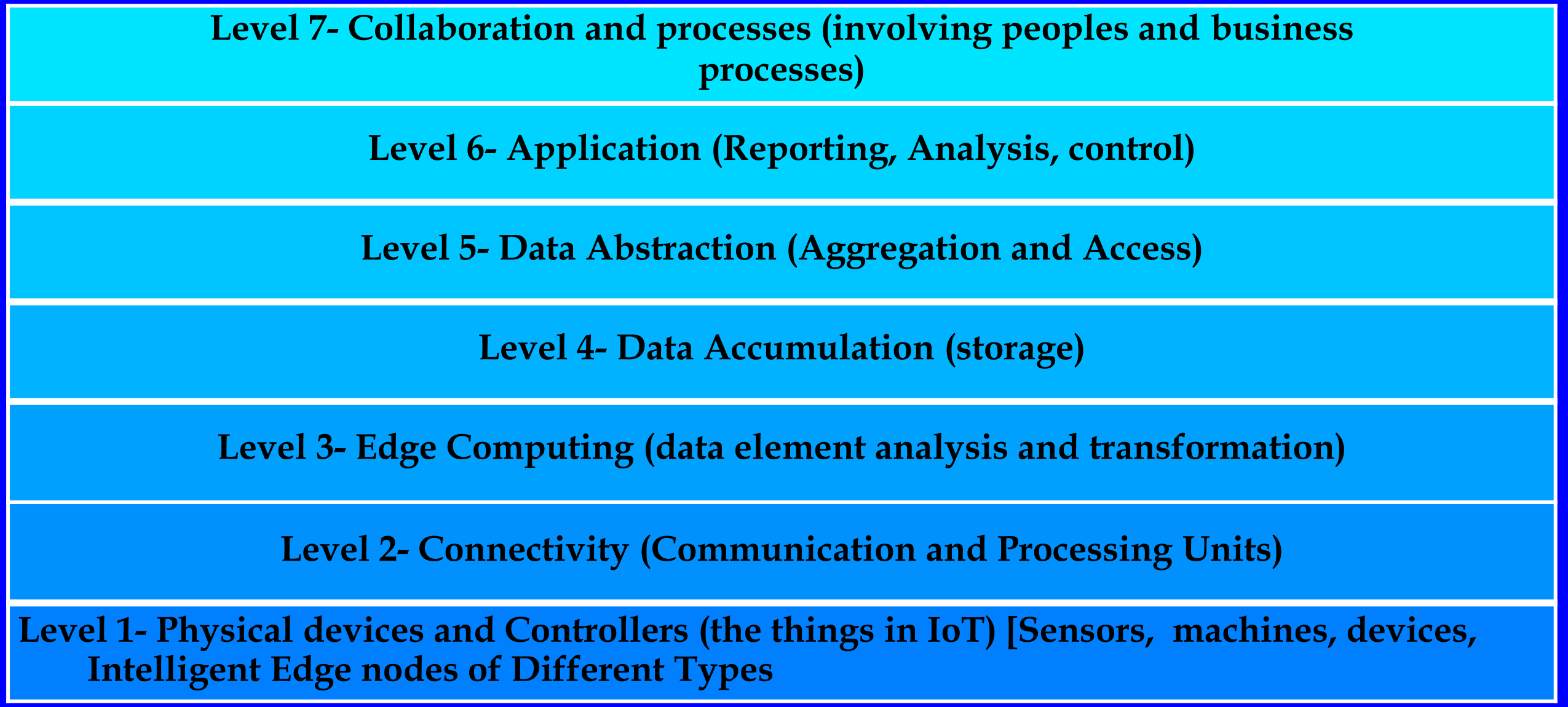


Figure 1.5 Oracle's IoT Architecture

Another IoT Conceptual Framework

- Gather + Consolidate + Connect + Collect + Assemble + Manage and Analyze = Internet of Things connected to Cloud Services … (1.3) [An Equation based on the IBM Framework.


Sensors
Gather
Gateway
Data
consolidation
Connect + Collect + Assemble +Manage
Cloud
Infrastructure
Smart Sensor
Application Framework
IoT Comm. Framework
Sensor
Application Framework
IoT Comm. Framework
Gateway
Data Consoli-dation Framework
IoT Comm. Framework
Network
Network
Comm. Mgmt
Protocol Handlers MQTT
Message Sight
Message Router
Message Cache
Publish/ Subscribe
Internet Firewall
Informix Time series service
Device Register and connect
Collect from things.
Manage a time-series view of data
Manage connections and Subscriptions
Assemble events from the IoT into logic flows.in Database
Data Centre Mgmt.
Server Mgmt
In-memory Analytics and Intelligence
Big Data Store
NoSQL
Relational Time Series service
Spatial Storage and Real Time Analytics Mgmt.
Consumer/Business



Ch01Fig. 1.4 An IOT reference model CISCO conceptual framework

Chapter 1: Introduction of IoT, Raj Kamal, et al.

