Security in Internet of Things

Dr. Rashmi Jain

Syllabus

UNIT I: Introduction to IoT

Introduction, Conceptual Framework, Architectural view, technology behind IoT, Sources of the IoT, M2M Communication.

Design Principles for Connected Devices: IoT/M2M systems layers and design standardization, communication technologies, data enrichment and consolidation, ease of designing and affordability.

UNIT II: Hardware for IoT

Analog and digital sensors, actuators, radio frequency identification (RFID) technology, wireless sensor networks, participatory sensing technology.

Embedded Platforms for IoT: Embedded computing basics, Overview of IOT supported Hardware platforms such as Arduino, Raspberry pi, ESP8266, ESP32.

UNIT III: IoT Protocols

Physical and MAC layers, topology and Security of IEEE 802.15.4, 802.11ah, LoRaWAN.

Network Layer: Constrained Nodes and Constrained Networks, Zigbee, Routing over Low Power and Lossy Networks

Application Transport Methods: Supervisory Control and Data Acquisition

Application Layer Protocols: Constrained Application Protocol and Message Queueing Telemetry Transport

UNIT IV: Internet of Things (IoT) Security

Understanding the security risks, modes of attack - denial of service guessing the credentials, getting access to stored credentials, man in the middle, sniffing network communication, port scanning and web crawling, search features and wildcards, breaking ciphers, IoT authentication and authorization.

UNIT V: Attacks and Security Tools

Attacks on sensors, attacks to RFIDs, attacks to back-end systems, hardware attacks, database attack.

Tools for achieving Security: Virtual Private Networks, X.509 certificates and encryption, Authentication of identities, Usernames and passwords, Using message brokers and provisioning servers, Centralization versus decentralization.

UNIT VI: Security Issues in Real-Time Applications

Internet of Things Privacy, Security and Governance: Introduction, Overview of Governance, Privacy and Security Issues.

Real-Time Applications: Smart Home, Smart Grid Network, Wearable Computing, Mobile HealthCare.

Text Books

1. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, Fei HU, 2016, CRC Press.
2. Security of Things: An Implementers’ Guide to Cyber-Security for Internet of Things Devices and Beyond, Ollie Whitehouse, 2014, NCC Group.

Reference Books

1. Internet of Things (A Hands-on-Approach), Vijay Madisetti, Arshdeep Bahga, 1st Edition, 2014, VPT.

2. Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, Francis daCosta, 1st Edition, 2013, Apress Publications.

3. Practical Internet of Things Security, Brian Russell, Dreyw Van Duren, 2nd Edition, 2016, Packt Publishing.

4. Getting Started with the Internet of Things, Cuno Pfister, 2011, O‟Reilly Media.

Course Objective &Outcomes

Course Objective
The course will explore the concept to safeguard connected devices and networks in Internet of Things. Also, it discusses main threats and attacks on IoT products and services to improve technical and entrepreneurship skills.

Course Outcomes	
After successful completion of this course the student will be able to:	
CO1	Understand: Understand conceptual framework and design principles for connected devices for IoT.
CO2	Apply: Apply various IoT protocols at different layers for appropriate design of IoT.
CO3	Apply: Identify vulnerabilities, including recent attacks, involved in the Internet of Things.
CO4	Understand: Demonstrate the knowledge and understanding of security issues of the Internet of Things.
CO5	Apply: Make use of different IoT tools and protocols to design Real-Time Applications.

Unit I
Introduction to IoT

- Introduction
- Conceptual Framework
- Architectural view
- Technology behind IoT
- Sources of the IoT
- M2M Communication.
- Design Principles for Connected Devices:
- IoT/M2M systems layers and design standardization
- Communication technologies
- Data enrichment and consolidation
- Ease of designing and affordability

IoT (Internet of Things)

- It refers to the interconnectedness of physical devices, such as appliances and vehicles, that are embedded with software, sensors, and connectivity which enables these objects to connect and exchange data.
- This technology allows for the collection and sharing of data from a vast network of devices
- It creates opportunities for more efficient and automated systems.
- **It** is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment.
- In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives.
- Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a very few of the categorical examples where IoT is strongly established.

Definition:

- ***IoT is network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data.***
- A forecast by International Data Corporation (IDC) estimates that there will be **41.6 billion** IoT devices in 2025.
- Capable of generating **79.4 zettabytes (ZB)** of data.

