UNIT 2 - FUNDAMENTAL MECHANISMS & KEY TECHNOLOGIES

Identification of IoT Objects and Services

There are various types of identifiers with different purposes and practicality.

Globally unique identifiers are highly desirable.

Identification codes can be classified as
(i) object IDs (OIDs) and
(ii) communication IDs.

Examples of the object IDs include but are not limited to radio frequency identification (RFID) / electronic product code (EPC), content ID, telephone number, and uniform resource identifier (URI) / uniform resource locator (URL);

Examples of the communication IDs include media access control (MAC) address, network layer/IP address, and session/protocol ID.

It is desirable and feasible for all objects to have a permanent unique identifier, an OID. It is also desirable as well as feasible for all end-point network locations and/or intermediary-point network locations to have a durable, unique network address (NAdr);

Every object then has a tuple (OID, NAdr) that is always unique, although the second entry of the tuple may change with time, location, or situation. However, there is a general trend toward object mobility, giving rise to a dynamic environment; hence, to retain maximal flexibility, it is best to separate, in principle, the OID from the NAdr and thus assign a general (OID, NAdr) tuple where the OID is completely invariant;

The basic requirement for an identification scheme is that it affords global uniqueness. Additionally, it is useful to have mechanisms for hierarchical grouping to deal with large populations. The aggregation feature of IPv6 address provides such hierarchical grouping. For a number of applications, there is a need to map/bind IP addresses (communications IDs) with other relevant OIDs. Additionally, modern layered communication architectures also require addressing and processing capabilities at several layers.

Object Naming

In addition to OID, there may be a need for object naming. Domain name system (DNS) is one example of a mechanism for Internet-based naming;

In the IoT context, some proponents have argued for the advantages of identifying information by name, not by node address.

DNS is used to map the "human-friendly" host names of computers to their corresponding "machine friendly" IP addresses. Hence, one is able, for example, to access the server (or large farm of servers) of CNN, Google, and so on, simply by the term www.cnn.com and so on.

To some large degree, **object name service (ONS)** will also be important in the IoT to map the "thing-friendly" names of object which may belong to heterogeneous name spaces (e.g., EPC, uCode, and any other self-defined code) on different networks (e.g., TCP/IP network) into their corresponding "machine-friendly" addresses or other related information of another TCP/IP network.

Web services

For some applications, especially where there is a need for simple end-user visibility of a small set of objects (i.e., where the objects are few and discretely identifiable – a home's thermostat, a home's refrigerator, a home's lighting system, a pet of the owner), the object may be identified through Web Services (WSs).

WSs provide standard infrastructure for data exchange between two different distributed applications. Lightweight WS protocols are of interest; for example, the representational state transfer (REST) interface may be useful in this context. REST is a software architecture for distributed systems to implement WSs. REST is gaining popularity compared with more classical protocols such as simple object access protocol (SOAP) and web services description language (WSDL) due to its relative simplicity.

Security and Privacy

Given the potential pervasive nature of IoT objects and IoT applications (e.g., grid control, home control, traffic control, and medical monitoring), security and privacy in communications and services become absolutely critical. Security needs to be intrinsically included in protocol development, and not just be a catch-up afterthought.

Strong authentication, encryption while transmitting, and also encryptions for data at rest is ideal; however, the computational requirements for encryption can be significant. Furthermore, at the central/authenticating site, rapid authentication support is desirable; otherwise objects would not be able to authenticate in large-population environments.

In some IoT applications, there is a need to know the precise physical location of objects; thus, the challenge is how to cost-effectively obtain location information; methods that rely on GPS or cellular services may be too expensive for some applications. In some cases, objects move independently; in other cases, the objects move as the one group. Different tracking methods may be required to achieve efficient handling of tracking information.

Capabilities for scalability are important in order to be able to support an IoT environment where there is a large population that is highly distributed. Solutions are necessary in the arena of distributed networking. Among the many issues driving this renewed interest are concerns about the scalability of the routing system. Proposals have been made recently based on the "locator/identifier separation."

Proponents of the separation architecture postulate that splitting these functions apart will yield several advantages, including improved scalability for the routing system. The separation aims to decouple locators and identifiers, thus allowing for efficient aggregation of the routing locator space and providing persistent identifiers in the identifier space. The locator/ID separationprotocol (LISP) IETF Working Group (WG) has completed the first set of experimental RFCs describing the LISP.

Structural aspects of IoT

Environment Characteristics

IoT/machineto- machine (M2M) nodes have noteworthy design constraints, such as but not limited to the following

- Low power (with the requirement that they will run potentially for years on batteries)
- Low cost (total device cost in single-digit dollars)
- Significantly more devices than in a LAN environment
- Severely limited code and RAM space
- Unobtrusive but very different user interface for configuration (e.g., using gestures or interactions involving the physical world)
- Requirement for simple wireless communication technology. In particular, the IEEE 802.15.4 standard is very promising for the lower (physical and link) layers.

Traffic Characteristics

The characteristics of IoT / M2M communication is different from other types of networks or applications. For example, cellular mobile networks are designed for human communication and communication is connection centric; it entails interactive communication between humans(voice, video), or data communication involving humans (web browsing, file downloads, and so on). Specifically, communication takes place with a certain length (sessions) and data volume;

On the other hand, in M2M the expectation is that there are many devices, there will be long idle intervals, transmission entails small messages, there may be relaxed delay requirements, and device energy efficiency is paramount.

Scalability

While some applications (e.g., smart grid, home automation, and so on) may start out covering a small geographic area or a small community of users, there invariably will be a desire over time for the service to expand.

When contemplating expansion, one wants to be able to build on previously deployed technology (systems, protocols), without having to scrap the system and start from scratch. Also, the efficiency of a larger system should be better than the efficiency of a smaller system. This is what is meant by scalability.

The goal is to make sure that capabilities such as addressing, communication, and service discovery, among others, are delivered efficiently in both small and large scale.

There is a need for enough name space to support increasing populations of devices and new applications.

Interoperability
Because of the plethora of applications, technology suppliers, and stakeholders, it is desirable to develop and/or re-use a core set of common standards. To the degree possible, existing standards may prove advantageous to a rapid and cost-effective deployment of the technology. Product and service interoperability is of interest.

Security and Privacy
When IoT relates to electric power distribution, goods distribution, transport and traffic management, e-health, and other key applications, as noted earlier, it is critical to maintain system-wide confidentiality, identity integrity, and trustworthiness.

Open Architecture
The goal is to support a wide range of applications using a common infrastructure, preferably based on a service-oriented architecture (SOA) over an open service platform, and utilizing overly networks.
In an SOA environment, objects expose their functionalities using a protocol such as SOAP or REST application programming interface (API). These devices may provide their functionality as a WS that can in turn be used by other entities.