Internet of Things Reference Model

Levels

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

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

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

4 **Data Accumulation**
(Storage)

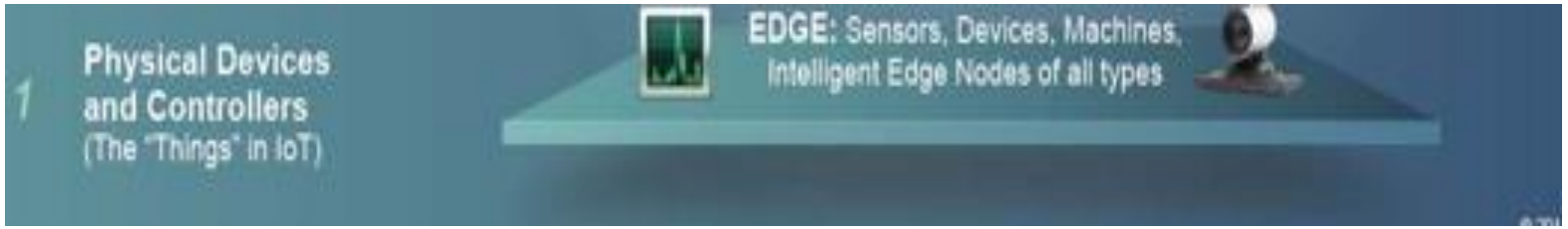
3 **Edge Computing**
(Data Element Analysis & Transformation)

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

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

IoT Reference Model Cntd…..

LAYER 1. Physical devices and controllers.



- They are the **physical devices, also called as "THINGS" in IOT .**
- Basically they are **Embedded Devices, Embedded hardware/software like** Sensors/Actuators , RFID, Hardware (Arduino, Raspberry Pi, Intel Edison, Beagle Bone Black and Wireless SoC…).
- They are **ready to send and receive the information.**
- Devices are **unlimited, diverse and no rules about the size, location etc….**
- Devices are capable of **Analog to digital conversion and vice versa.**

LAYER 2. Connectivity (Communication and processing units) Processing Units:

Processing Units:

- Contains **Routers and Gateways**
- Main task is to deliver the right information at right time and to right machine i.e. reliable transmission.

Communication:

- Includes **protocol handlers, message routers, message cache**
- It can be between smart device and network/ internet directly
- It can be through gateways then to network
- **Therefore main task involves switching and routing, enriching, transcoding, translation between protocols, security and self learning etc.**
- **Communication occurs networks –EAST-WEST communication**

Layer 3 [Edge Computing Or Fog Computing]

- Edge computing is an architecture that uses **edge devices / network edge like routers, gateways, switches, multiplexers, integrated access devices to do some preprocessing of data.**

- **Preprocessing includes data aggregation, storage, data filtering, cleanup, analysis, transformation (formatting, decoding, distillation) , Threshold(alert), event generation etc.**

- Finally the data is routed to web servers/cloud.

Layer 4 [Data Accumulation and storage]

Data management is done at backend server/cloud or data base centers

Main roles of layer 4 are:

- Convert data in motion to data at rest.
- Convert format from network packets to database relational tables.
- Convert Event based data to query based data (it bridges the gap between real time networking and non real time)
- The concept of BIG DATA is used at layer 4.

Layer 5 Data Abstraction

Data abstraction is done at backend server/cloud or data base centres

Abstraction **means providing the essential and relevant information of the data by hiding the irrelevant one.**

Main roles are:

1)Provide multiple storage systems to accommodate data from different IOT devices.

2)Reconciling multiple data format from different sources.

3)Combining data from multiple sources and simplifying the application i.e consolidating the data into one place.

4)Filtering, selecting, projecting and reformatting the data to serve client application.

5)Protecting the data with appropriate authentication and authorization.

Layer 6 Application

- Layer 6 deals with reporting, analysis and control
- i.e. the data is analyzed and then send to controlling device like actuator.
- And then the data is passed to specific application like mobile application or webpage or to the business enterprise which require that data.

Layer 7 Collaboration and processes.

- It means involving people and business process.
- Basically multiple people are using same applications for a range of different purpose
- But in IOT the main objective is to empower people to do their work better, not the application.

Architectural Overview

- An architecture can be described in several different views to capture specific properties that are of relevance to model, and the views chosen in are
- **Functional view (*Logical view):*** Description of what the system does, and its main functions.
- **Deployment view (*Physical view):*** Description of the main real-world components of the system such as devices, network routers, servers, etc.

Architectural Overview Cntd…

- **Process view (Behavioral view):** deals with the dynamic aspects of the system, explains the system processes and how they communicate, and focuses on the run time behavior of the system.
- **Implementation view (Development view):** Used to capture the architectural decisions made for the implementation.
- **Scenarios (use case diagram):** in which your system or application interacts with people, organizations, or external systems.

Design Principles and Needed Capabilities

The overall design objective of IoT architecture shall be to target a horizontal system of real-world services that are open, service-oriented, secure, and offer trust.

- Design for reuse of deployed IoT resources across application domains.
- Design for a set of support services that provide open service-oriented capabilities and can be used for application development and execution.
- Design for different abstraction levels that hide underlying complexities and heterogeneities.
- Design for sensing and actuators taking on different roles of providing and using services across different business domains and value chains.

Design Principles and Needed Capabilities cntd…….