Main components used in IoT:

- **Low-power embedded systems:** Less battery consumption, high performance are the inverse factors that play a significant role during the design of electronic systems.
- **Sensors :** Sensors are the major part of any IoT applications. It is a physical device that measures and detect certain physical quantity and convert it into signal which can be provide as an input to processing or control unit for analysis purpose.

Different types of Sensors :

1. Temperature Sensors
2. Image Sensors
3. Gyro Sensors
4. Obstacle Sensors
5. RF Sensor
6. IR Sensor
7. MQ-02/05 Gas Sensor
8. LDR Sensor
9. Ultrasonic Distance Sensor

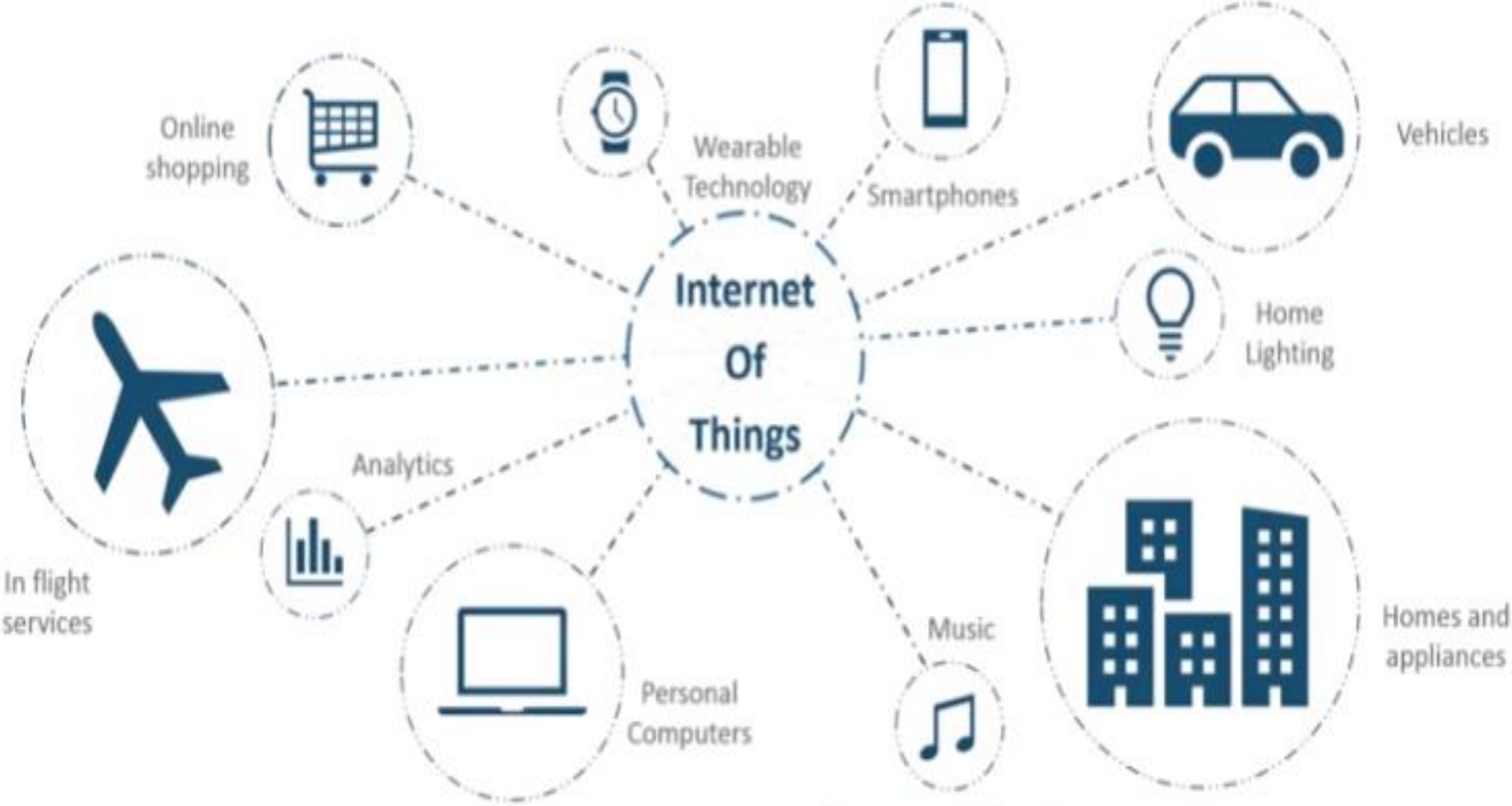
Main components used in IoT….