Key IoT Technologies

The following are some key technologies

- Device Intelligence,
- Communication Capabilities,
- Mobility Support,
- Device Power,
- Sensor Technology,
- RFID Technology,
- Satellite Technology

Device Intelligence
A key consideration relates to on-board intelligence. In order for the IoT to become a reality, the objects should be able to intelligently sense and interact with the environment, possibly store some passive or acquired data, and communicate with the world around them.

Object-to-gateway device communication, or even direct object to- object communication, is desirable. These intelligent capabilities are necessary to support the ubiquitous networking to provide seamlessly interconnection between humans and objects. Some have called this mode of communication Any Services, Any Time, Any Where, Any Devices, and Any Networks.

Communication Capabilities
To achieve ubiquitous connectivity human-to-object and object-to object communications, networking capabilities will need to be implemented in the objects ("things"). In particular, IP is considered to be key capability for IoT objects; furthermore, the entire TCP/IP Internet Suite is generally desirable.

Self-configuring capabilities, especially how an IoT device can establish its connectivity automatically without human intervention, are also of interest. IPv6 auto-configuration andmulti-homing features are useful in this context, particularly the scope-based IPv6 addressing features.

Mobility Support
Mobility-enabled architectures and protocols are required. Some objects move independently, while others will move as one of group. Therefore, according to the moving feature, different tracking methods are required. It is important to provide ubiquitous and seamless communication among objects while tracking the location of objects. Mobile IPv6 (MIPv6) offers several capabilities that can address this requirement.

Device Power
A key consideration relates to the powering of the "thing," especially for mobile devices or for devices that otherwise would not have intrinsic power. M2M/IoT applications are almost invariably constrained by the following factors: devices have ultra-low-power capabilities, devices must be of low cost, and devices generally must have small physical size and be light.

A number of devices operate with a small battery, while other devices use a self-energizing energy source, for example a small solar cell array. Yet other devises are passive (e.g., passive RFID) and, thus, need to derive energy indirectly from the environment, such as an intercepting electric/magnetic field.

Batteries are critical to all sorts of products including laptops, pads, smartphones, and IoT objects. The so-called "coin batteries," also known as "button batteries," are typical in many IoT applications.

Batteries convert chemical energy released in particular chemical reactions into electrical energy. Batteries have a positive and a negative electrode (the cathode and the anode), separated by an electrolyte. When the electrodes are connected to a closed circuit, a series of chemical reactions occurs such that at one end charged particles (ions) from the electrolyte flow to the anode, react, and free up electrons; at the other end, reactions at the cathode attract free electrons. Thus, electrons at the anode move to the cathode and the flow of electrons through the electric circuit creates an electric current—the electrolyte also prevents the electrons from taking the shortest direct path, instead forcing them through the attached circuit.

In rechargeable batteries, the reactions are reversible, with the ions and electrons flowing back in the opposite direction during charging. Batteries can be classified into primary and secondary systems.

Primary Battery
Primary batteries are disposable batteries, that is, batteries that cannot be recharged, and their conversion of chemical energy into electrical energy is irreversible.
The most common primary systems are alkaline, lithium, and metal/air batteries.

Secondary Battery
Secondary batteries can be recharged, and the electrode material is reconstituted using an electric charge, so that discharge process can be repeated a number of times during the lifecycle of the battery.
Among secondary batteries, lead acid, nickel/cadmium (NiCd), nickel/metal hybrid (NiMH), and lithium-ion (Liion)/lithium-polymer (Li-polymer) batteries dominate the market.

Rechargeable Liion batteries have an anode comprising carbon (e.g., graphite), a metal oxide cathode, and an electrolyte containing lithium salt. It is relatively easy to peel ions from lithium metal. The widespread deployment of this battery technology is due to the fact that the resulting batteries are lightweight, have a high energy density, hold their charge better than other batteries, and they do not suffer from the "memory effect," where batteries hold less and less charge over time if they are not drained and then recharged completely.

Recent Advancements in battery Technologies
Materials such as silicon and others are being studied as possible replacement of the graphite anodes in Liion batteries. Silicon is of interest because it is inexpensive, it is abundant, and, by weight, it can store 10 times more lithium ions than graphite; this implies that it could theoretically allow a 10-fold increase in performance.

Another approach is the fuel cell, Fuel cells convert chemical energy into electricity by converting the chemical energy from a fuel (e.g., alcohol) into electricity through a chemical reaction with oxygen. Fuel cells have a high energy density: hydrogen contains nearly 150 times the energy of an equivalent weight of lithium. However, to be practical, they need to be smalland have an easily rechargeable reservoir for fuel.

Micro-electromechanical system (MEMS) technology is being investigated for this purpose. MEMSs are miniaturized mechanical devices that are already used in solar cells and flat-screen TVs.

Some evolving technologies use small solar panels embedded in the screen of a smartphone or object; other systems may use kinetic devices that translate movement of objects into an electric current. Solar cells are an example of an energy harvester, but they are for low efficiency when converting ambient light into useful electrical energy. A 3 cm2 solar cell (dimensions similar to the common CR2032 coin cell) yields only 12 μW.

There are a number of factors that must be considered in selecting the most suitable battery for a particular application; key considerations include

- Operating voltage level
- Load current and profile

- Duty cycle—continuous or intermittent
- Service life
- Physical requirement
    - Size
    - Shape
    - Weight
- Environmental conditions
    - Temperature
    - Pressure
    - Humidity
    - Vibration
    - Shock
    - Pressure
- Safety and reliability
- Shelf life
- Maintenance and replacement
- Environmental impact and recycling capability
- Cost

Sensor Technology

A sensor network is an infrastructure comprising sensing (measuring), computing, and communication elements that gives the administrator the ability to instrument, observe, and react to events and phenomena in a specified environment.

Network(ed) sensor systems support a plethora of applications, not the least being Homeland Security. Typical applications include, but are not limited to, data collection, monitoring, surveillance, and medical telemetry.

There are four basic components in a sensor network:
(i) an assembly of distributed or localized sensors;
(ii) an interconnecting network (usually, but not always, wireless based);
(iii) a central point of information clustering; and
(iv) a set of computing resources at the central point (or beyond) to handle data correlation, event-trending, querying, and data mining. Because the interconnecting network is generally wireless, these systems are known as wireless sensor networks (WSNs).

Sensors, the things or objects in this discussion, are active devices that measure some variable of the natural or man-made environment (e.g., a building, an assembly line, an industrial assemblage). Sensors in a WSN have a variety of purposes, functions, and capabilities.

Sensors can be described as “smart” inexpensive devices equipped with multiple on-boardsensing elements: they are low cost, low power, untethered multifunctional nodes that arelogically homed to a central sink node. Sensors are typically internetworked via a series of multihop short-distance low power wireless links.