- Design for ensuring trust, security, and privacy.
- Design for scalability, performance, and effectiveness.
- Design for evolvability, heterogeneity, and simplicity of integration.
- Design for simplicity of management.
- Design for different service delivery models.
- Design for lifecycle support. The lifecycle phases are: planning, development, deployment, and execution. Management aspects include deployment efficiency, design time tools, and run-time management.

M2M And IoT Technology Fundamentals

Devices and Gateways

Device:

- A device is a hardware unit that can sense aspects of it's environment and/or actuate, i.e. perform tasks in its environment.
- A device can be characterized as having several properties, including:
  - **Microcontroller**: 8-, 16-, or 32-bit working memory and storage.
  - **Power Source**: Fixed battery, energy harvesting, or hybrid.
  - **Sensors and Actuators:** Onboard sensors and actuators, or circuitry that allows them to be connected, sampled, conditioned, and controlled.
  - **Communication:** Cellular, wireless, or wired for LAN and WAN communication.

Types of devices

1. Basic Devices
2. Advanced Devices

Basic Devices

- Devices that only provide the basic services of sensor readings and/or actuation tasks, and in some cases limited support for user interaction.
- LAN communication is supported via wired or wireless technology, thus a gateway is needed to provide the WAN connection.

- These devices are often intended for a single purpose, such as measuring air pressure or closing a valve. I
- In some cases several functions are deployed on the same device, such as monitoring humidity, temperature, etc,..
- Another common goal is to enable battery as a power source, with a lifespan of a year and upwards by using ultra-low energy microcontrollers.

Advanced devices

- In this case the devices also host the application logic and a WAN connection. They may also feature device management and an execution environment for hosting multiple applications. Gateway devices are most likely to fall into this category.
- A powerful CPU or microcontroller with enough memory and storage to host advanced applications, such as a printer offering functions for copying, faxing, printing, and remote management.
- A more advanced user interface with, for example, display and advanced user input in the form of a keypad or touch screen.
- Video or other high bandwidth functions.

Gate ways:

- A gateway serves as a translator between different protocols, e.g. between IEEE 802.15.4 or IEEE 802.11, to Ethernet or cellular.
- There are many different types of gateways, which can work on different levels in the protocol layers.
- A gateway refers to a device that performs translation of the physical and link layer, but application layer gateways (ALGs) are also common.

- Some examples of ALGs include the ZigBee Gateway Device which translates from ZigBee to SOAP and IP, or gateways that translate from Constrained Application Protocol (CoAP) to Hyper Text Transfer Protocol/Representational State Transfer (HTTP/REST).
- The gateway device is also used for many other tasks, such as data management, device management, and local applications.

- Typical functions for **data management** include performing sensor readings and caching this data, as well as filtering, concentrating, and aggregating the data before transmitting it to back-end servers.
- **Device management** (DM) is an essential part of the IoT and provides efficient means to perform many of the management tasks for devices:
  - **Provisioning:** Initialization (or activation) of devices in regards to configuration and features to be enabled.
  - **Device Configuration:** Management of device settings and parameters.
  - **Software Upgrades:** Installation of firmware, system software, and applications on the device.

Local applications

- Examples of local applications that can be hosted on a gateway include closed loops, home alarm logic, and ventilation control, etc,..

DATA MANAGEMENT

Introduction

➢In the era of M2M, where billions of devices interact and generate data at exponential growth rates, data management is of critical importance as it sets the basis upon which any other processes can rely and operate

Some of the key characteristics of M2M data include:

- **Big Data:** Huge amounts of data are generated, capturing detailed aspects of the processes where devices are involved.
- **Heterogeneous Data:** The data is produced by a huge variety of devices and is itself highly heterogeneous, differing on sampling rate, quality of captured values, etc.

- Real-world data
- Real-time data
- Temporal data
- Spatial data
- Polymorphic data
- Proprietary data
- Security and privacy data aspects

Business Process in IoT

Introduction

- A business process refers to a series of activities, often a collection of interrelated processes in a logical sequence, within an enterprise, leading to a specific result.
- There are several types of business processes such as management, operational, and supporting, all of which aim at achieving a specific mission objective.
- As business processes usually span several systems and may get very complex, several methods and techniques have been developed for their modeling, such as the Business Process Model and Notation (BPMN), which graphically represents business processes in a business process model.