- **Control Units :**
  - A unit of small computer on a single integrated circuit.
  - Contains microprocessor or processing core, memory and programmable input/output devices/peripherals.
  - Responsible for major processing work of IoT devices and all logical operations are carried out here.
- **Cloud computing:**
  - Data collected through IoT devices is massive and this data has to be stored on a reliable storage server.
  - Cloud computing comes into picture for storing data.
  - The data is processed and learned, giving more room to discover where things like electrical faults/errors are within the system.

Main components used in IoT….

- ❖**Availability of big data:**
  - ➢IoT relies heavily on sensors, especially in real-time.
  - ➢As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.
- ❖**Networking connection:**
  - ➢In order to communicate the data, internet connectivity is a must.
  - ➢Here each physical object is represented by an IP address.
  - ➢However, there are only a limited number of addresses available according to the IP naming.
  - ➢Due to the growing number of devices, this naming system will not be feasible anymore.
  - ➢Therefore, researchers are looking for other options (in place of IPv4 we have IPv6).

IOT Applications


Internet
Of
Things
Online shopping
Wearable Technology
Smartphones
Vehicles
Home Lighting
In flight services
Analytics
Personal Computers
Music
Homes and appliances

Two ways of building IoT

1. Form a separate internetwork including only physical objects.
2. Make the Internet ever more expansive, but this requires hard-core technologies such as rigorous cloud computing and rapid big data storage (expensive).

In the near future, IoT will become broader and more complex in terms of scope. It will **change the world in terms of**

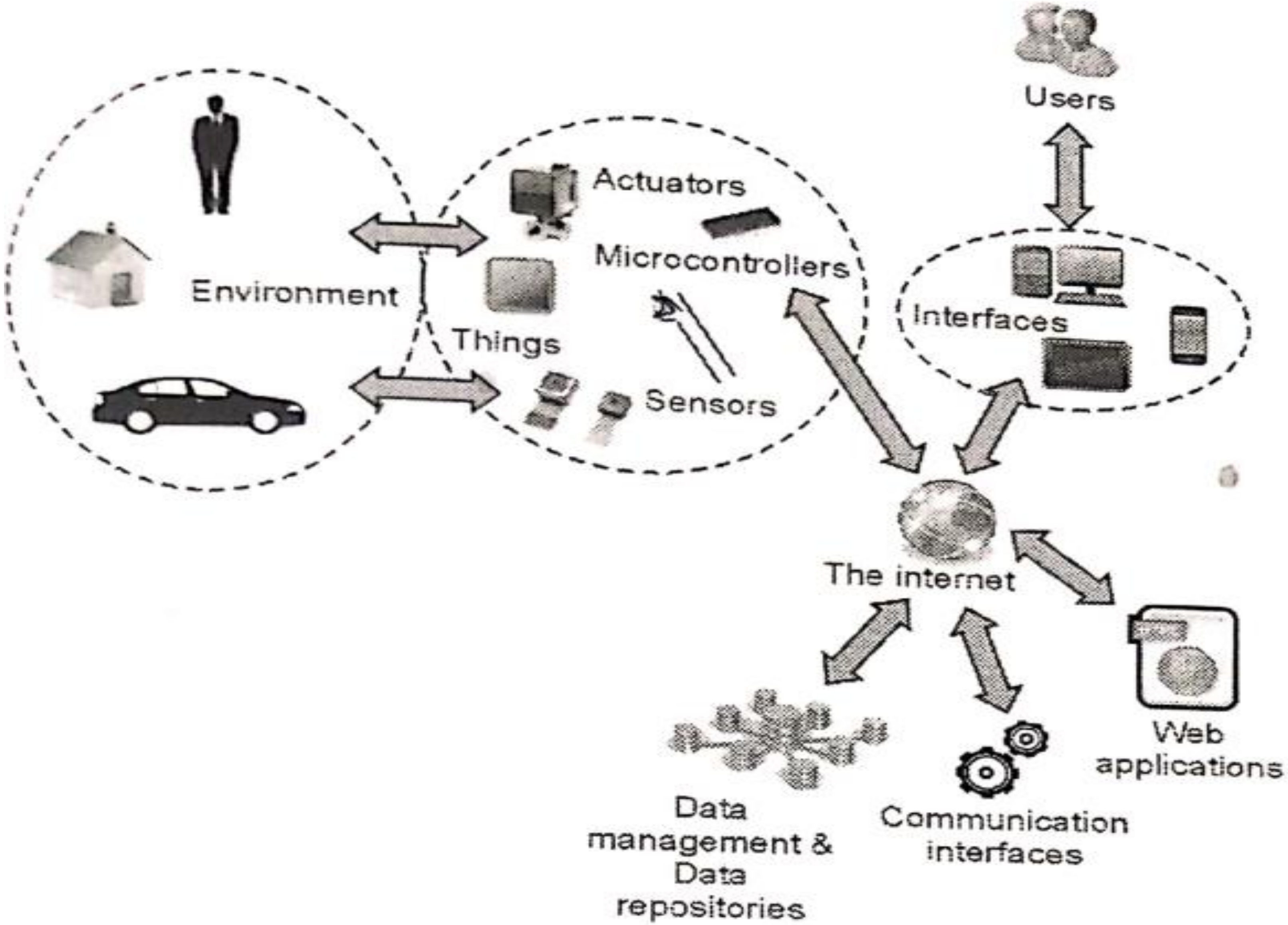
“anytime, anyplace, anything in connectivity.”