They typically utilize the Internet or some other network for long-haul delivery of information to

a point (or points) of final data aggregation and analysis. In general, within the "sensor field," WSNs employ contention-oriented random access channel sharing/transmission techniques that are now incorporated in the IEEE 802 family of standards;

A WSN consists of densely distributed nodes that support sensing, signal processing, embedded computing, and connectivity; sensors are logically linked by self-organizing means. Wireless sensors typically transmit information to collecting (monitoring) stations that aggregate some or all of the information.

WSNs have unique characteristics, such as, but not limited to, power constraints/limited battery life for the wireless sensors, redundant data, low duty cycle, and many-to-one flows.

Sensor Types Based on Size

Sensors span several orders of magnitude in physical size; they range from nanoscopic-scale devices to mesoscopic-scale devices at one end; and, from microscopic-scale devices to macroscopic-scale devices at the other end.

- Nanoscopic (also known as nanoscale) refers to objects or devices in the order of 1–100 nm in diameter;
- mesoscopic scale refers to objects between 100 and 10,000 nm in diameter;
- the microscopic scale ranges from 10 to 1000 microns; and
- the macroscopic scale is at the millimeter-to-meter range.

At the low end of the scale, one finds, among others, biological sensors, small passive microsensors (such as "smart dust"), and "lab-on-a-chip" assemblies.

At the other end of the scale, one finds platforms such as, but not limited to, identity tags, toll collection devices, controllable weather data collection sensors, bioterrorism sensors, radars, and undersea submarine traffic sensors based on sonars.

Sensors may be passive and/or be self-powered; further along in the power consumption chain, some sensors may require relatively low power from a battery. or line feed. At the high end of the power-consumption chain, some sensors may require very high power feeds (e.g., for radars).

Applications of sensors

Commercial market segments include the following:

- Industrial monitoring and control
- Commercial building and control
- Process control
- Home automation
- Wireless automated meter reading (AMR)/ LM
- Metropolitan operations (traffic, automatic tolls, fire, and so on)
- Homeland Security applications: chemical, biological, radiological, and nuclear wireless sensors
- Military sensors
- Environmental (land, air, sea)/agricultural wireless sensors

Challenges

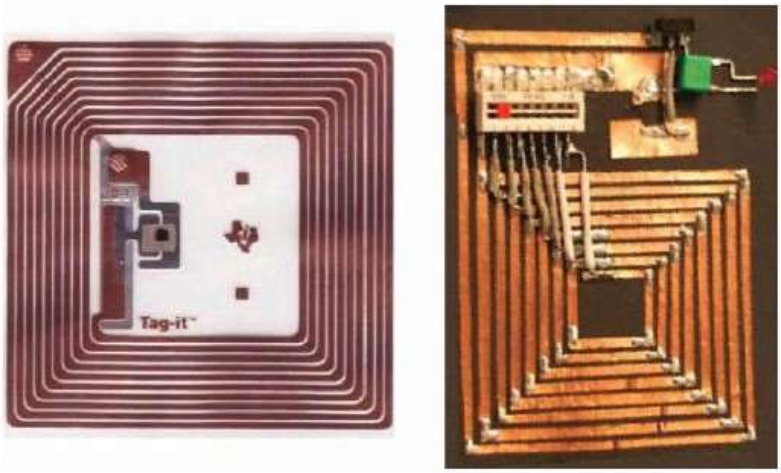
One of the challenges of WSNs is the need for extended temporal operation of the sensing node in spite of a (typically) limited power supply. In practical terms, this implies low power consumption for transmission over low bandwidth channels and low power-consumption logic topre-process and/or compress data. Energy-efficient wireless communications systems are being sought and are typical of WSNs. Low power consumption is a key factor in ensuring long operating horizons for non-power-fed systems.

Power efficiency in WSNs is generally accomplished in three ways:
(i) Low duty cycle operation
(ii) Local/in-network processing to reduce data volume (and, hence, transmission time)
(iii) Multihop networking (this reduces the requirement for long-range transmission since signal path loss is an inverse power with range/distance (e.g., 4)—each node in the sensor network can act as a repeater, thereby reducing the link range coverage required, and, in turn, the transmission power.

RFID Technology

RFIDs are electronic devices associated with objects ("things") that transmit their identity (usually a serial number) via radio links.

RFID tags are devices that typically have a read-only chip that stores a unique number but has no processing capability. RFID tags have broad applications, including the rapid collection of data in commercial environments.



Illustrative examples of RFIDs.

For example, RFID and bar coding are nearly ubiquitous in the inventory process, providing both accuracy and speed of data collection. These technologies facilitate the global supply chain and impact all subsystems within that overall process, including material requirement planning (MRP), just in time (JIT), electronic data interchange (EDI), and electronic commerce (EC).

RFIDs are also used in industrial environments, such as but not limited to dirty, wet, or harsh environments. The technology can also be used for identification of people or assets.

Contactless smart cards (SCs) are more sophisticated than RFID tags, being that they contain a microprocessor that enables
(i) on-board computing,
(ii) two-way communication including encryption, and
(iii) storage of predefined and newly acquired information.

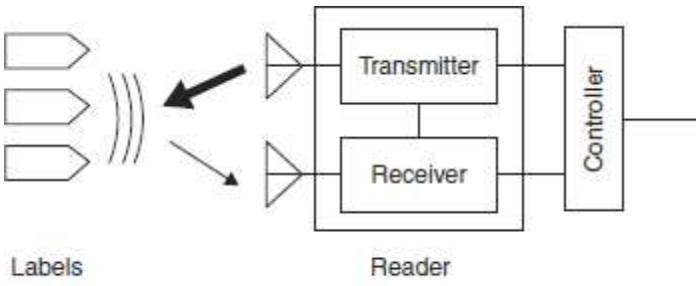


FIGURE 4.2 RFID reader operation.

RFID examples applicable to IoT include but are not limited to the following:

- Warehouse retailer automotive
- Grocery chain transportation
- Distribution center asset management
- Manufacturing
- Inventory management
- Warehousing and distribution
- Shop floor (production)
- Document tracking and asset management
- Industrial applications (e.g., time and attendance, shipping document tracking, receiving fixed assets)
- Retail applications

RFID Standards

There are a number of standards for RFIDs. Some of the key ones include the following:

Standard	Characteristics
ISO 14443	13.56 MHz frequency that embed a CPU; power consumption is about 10mW; data throughput is about 100 Kbps and the maximum working distance (from the reader) is around 10 cm.
ISO 15693	13.56 MHz frequency, but it enables working distances as high as 1 m, with a data throughput of a few Kbps.
ISO 18000	frequency such as 135 KHz, 13.56 MHz, 2.45 GHz, 5.8 GHz, 860–960 MHz, and 433 MHz. The ISO 18000–6 standard uses the 860–960MHz range and is the basis for the Class-1 Generation-2 UHF RFID, introduced by the EPCglobal Consortium.