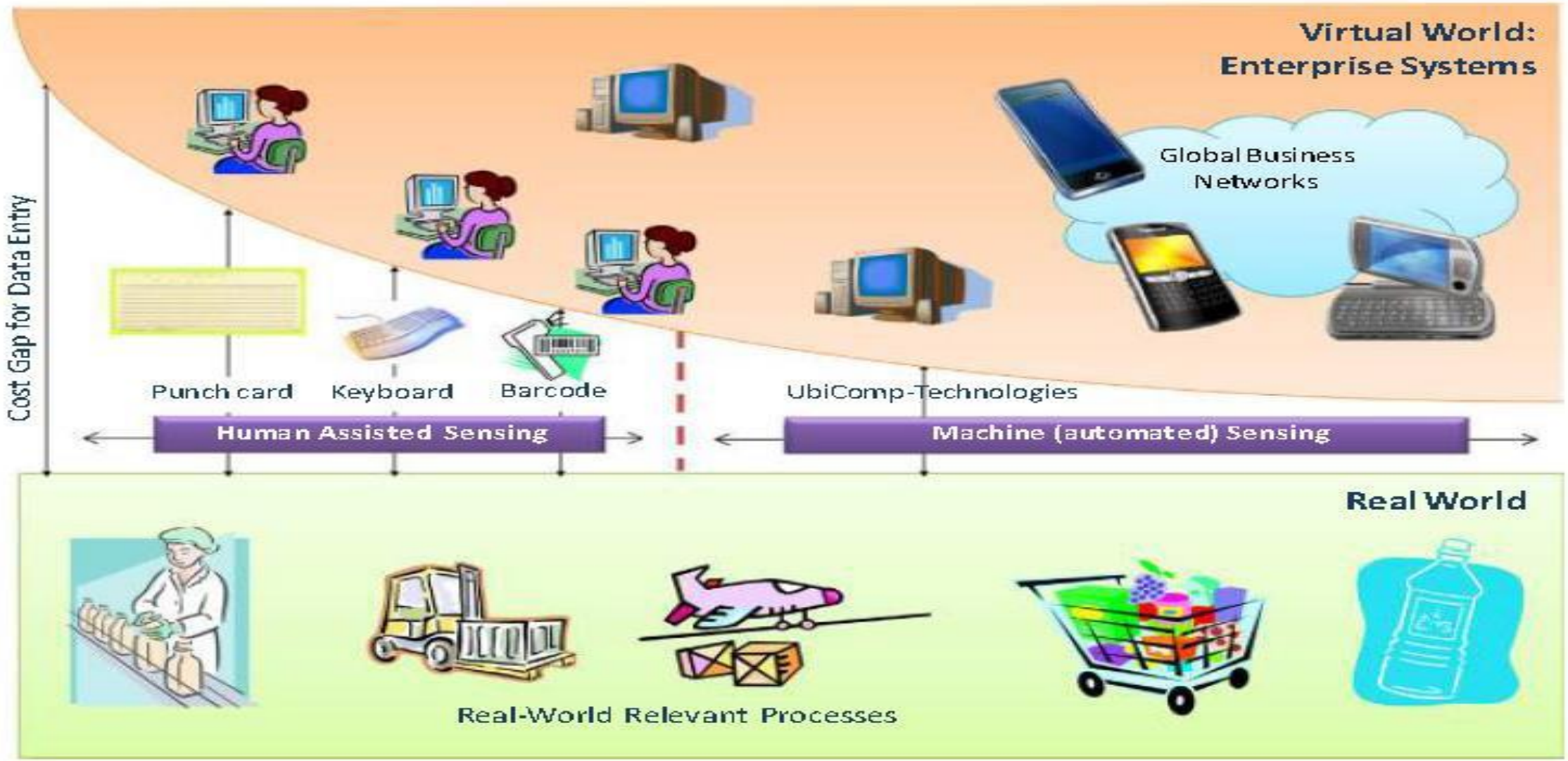


FIGURE 5.6

The decreasing cost of information exchange between the real-world and enterprise systems with the advancement of M2M.

IoT integration with enterprise systems

➢M2M communication and the vision of the IoT pose a new era where billions of devices will need to interact with each other and exchange information in order to fulfill their purpose.

In Figure, cross-layer interaction and cooperation can be pursued:

- At the M2M level, where the machines cooperate with each other (machine-focused interactions)
- At the machine-to-business (M2B) layer, where machines cooperate also with network-based services, business systems (business service focus), and applications.