IoT Enablers

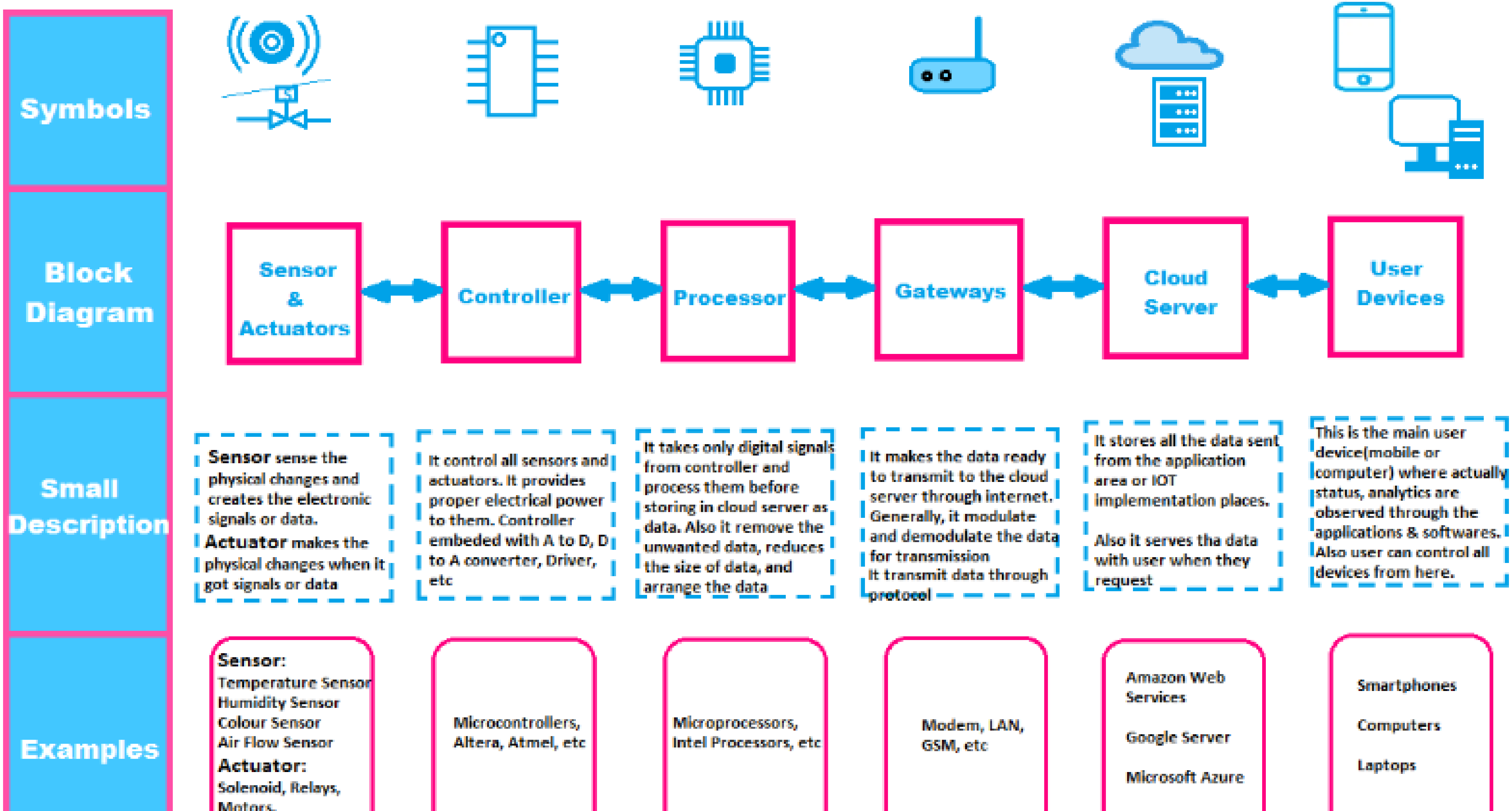
- **RFIDs:** uses radio waves in order to electronically track the tags attached to each physical object.
- **Sensors:** devices that are able to detect changes in an environment (ex: motion detectors).
- **Nanotechnology:** as the name suggests, these are extremely small devices with dimensions usually less than a hundred nanometers.
- **Smart networks:** (ex: mesh topology).