RFID Layers

An RFID system is logically comprising several layers, as follows:

- the tag layer,
- the air interface (also called media interface) layer, and
- the reader layer;

additionally there are network, middleware, and application aspects. Some of the key aspects of the basic layers are as follows:

- Tag (device) layer: Architecture and EPCglobal Gen2 tag finite state machine
- Media interface layer: Frequency bands, antennas, read range, modulation, encoding, data rates
- Reader layer: Architecture, antenna configurations, Gen2 sessions, Gen2

Basic RFID Concept

Concept	Definition
Air interface	The complete communication link between an interrogator and a tag including the physical layer, collision arbitration algorithm, command and response structure, and data-coding methodology
Continuous wave (CW)	Typically a sinusoid at a given frequency, but more generally any interrogator waveform suitable for powering a passive tag without amplitude and/or phase modulation of sufficient magnitude to be interpreted by a tag as transmitted data
Cover-coding	A method by which an interrogator obscures information that it is transmitting to a tag. To cover-code data or a password, an interrogator first requests a random number from the tag.
EPC	EPC A unique identifier for a physical object, unit load, location, or other identifiable entity playing a role in business operations. EPCs are assigned following rules designed to ensure uniqueness despite decentralized administration of code space, and to accommodate legacy coding schemes in common use.
EPCglobal architecture framework	A collection of interrelated standards (“EPCglobal Standards”), together with services operated by EPCglobal, its delegates, and others (“EPC Network Services”), all in service of a common goal of enhancing business flows and computer applications through the use of EPCs
Interrogator	A device that modulates/transmits and receives/demodulates a sufficient set of the electrical signals defined in the signaling layer to communicate with conformant tags, while conforming to all local radio regulations. A typical interrogator is a passive-backscatter, interrogator-talks-first (ITF), RFID system operating in the 860–960 MHz frequency range.
Operating environment	A region within which an interrogator’s RF transmissions are attenuated by less than 90dB. In free space, the operating environment is a sphere whose radius is approximately 1000 m, with the interrogator located at the center. Ina building or other enclosure, the size and shape of the operating environment depends on factors such as the material properties and shape of the building and may be less than 1000 m in certain directions and greater than 1000 m in other directions

Operating procedure	Collectively, the set of functions and commands used by an interrogator to identify and modify tags (also known as the tag-identification layer)
Passive tag (or passive label)	A tag (or label) whose transceiver is powered by the RF field
Physical layer	The data coding and modulation waveforms used in interrogator-to-tag and tag-to-interrogator signaling
Singulation	Identifying an individual tag in a multiple-tag environment
Slotted random anticollision	An anticollision algorithm where tags load a random (or pseudo-random) number into a slot counter, decrement this slot counter based on interrogator commands, and reply to the interrogator when their slot counter reaches zero
Tag air interface	As defined in ISO 19762–3, a conductor-free medium, usually air, between a transponder and a reader/interrogator through which data communication is achieved by means of a modulated inductive or propagated electromagnetic field
Tag identification layer	Collectively, the set of functions and commands used by an interrogator to identify and modify tags (also known as the operating procedure)

The EPCglobal Architecture Framework

The EPCglobal Architecture Framework is a collection of interrelated standards ("EPCglobal Standards"), together with services operated by EPCglobal, its delegates, and others ("EPC Network Services"), all in service of a common goal of enhancing business flows and computer applications through the use of EPCs. It describes the collection of interrelated standards for hardware, software, and data interfaces, together with core services that are operated EPCglobal and its delegates, all in service of a common goal of enhancing the supply chain through the use of EPCs.

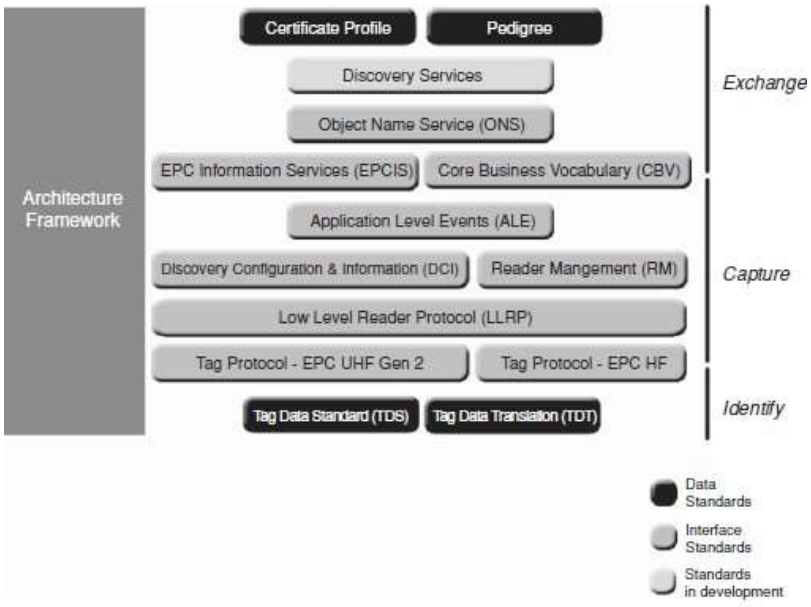
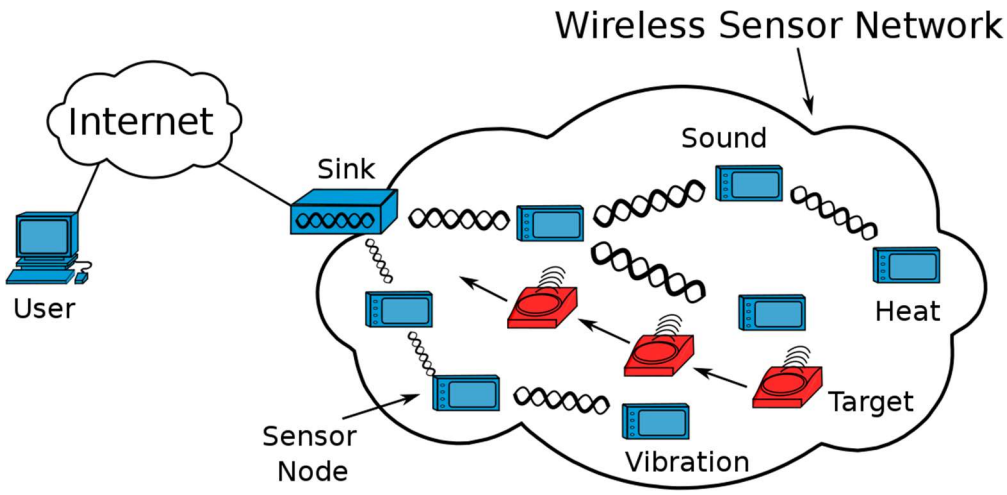


FIGURE 4.4 Standards that comprise the EPCglobal environment.