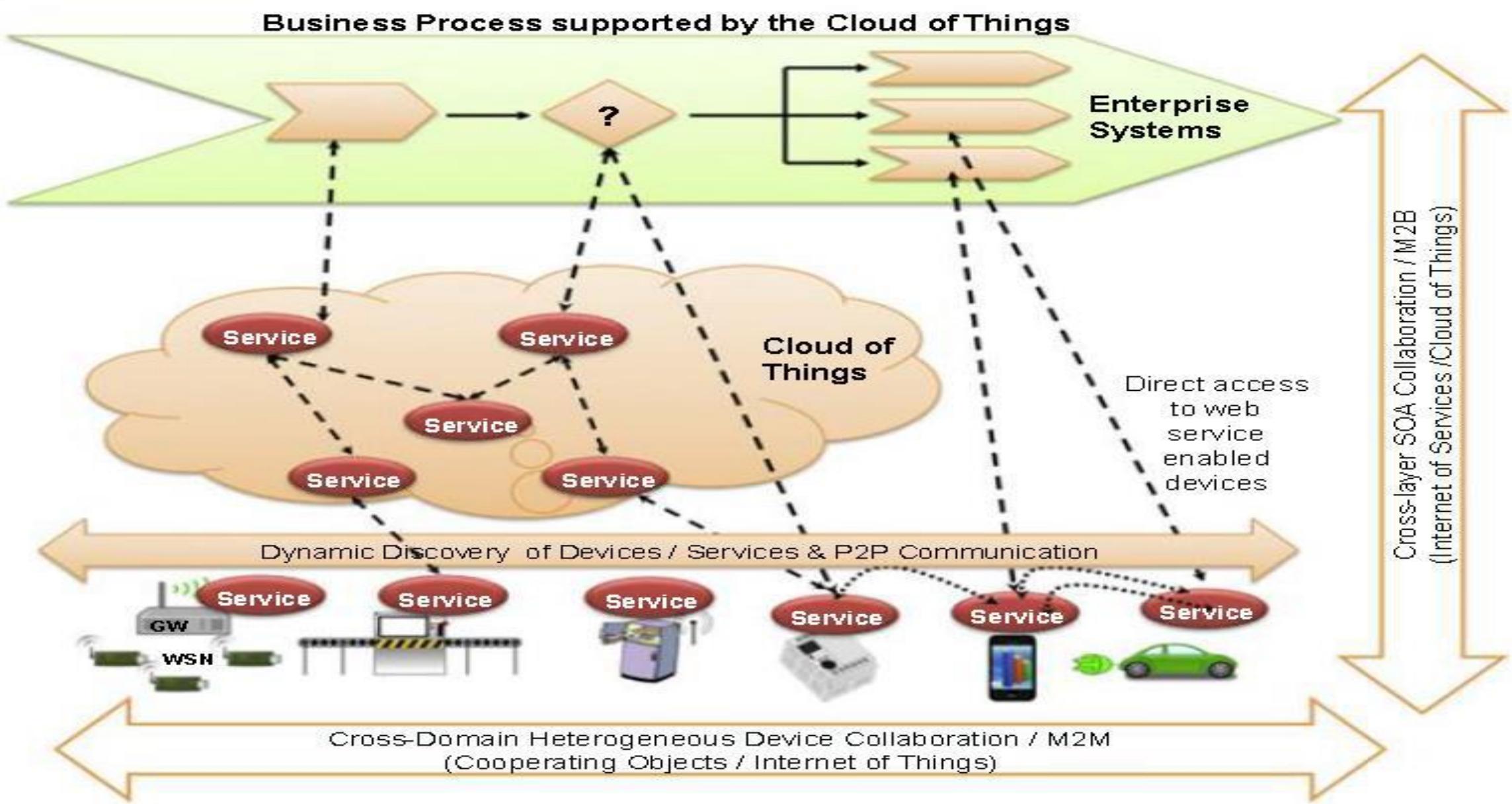


FIGURE 5.7

A collaborative infrastructure driven by M2M and M2B.