Working of IoT Devices

- ***Collect and Transmit Data :*** For this purpose sensors are widely used they are used as per requirements in different application areas.
- ***Actuate device based on triggers produced by sensors or processing devices :*** If certain condition is satisfied or according to user's requirements if certain trigger is activated then which action to performed that is shown by Actuator devices.
- ***Receive Information*** ***:*** From network devices user or device can take certain information also for their analysis and processing purposes.
- ***Communication Assistance :*** Communication assistance is the phenomena of communication between 2 network or communication between 2 or more IoT devices of same or different Networks. This can be achieved by different communication protocols like : MQTT , Constrained Application Protocol, ZigBee, FTP, HTTP etc.


Users
Environment
Actuators
Microcontrollers
Things
Sensors
Interfaces
The internet
Web applications
Data management & Data repositories
Communication interfaces

Architectural view



Symbols						
Block Diagram	Sensor & Actuators	Controller	Processor	Gateways	Cloud Server	User Devices
Small Description	**Sensor** sense the physical changes and creates the electronic signals or data. **Actuator** makes the physical changes when it got signals or data	It control all sensors and actuators. It provides proper electrical power to them. Controller embeded with A to D, D to A converter, Driver, etc	It takes only digital signals from controller and process them before storing in cloud server as data. Also it remove the unwanted data, reduces the size of data, and arrange the data	It makes the data ready to transmit to the cloud server through internet. Generally, it modulate and demodulate the data for transmission It transmit data through protocol	It stores all the data sent from the application area or IOT implementation places. Also it serves tha data with user when they request	This is the main user device(mobile or computer) where actually status, analytics are observed through the applications & softwares. Also user can control all devices from here.
Examples	**Sensor:** Temperature Sensor Humidity Sensor Colour Sensor Air Flow Sensor **Actuator:** Solenoid, Relays, Motors,	Microcontrollers, Altera, Atmel, etc	Microprocessors, Intel Processors, etc	Modem, LAN, GSM, etc	Amazon Web Services Google Server Microsoft Azure	Smartphones Computers Laptops

Characteristics of IoT

- Massively scalable and efficient
- IP-based addressing will no longer be suitable in the upcoming future.
- An abundance of physical objects is present that do not use IP, so IoT is made possible.
- Devices typically consume less power. When not in use, they should be automatically programmed to sleep.
- A device that is connected to another device right now may not be connected in another instant of time.
- Intermittent connectivity – IoT devices aren’t always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not

Sources of the IoT

- IoT Development Boards
- RFID and IoT Applications
- Wireless Sensor Networks

IoT Development Boards

Facilities Provided:

- **Power circuit**– Generally set up to run off of a 9V power supply
- **Programming interface**– Let you program the microcontroller from a computer
- **Basic input** – Usually buttons
- **Basic output**– Usually LEDs
- **I/O pins**– Used for motors, temperature sensors, LCD screens, etc.