IoT Enabling Technologies

Wireless Sensors Networks

- Wireless sensor network (WSN) comprise of distributed devices with the sensor which are used to monitor the environmental and physical conditions. A WSN consists of a number of end nodes and routers and a coordinator.
- End nodes have several sensors attached to them. End node can also act as a routers.
- Routers are responsible for routing the data packet from end nodes to the coordinator.
- A sink or base station acts like an interface between users and the network.
- The coordinator node collect the data from all the notes coordinator also act as a Gateway that connects the WSN to the internet.
- WSNs can measure environmental conditions such as temperature, sound, pollution levels, humidity and wind.



Constraints of WSN

Limited processing speed, storage capacity, and communication bandwidth

There are a lot of challenges placed by the deployment of sensor networks which are a superset of those found in wireless ad hoc networks. Sensor nodes communicate over wireless, lossy lines with no infrastructure. An additional challenge is related to the limited, usually non-renewable energy supply of the sensor nodes. In order to maximize the lifetime of the network, theprotocols need to be designed from the beginning with the objective of efficient management of the energy resources

Scalability: Sensor networks vary in scale from several nodes to potentially several hundred thousand. In addition, the deployment density is also variable. For collecting high-resolution data, the node density might reach the level where a node has several thousand neighbours in their transmission range.

Production Costs: Because many deployment models consider the sensor nodes to be disposable

devices, sensor networks can compete with traditional information gathering approaches only if the individual sensor nodes can be produced very cheaply. The target price envisioned for a sensor node should ideally be less than $1.

Hardware Constraints: At minimum, every sensor node needs to have a sensing unit, a processing unit, a transmission unit, and a power supply. Optionally, the nodes may have several built-in sensors or additional devices such as a localization system to enable location-aware routing. However, every additional functionality comes with additional cost and increases the power consumption and physical size of the node. Thus, additional functionality needs to be always balanced against cost and low-power requirements.

Sensor Network Topology: Although WSNs have evolved in many aspects, they continue to be networks with constrained resources in terms of energy, computing power, memory, and communications capabilities. Of these constraints, energy consumption is of paramount importance, which is demonstrated by the large number of algorithms, techniques, and protocols that have been developed to save energy, and thereby extend the lifetime of the network.Topology Maintenance is one of the most important issues researched to reduce energy consumption in wireless sensor networks.

Transmission Media: The communication between the nodes is normally implemented using radio communication over the popular ISM bands. However, some sensor networks use opticalor infrared communication, with the latter having the advantage of being robust and virtually interference free.

Power Consumption: As we have already seen, many of the challenges of sensor networks revolve around the limited power resources. The size of the nodes limits the size of the battery. The software and hardware design needs to carefully consider the issues of efficient energy use. For instance, data compression might reduce the amount of energy used for radio transmission, but uses additional energy for computation and/or filtering. The energy policy also depends on the application; in some applications, it might be acceptable to turn off a subset of nodes in orderto conserve energy while other applications require all nodes operating simultaneously.

Applications of WSN

- Military applications
- Transportation (Traffic analysis)
- Health applications
- Environmental Applications
- Air pollution monitoring
- Forest fires detection
- Greenhouse monitoring
- Landslide detection
- Structural monitoring
- Industrial monitoring
- Agricultural sector

Cloud Computing

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and system software in the datacenters that provide those services.

The National Institute of Standards and Technology (NIST) characterizes cloud computing as Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- Cloud computing is based on the concept of dynamic provisioning, which is applied not only to services but also to compute capability, storage, networking, and information technology(IT) infrastructure in general.
- Resources are made available through the Internet and offered on a pay-per-use basis from cloud computing vendors.
- Cloud computing allows renting infrastructure, runtime environments, and services on a pay-per-use basis.

Cloud computing has been coined as an umbrella term to describe a category of sophisticated on-demand computing services initially offered by commercial providers, such as Amazon, Google, and Microsoft.

It denotes a model on which a computing infrastructure is viewed as a "cloud," from which businesses and individuals access applications from anywhere in the world on demand.

The main principle behind this model is offering computing, storage, and software "as a service.

A cloud should have:

- pay-per-use (no ongoing commitment, utility prices);
- elastic capacity and the illusion of infinite resources;
- self-service interface; and
- resources that are abstracted or virtualized.

Applications of Cloud

Cloud computing is helping enterprises, governments, public and private institutions, and research organizations shape more effective and demand-driven computing systems. Access to,as well as integration of, cloud computing resources and systems is now as easy as performing a credit card transaction over the Internet.

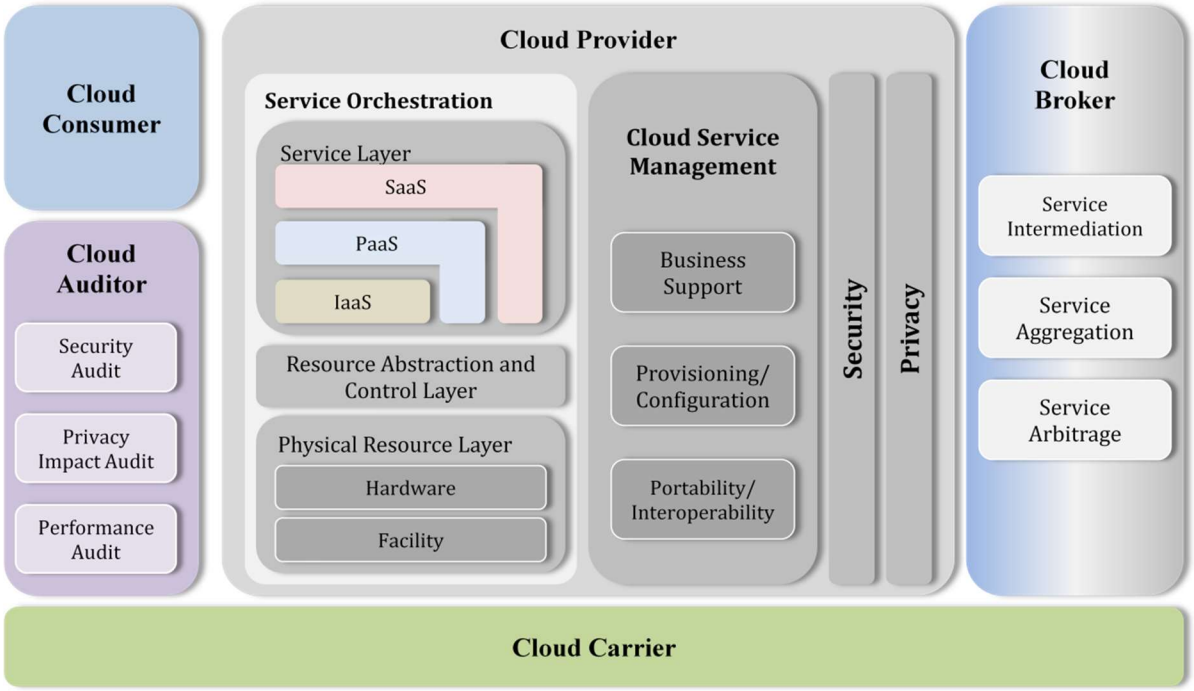
- Large enterprises can offload some of their activities to cloud-based systems. Recently, the New York Times has converted its digital library of past editions into a Web-friendly format.
- Small enterprises and start-ups can afford to translate their ideas into business results more quickly, without excessive up-front costs.