Distributed business processes in IoT

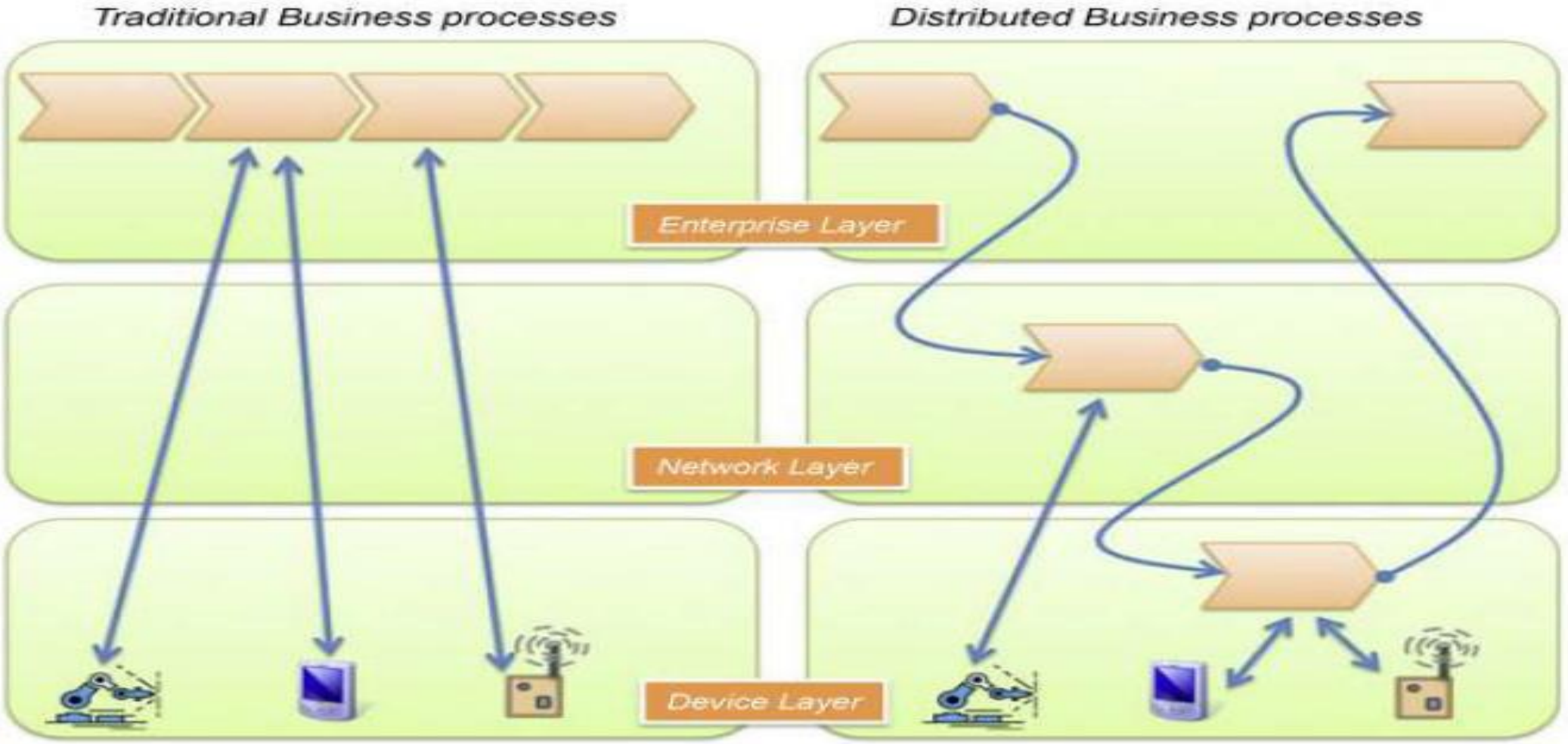


FIGURE 5.9

Distributed Business Processes in M2M era.

- The first step is to minimize communication with enterprise systems to only what is relevant for business.
- With the increase in resources (e.g. computational capabilities) in the network, and especially on the devices themselves (more memory, multi-core CPUs, etc.), it makes sense not to host the intelligence and the computation required for it only on the enterprise side, but actually distribute it on the network, and even on the edge nodes (i.e. the devices themselves), as depicted on the right side of Figure 5.9.

Everything As A Service(XaaS)

Cloud computing is a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be provisioned, configured, and made available with minimal management effort or service provider interaction.

- All applications need access to three things: compute, storage, and data processing capacities.
- With cloud computing, a fourth element is added _ distribution services _ i.e. the manner in which the data and computational capacity are linked together and coordinated.

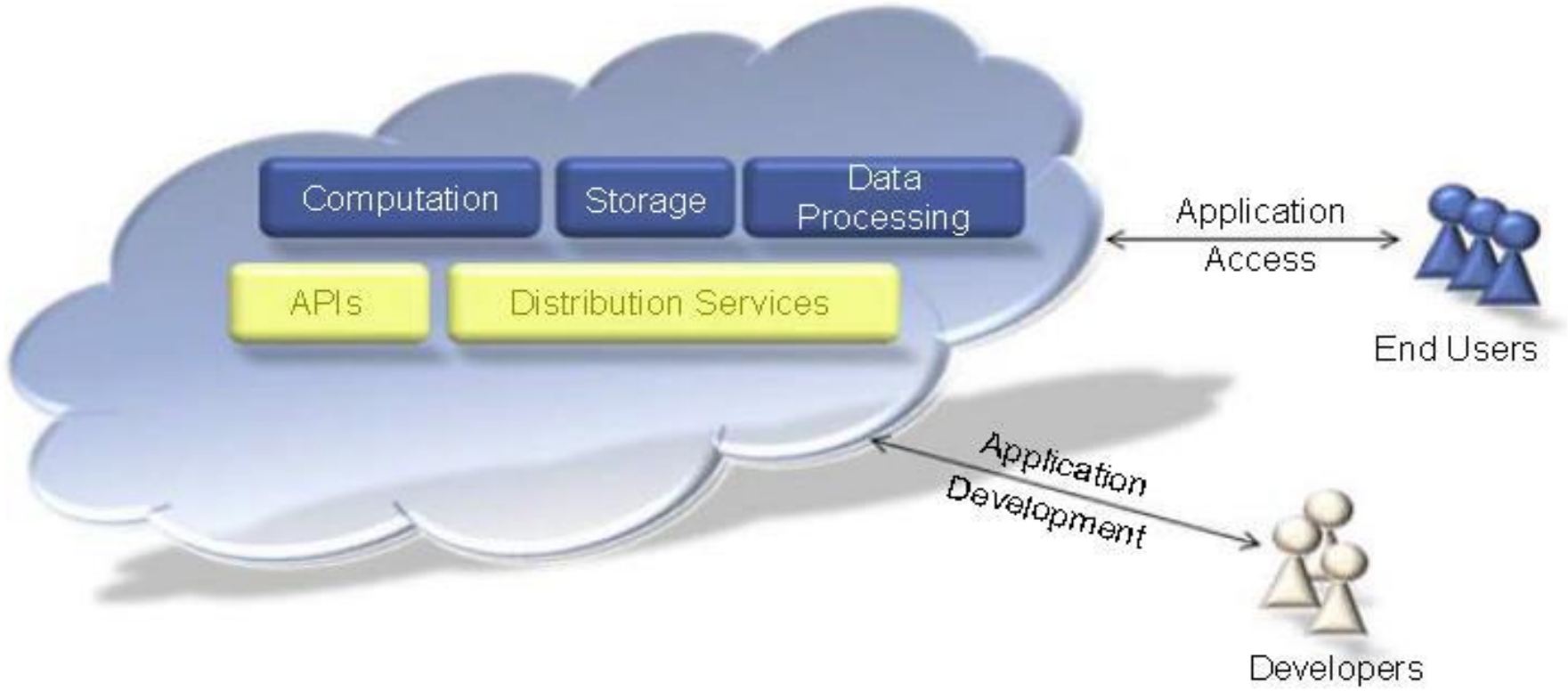


FIGURE 5.11

Conceptual Overview of Cloud Computing.