Example Boards

- Raspberry Pi
- Omega 2
- Particle Photon
- Beagle bone –
- Jetson Nano
- ESP 32
- Banana Pi
- Arduino Nano 33 IoT
- Tessel 2
- i.MX 8

Radio Frequency Identification (RFID)

- Radio Frequency Identification (RFID) refers to a wireless system
- comprised of two components: tags and readers.
- The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag.
- Tags use radio waves to communicate their identity and other information to nearby readers,
- It can be passive or active.
  - Passive RFID tags are powered by the reader and do not have a battery.
  - Active RFID tags are powered by batteries.
- RFID tags can store a range of information from one serial number to several pages of data.
- Readers can be mobile so that they can be carried by hand, or they can be mounted on a post or overhead.
- Reader systems can also be built into the architecture of a cabinet, room, or building.

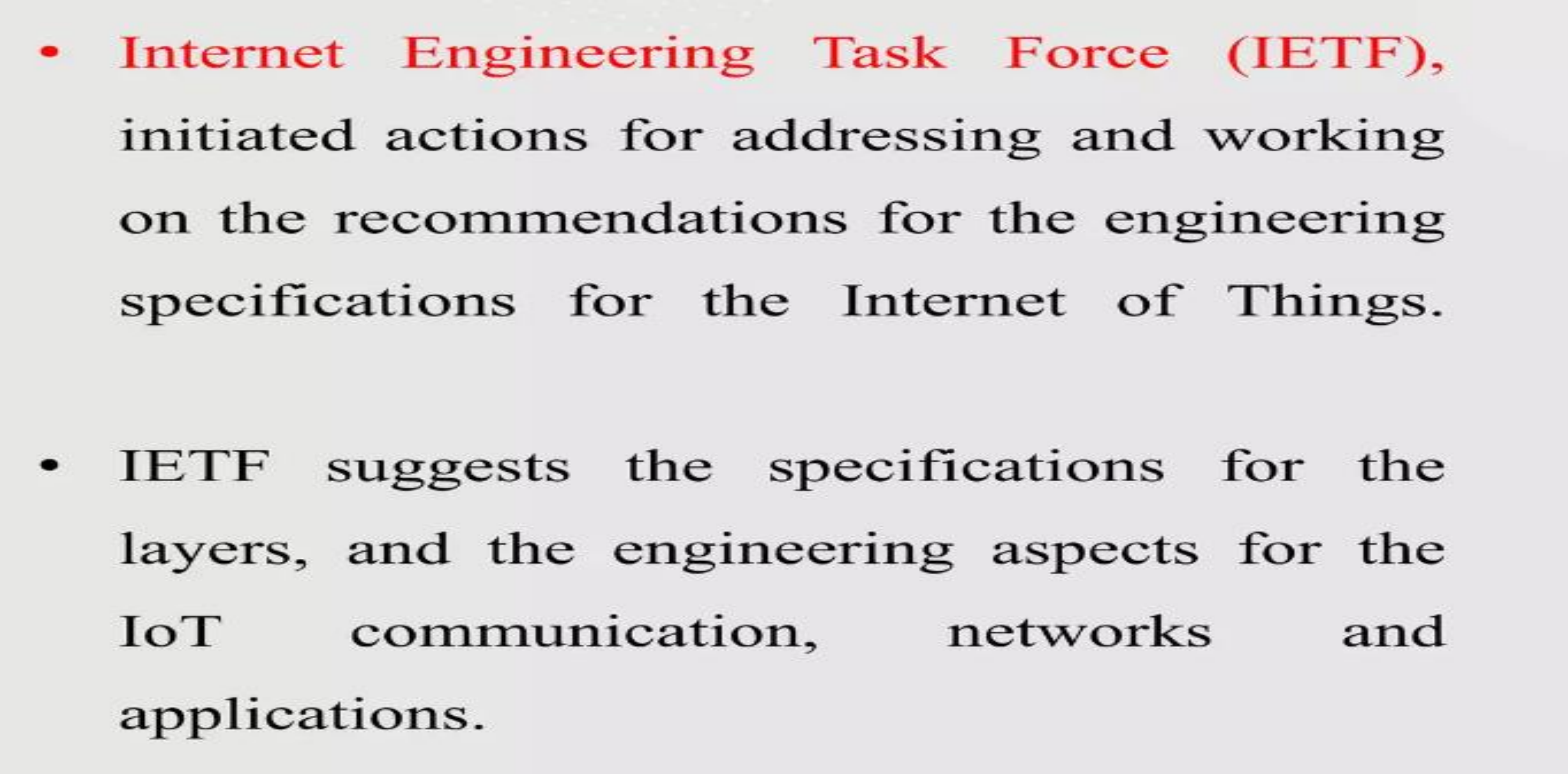
Wireless Sensor Networks

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.