- System developers can concentrate on the business logic rather than dealing with the complexity of infrastructure management and scalability.
- End users can have their documents accessible from everywhere and any device.

The Conceptual Reference Model

NIST cloud computing reference architecture, which identifies the major actors, their activities and functions in cloud computing.

The diagram depicts a generic high-level architecture and is intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing.



The NIST cloud computing reference architecture defines five major actors:

- *cloud consumer,*
- *cloud provider,*
- *cloud carrier,*
- *cloud auditor* and
- *cloud broker*.

Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing.

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Table 1: Actors in Cloud Computing

Cloud Services

IaaS

- IaaS (Infrastructure as a Service): provides you the computing infrastructure, physical or (quite often) virtual machines and other resources like virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks etc.
- A cloud infrastructure enables on-demand provisioning of servers running several choices of operating systems and a customized software stack. Infrastructure services are considered to be the bottom layer of cloud computing systems
- This model allows users to use virtualized IT resources for computing, storage, and networking.
- In short, the service is performed by rented cloud infrastructure. The user can deploy and run his applications over his chosen OS environment.
- They deliver customizable infrastructure on demand.

PaaS

- Platform-as-a-Service (PaaS) solutions provide a development and deployment platform for running applications in the cloud. They constitute the middleware on top of which applications are built.
- In PaaS we can able to develop, deploy, and manage the execution of applications using provisioned resources demands a cloud platform with the proper software environment.
- Such a platform includes operating system and runtime library support.
- PaaS (Platform as a Service provides you computing platforms which typically includes operating system, programming language execution environment, database, web server etc.

SaaS

- Software-as-a-Service (SaaS) is a software delivery model that provides access to applications through the Internet as a Web-based service.
- It provides a means to free users from complex hard- ware and software management by offloading such tasks to third parties, which build applications accessible to multiple users through a Web browser.
- SaaS (Software as a Service) model you are provided with access to application software often referred to as "on-demand software".
- No need to worry about the installation, setup and running of the application. Service provider will do that for you. You just have to pay and use it through some client.
- On the provider side, the specific details and features of each customer's applica- tion are maintained in the infrastructure and made available on demand

Cloud Deployment Models

A cloud infrastructure may be operated in one of the following deployment models:

- public cloud,
- private cloud,
- community cloud, or
- hybrid cloud.

Public Cloud

- A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network. A public cloud is owned by an organization selling cloud services, and serves a diverse pool of clients.
- A public cloud is built over the Internet and can be accessed by any user who has paid for the service .
- In Public cloud, the services offered are made available to anyone, from anywhere, and at any time through the Internet.
- From a structural point of view public cloud is a distributed system, most likely composed of one or more datacenters connected together, on top of which the specific services offered by the cloud are implemented.
- Any customer can easily sign in with the cloud provider, enter her credential and billing details, and use the services offered.
- Public cloud offer solutions for minimizing IT infrastructure costs and serve as a viable option for handling peak loads on the local infrastructure.

Benefit of Public Cloud

- Public clouds promote standardization, preserve capital investment, and offer application flexibility.

Drawbacks

- In the case of public clouds, the provider is in control of the infrastructure and, eventually, of the customers' core logic and sensitive data.
- The risk of a breach in the security infrastructure of the provider could expose sensitive information to others.
- Public cloud service offering has low degree of control and physical and security aspects of the cloud.

Private Cloud

- A private cloud gives a single Cloud Consumers organization the exclusive access to and usage of the infrastructure and computational resources.
- In private cloud, the cloud infrastructure is operated solely for an organization.
- It may be managed either by the Cloud Consumer organization or by a third party, and may be hosted on the organizations premises
- Private clouds give local users a flexible and agile private infrastructure to run service workloads within their administrative domains.
- A private cloud is supposed to deliver more efficient and convenient cloud services. It may impact the cloud standardization, while retaining greater customization and organizational control.

Private cloud may exist off premises and can be managed by third party. Thus two private cloud scenarios exist, as follows,

On premises or On site Private Cloud

- Applies to private cloud implemented at a customer premises.

Outsourced Private Cloud

- Applies to private clouds where the server side is outsourced to a hosting company.

Key advantages of using a private cloud computing infrastructure

- Customer information protection.- In-house security is easier to maintain and rely on.
- Infrastructure ensuring SLAs.
- Compliance with standard procedures and operations.
- Private clouds attempt to achieve customization and offer higher efficiency, resiliency, security, and privacy.

Drawback

- From an architectural point of view, private clouds can be implemented on more heterogeneous hardware: They generally rely on the existing IT infrastructure already deployed on the private premises.
- Private clouds can provide in-house solutions for cloud computing, but if compared to public clouds they exhibit more limited capability to scale elastically on demand.

Hybrid and Community Cloud

- A hybrid cloud is a composition of two or more clouds (on-site private, on-site community, off-site private, off-site community or public) that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability.
- Hybrid clouds allow enterprises to exploit existing IT infrastructures, maintain sensitive information within the premises, and naturally grow and shrink by provisioning external resources and releasing them when they're no longer needed.
- Hybrid clouds address scalability issues by leveraging external resources for exceeding capacity demand.

Community Cloud

- A community cloud serves a group of Cloud Consumers which have shared concerns such as mission objectives, security, privacy and compliance policy, rather than serving a single organization as does a private cloud.

- A community cloud is "shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations)

Big data Analytics

What is big data?

Big data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.

Big data is a term applied to data sets whose size or type is beyond the ability of traditional relational databases to capture, manage and process the data with low latency.

Big data is larger, more complex data sets, especially from new data sources. These data sets are so voluminous that traditional data processing software just can't manage them.

SOURCES OF BIG DATA

This data comes from a wide variety of sources: sensors used to gather climate information, posts to social media sites, digital pictures and videos, purchase transaction records and cell phone GPS signals, to name a few.

Artificial intelligence (AI), Mobile, Social Media and the Internet of Things (IoT) are driving data complexity through new forms and sources of data.

For example, big data comes from Sensors, Devices, Video/Audio, Networks, Log files, Transactional applications, Web, and Social media — much of it generated in real time and at a very large scale.