Characteristics of cloud computing

On-Demand Self-Service

- A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, or automatically, without requiring human interaction with each service provider.

Broad Network Access

- Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).

Resource Pooling

- The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- Examples of resources include storage, processing, memory, and network bandwidth.

Rapid Elasticity

- Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

Comparison of internet of things and cloud computing

- Cloud is a centralized system helping to transfer and deliver data and files to data centers over the Internet. A variety of data and programs are easy to access from a centralized cloud system.
- The Internet of Things refers to devices connected to the Internet. In the IoT, data is stored in real-time, as well as historical data. The IoT can analyze and instruct devices to make effective decisions, as well as track how certain actions function.

- Cloud computing encompasses the delivery of data to data centers over the Internet. IBM divides cloud computing into six different categories:

- **Software as a Service (SaaS)**

  In this case, applications run in the cloud and other companies operate devices that connect to users' computers through a web browser.

- **Platform as a Service (PaaS)**

  The cloud contains everything you need to build and deliver cloud applications so there is no need to maintain and buy equipment, software, etc.

- **Infrastructure as a Service (IaaS)**

  IaaS is an option providing companies with storage, servers, networks and hubs processing data for each use.

- **Public cloud**

Companies manage spaces and provide users with quick access through the public network.

- **Private cloud**

The same as a public cloud, but only one person has access here, which can be an organization, an individual company, or a user.

- **Hybrid cloud**

Based on a private cloud, but provides access to a public cloud.

The Role of Cloud Computing on the Internet of Things

- Cloud computing works to improve the efficiency of daily tasks in conjunction with the Internet of Things.
- Cloud computing is about providing a path for data to reach its destination while the Internet of Things generates a huge amount of data.

According to Amazon Web Services, there are some benefits of cloud computing

- No need to pre-guess infrastructure capacity needs
- Saves money, because you only need to pay for those resources that you use,

  the larger the scale, the more savings
- In a few minutes, platforms can be deployed around the world
- Flexibility and speed in providing resources to developers

Thus, the role of cloud computing in IoT is to work together to store IoT data, providing easy access when needed. It's important to note that cloud computing is an easy way to move large data packets across the Internet generated by the IoT.

Security aspects in IoT

Physical security

➢Physical security of IoT systems prevents unauthorized physical access to servers, storage, and network devices.

➢In IoT solutions, physical security also includes unauthorized access to IoT devices, for example, to redirect or manipulate data from devices, read credentials from devices or change a device's configuration.

Network security

➢Network security prevents unauthorized access to data transmitted over the network and tampering with or unauthorized modification of data. It also ensures that network services are available.

Unencrypted communications

- IoT platform allows old or low-power devices to connect to it over unencrypted protocols like HTTP since such devices are not capable of doing encryption or only provide weak encryption methods (e.g. TLSv1.0). Using old devices and unencrypted communications is discretionary and considering the risk that such communications are prone to attacks.
- Hence, it is recommended to use transport-level encryption (SSL/TLS) to protect all communications passing between the device and the platform.

Application security:

- Application security addresses security at the software level.
- IoT follows standard practices for application-level hardening as making sure that only properly upgraded operating systems and web servers are in use. A number of additional “best practices” are employed to make IoT secure by design.

Everything As A Service(XaaS)

Cloud computing is a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be provisioned, configured, and made available with minimal management effort or service provider interaction.

- All applications need access to three things: compute, storage, and data processing capacities.
- With cloud computing, a fourth element is added _ distribution services _ i.e. the manner in which the data and computational capacity are linked together and coordinated.