APPLICATIONS OF BIG DATA

Healthcare
– Predictive Analysis
– Tele-medicine
– Fitness wearables
– Remote Monitoring
• Banking
– ATM's
– E-Wallets
• Stock Market
• Education / Academics
• Manufacturing
• E-Commerce
• IT
• Government
• Social Media

TYPES OF BIG DATA

1. Structured Data

It owns a dedicated data model. It also has a well defined structure, it follows a consistent order and it is designed in such a way that it can be easily accessed and used by person or a computer. Structured data is usually stored in well defined columns and databases.
– Structured Schema
– Tables with rows and columns of data
– Example : DBMS,RDBMS

2. Semi-Structured Data

It is considered as another form of structured data. It inherits few properties of structured data, but major parts of this kind of data failures to have a definitive structure and also it does not obeythe formal structure of data models such as RDBMS.
– Schema is not defined properly
– JSON, XML, CSV,RSS
– Ex: Transactional history file, Log file

3. Unstructured Data

Unstructured data is completely different of which neither has a structure nor obeys to follow formal structural rules of data models. It does not even have a consistent format and it found to be varying all the time. But rarely it has information related to data and time.
– Heterogeneous Data
– Text file, Images, Videos, Audio.

BIG DATA CHARACTERISTICS

Big data characteristics are mere word that explain the remarkable potential of big data. In early stages development of big data and related terms there were only 3 V's (Volume, Variety, Velocity) considered as potential characteristics.
But ever growing technology and tools and variety of sources where information being received

has potentially increased these 3 V's into 5 V's and still evolving.
The 5 V's are

- Volume
- Variety
- Velocity
- Veracity
- Value

Volume

- Volume refers to the unimaginable amounts of information generated every second. This information comes from variety of sources like social media, cell phones, sensors, financial records, stock market etc.

Variety

- Variety refers to the many types of data that are available. A reason for rapid growth of data volume is that the data is coming from different sources in various formats.

- Big data extends beyond structured data to include unstructured data of all varieties: text, sensor data, audio, video, click streams, log files and more.

  The variety of data is categorized as follows:
  - Structured – RDBMS
  - Semi Structured – XML, HTML, RDF, JSON
  - Unstructured- Text, audio, video, logs, images

Velocity

- Velocity is the fast rate at which data is received and (perhaps) acted on. In other words it is the speed at which the data is generated and processed to meet the demands and challenges that lie in the path of growth and development.

Veracity

- Data veracity, in general, is how accurate or truthful a data set may be. More specifically, when it comes to the accuracy of big data, it's not just the quality of the data itself but how trustworthy the data source, type, and processing of it is.

- The data quality of captured data can vary greatly, affecting the accurate analysis.

Value

- Value is the major issue that we need to concentrate on. It is not just the amount of data that we store or process. It is actually the amount of valuable, reliable and trustworthy data that needs to be stored, processed, analyzed to find insights.

- Mine the data, i.e., a process to turn raw data into useful data. Value represents benefits of data to your business such as in finding out insights, results, etc. which were not possible earlier.

Big Data Analytics

Big data analytics techniques can be used to leverage the business benefits and by increasing the value of an organization. Big data has beneficial in many applications and in general thefollowing are the common categories. It is derived from The Apache Software Foundation's Powered By Hadoop Web site.

- **Business intelligence**, querying, reporting, searching, including many implementation of searching, filtering, indexing, speeding up aggregation for reporting and for report generation, trend analysis, search optimization, and general information retrieval.

- **Improved performance** for common data management operations, with the majority focusing on log storage, data storage and archiving, followed by sorting, running joins, extraction/transformation/ loading (ETL) processing, other types of data conversions, as well as duplicate analysis and elimination.

- **Non-database applications**, such as image processing, text processing in preparation for publishing, genome sequencing, protein sequencing and structure prediction, web crawling, and monitoring workflow processes.

- **Data mining and analytical applications**, including social network analysis, facial recognition, profile matching, other types of text analytics, web mining, machine learning, information extraction, personalization and recommendation analysis, ad optimization, and behavior analysis.

The ability to design, develop, and implement a big data application is directly dependent on an awareness of the architecture of the underlying computing platform, It includes the following four resources,

1. Processing capability, often referred to as a CPU, processor, or node. Modern processing nodes often incorporate multiple cores that are individual CPUs that share the node's memory and are managed and scheduled together, allowing multiple tasks to be run simultaneously; this is known as multithreading.

2. Memory, which holds the data that the processing node is currently working on. Most single node machines have a limit to the amount of memory.

3. Storage, providing persistence of data—the place where datasets are loaded, and from which the data is loaded into memory to be processed.

4. Network, which provides the "pipes" through which datasets are exchanged between different processing and storage nodes.

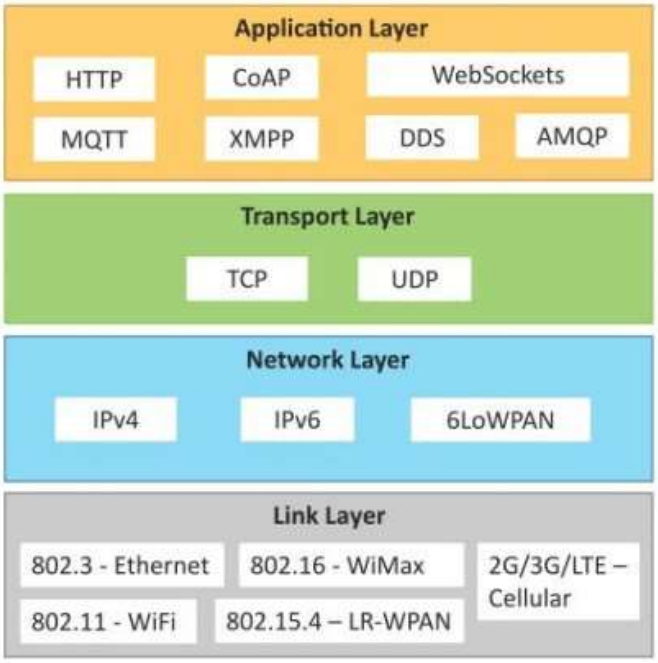
Why Big Data Analytics ?

- Advance analytics
- Business Intelligence

- Better Informed Decisions
- BI to increase sales, profit, customers
- Identify Business Risks
- Predict New Business Opportunities

Communication Protocols

- Communications protocols form the backbone of IoT system and enable network connectivity and coupling to applications.
- Communications protocols allow device to exchange data over the network.
- These protocols define the data exchange formats and data encoding schemes for devices and routing of packets from source to destination.
- Other function of the protocol include sequence control flow control and transmissions of Lost packet.



WiFi

WiFi is a wireless local area network (WLAN) that utilizes the IEEE 802.11 standard through 2.4GhZ UHF and 5GhZ ISM frequencies.

WiFi provides Internet access to devices that are within the range (about 66 feet from the access point).

Common Standards

- 802.11a – 5 GHz,
- 802.11b & 802.11g – 2.4/5 GHz,
- 802.11n - 2.4/5 GHz,
- 802.11ac – 5 GHz
- 802.11ad – 60 GHz

1 Mbps to 6.75 Gbps

WiMax

- WiMax or Worldwide Interoperability for Microwave Access is a set of compatibility standards for wireless networks supported by the WiMax Alliance.
- WiMAX technology is a wireless broadband communications technology based around the IEEE 802.16 standard providing high speed data over a wide area.
- It is faster than WiFi (75Mbps maximum) and has superior range, of up to 31 miles.
- WiMax is designed primarily for data transmission
- WiMAX technology is a standard for Wireless Metropolitan Area Networks
- 802.16.1a, 802.16.1b, 802.16.n, 802.16.p, 802.16-2017

LoRaWAN

- LoRaWAN (Long Range) is a proprietary low-power wide-area network protocol designed to connect battery operated 'things' to the internet in regional, national or global networks
- The LoRaWAN design to provide low-power WANs with features specifically needed to support low-cost mobile secure communication in IoT, smart city, and industrial applications.
- Specifically meets requirements for low-power consumption and supports large networks with millions and millions of devices, data rates range from 0.3 kbps to 50 kbps.
- Range- Approx. 2.5 km(Urban environment), 15 km (Suburban environment)
- Smart street lighting is a practical example, where the street lights are connected with the LoRa gateway that uses the LoRaWAN protocol.

ZigBee

- ZigBee is similar to Bluetooth and is majorly used in industrial settings.
- It has some significant advantages in complex systems offering low-power operation, high security, robustness suitable for sensor networks in IoT applications.
- The latest version of ZigBee is the recently launched 3.0, which is essentially the unification of the various ZigBee wireless standards into a single standard.

Standard- Zigbee 3.0 based on IEEE802.15.4
Frequencies- 2.4 Ghz
Range- Approx. 10-100m
Data Rates – 250 kbps

Z-Wave

Z-Wave is a low-power RF communications IoT technology that primarily design for home automation for products such as lamp controllers and sensors among many other devices.
Standard- Z-wave Alliance
Frequencies- Various
Range- Approx. 30m
Data Rates – 0.3 to 50 Kbps
It's very scalable enabling control for up to 232 devices.

2G/3G/4G (Mobile Communication)

- 2G – GSM / CDMA, GPRS, EDGE 9.6 kbps to 384 kbps
- 3G – UMTS / CDMA2000, 2 Mbps

- 4G – LTE – 100 Mbps
- Used through cellular networks
- Any IoT application that requires operation over longer distances can take advantage of GSM/3G/4G cellular communication capabilities.
- While cellular is clearly capable of sending high quantities of data, especially for 4G, the cost and also power consumption will be too high for many applications.

Embedded System

Embedded System is a system composed of hardware, application software and real time operating system. It can be small independent system or large combinational system.

An Embedded System is a system that has software embedded into computer-hardware, which makes a system dedicated for a variety of application or specific part of an application or product or part of a larger system.

An embedded system can be a small independent system or a large combinational system. It is a microcontroller-based control system used to perform a specific task of operation.

An embedded system is a combination of three major components:

- Hardware: Hardware is physically used component that is physically connected with an embedded system. It comprises of microcontroller based integrated circuit, power supply, LCD display etc.

- Application software: Application software allows the user to perform varieties of application to be run on an embedded system by changing the code installed in an embedded system.

- Real Time Operating system (RTOS): RTOS supervises the way an embedded system work. It act as an interface between hardware and application software which supervises the application software and provide mechanism to let the processor run on the basis of scheduling for controlling the effect of latencies.

In contrast to general purpose computers or personal computers which can perform various types of tasks, embedded systems are designed to perform a specific set of tasks.

Embedded system include Microprocessor and Microcontroller memory Ram ROM cache networking units (Ethernet WI-FI adaptor) input/output unit display keyboard , display and storage such as Flash Memory some embedded system have specialist processes such as digital signal processor DSP graphic processor and application.

Embedded System Applications

Smart Homes

Most of the products in your home are embedded which gives excellent experience and comfort to the user. Examples are Home Security system, Setup Box, Digital Camera, Television,

Microwave Oven, Air cooler, Refrigerator, Washing Machine and much more.

Offices
They are also into commercial enterprise solutions for inter-networking business clients. Examples are Router, Modem, Printer, and Gateways.

Transportation
The automotive industry is well competing worldwide. Some of the Embedded subsystems in automobiles are Anti-lock Braking System (ABS), Air conditioning control, Ignition control, Airbag control, Rain sensing wipers.

Healthcare
The medical field is a critical one, and the use of embedded systems is a nightmare. The odd design may lead to a disastrous effect on society or an individual. Examples are Blood pressure monitors, Heartbeat monitors, pacemakers, telesupervision and surgery, Scanners, Portable Ventilators.

Industrial world
The recent challenges of embedded systems extended its scope towards automation. Automation is the process of doing a task repetitively. Automation increases machine productivity, reducing development cost and design time. Examples are Industrial machinery and control, Temperature monitoring, 3D printing machines, Robotics, and Industrial Internet of Things.

Aerospace and Defense
Aerospace and Defense is a rugged area where security and performance are most important. To achieve this reliable firmware and embedded software have to be built. Examples are Flight control systems, Actuation, Air and Thermal Management, Engine power, Vehicle turbochargers, Navigation system, Embedded Imaging.

Embedded Hardware
The core of any embedded target is the electronic hardware – which resides on a Printed Circuit Board. The embedded development board is divided into five modules. They are Processor, Memory, Input devices, Output devices, and Bus controllers.

Hardware abstraction layer (HAL) is the fundamental resource of any embedded device and choosing a particular component depends on the requirement and specification of the designer. In the global market, there are many variants of hardware produced for different applications. Some of them are:

- Microcontroller (CPU)
- System on Chip (SoC)
- ASIC processor
- DSP processor

Input Devices
Input devices take input from the outside world. Some of the examples of input devices are

sensors, switches, photo-diode, optocoupler etc. They accept input from the user and respond accordingly.

Output Devices

The output devices are the indications or results that occur due to input events from outside the microcontroller. Examples of output devices are LCD, Touch screen, LED, Motors, Sevensegment displays, Buzzer, Relays, etc.

Bus controllers

The bus controller is a communication device that transfers data between the components inside an embedded system. Some of the bus controllers are Serial Buses (I2C, SPI, SMBus etc.), RS232, RS485 and Universal Serial Bus.

Memory

To store the data and deal with memory management, memory devices like flash and SD card, EEPROM is required. Some of the memories used in the embedded system are Non-Volatile RAM, Volatile RAM, DRAM (Dynamic Random Access Memory) etc.

Embedded Software

Software components are essential building blocks of embedded systems. Embedded software (sometimes called as firmware) written for Device drivers, Operating system, Application Software, Error handling, and debugging software.