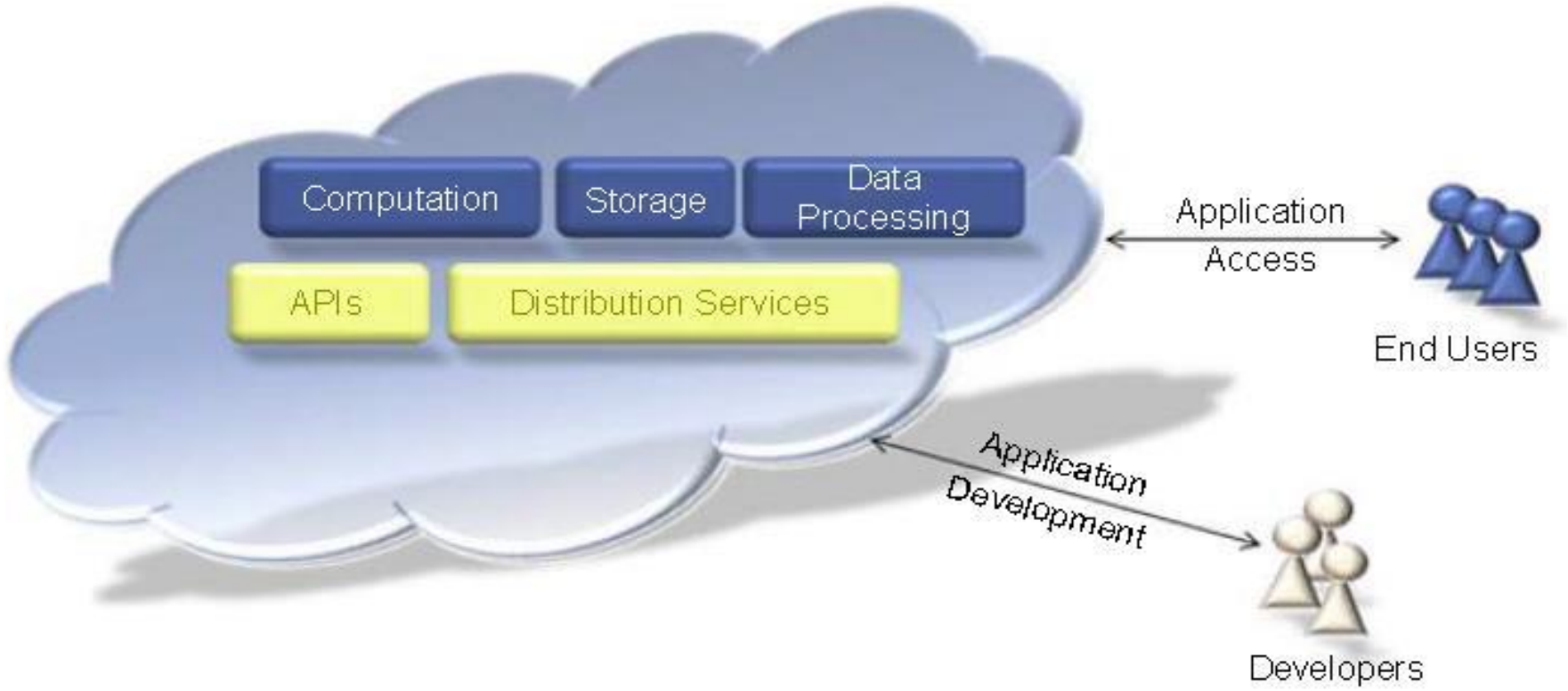


FIGURE 5.11

Conceptual Overview of Cloud Computing.

Characteristics of cloud computing

On-Demand Self-Service

- A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, or automatically, without requiring human interaction with each service provider.

Broad Network Access

- Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).

Resource Pooling

- The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- Examples of resources include storage, processing, memory, and network bandwidth.

Rapid Elasticity

- Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

Comparison of internet of things and cloud computing

- Cloud is a centralized system helping to transfer and deliver data and files to data centers over the Internet. A variety of data and programs are easy to access from a centralized cloud system.
- The Internet of Things refers to devices connected to the Internet. In the IoT, data is stored in real-time, as well as historical data. The IoT can analyze and instruct devices to make effective decisions, as well as track how certain actions function.

- Cloud computing encompasses the delivery of data to data centers over the Internet. IBM divides cloud computing into six different categories:

- **Software as a Service (SaaS)**

  In this case, applications run in the cloud and other companies operate devices that connect to users' computers through a web browser.

- **Platform as a Service (PaaS)**

  The cloud contains everything you need to build and deliver cloud applications so there is no need to maintain and buy equipment, software, etc.

- **Infrastructure as a Service (IaaS)**

  IaaS is an option providing companies with storage, servers, networks and hubs processing data for each use.

- **Public cloud**

Companies manage spaces and provide users with quick access through the public network.

- **Private cloud**

The same as a public cloud, but only one person has access here, which can be an organization, an individual company, or a user.

- **Hybrid cloud**

Based on a private cloud, but provides access to a public cloud.

The Role of Cloud Computing on the Internet of Things

- Cloud computing works to improve the efficiency of daily tasks in conjunction with the Internet of Things.
- Cloud computing is about providing a path for data to reach its destination while the Internet of Things generates a huge amount of data.

According to Amazon Web Services, there are some benefits of cloud computing

- No need to pre-guess infrastructure capacity needs
- Saves money, because you only need to pay for those resources that you use,

  the larger the scale, the more savings
- In a few minutes, platforms can be deployed around the world
- Flexibility and speed in providing resources to developers

Thus, the role of cloud computing in IoT is to work together to store IoT data, providing easy access when needed. It's important to note that cloud computing is an easy way to move large data packets across the Internet generated by the IoT.

Security aspects in IoT

Physical security

➢Physical security of IoT systems prevents unauthorized physical access to servers, storage, and network devices.

➢In IoT solutions, physical security also includes unauthorized access to IoT devices, for example, to redirect or manipulate data from devices, read credentials from devices or change a device's configuration.

Network security

➢Network security prevents unauthorized access to data transmitted over the network and tampering with or unauthorized modification of data. It also ensures that network services are available.

Unencrypted communications

- IoT platform allows old or low-power devices to connect to it over unencrypted protocols like HTTP since such devices are not capable of doing encryption or only provide weak encryption methods (e.g. TLSv1.0). Using old devices and unencrypted communications is discretionary and considering the risk that such communications are prone to attacks.
- Hence, it is recommended to use transport-level encryption (SSL/TLS) to protect all communications passing between the device and the platform.

Application security:

- Application security addresses security at the software level.
- IoT follows standard practices for application-level hardening as making sure that only properly upgraded operating systems and web servers are in use. A number of additional “best practices” are employed to make IoT secure by design.