Base Station in a WSN System is connected through the Internet to share data.

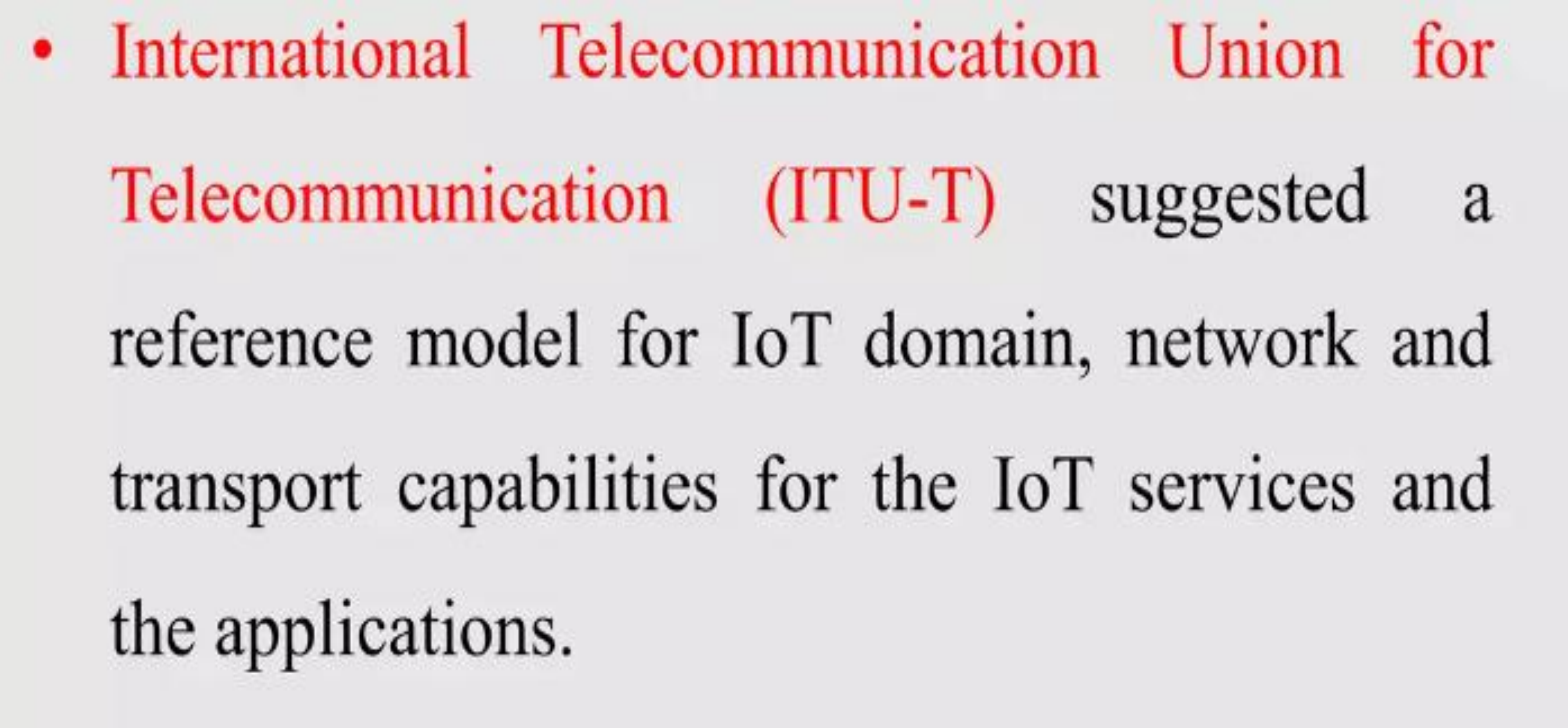
IoT/M2M Systems Layers and Design Standardization



- Internet Engineering Task Force (IETF), initiated actions for addressing and working on the recommendations for the engineering specifications for the Internet of Things.

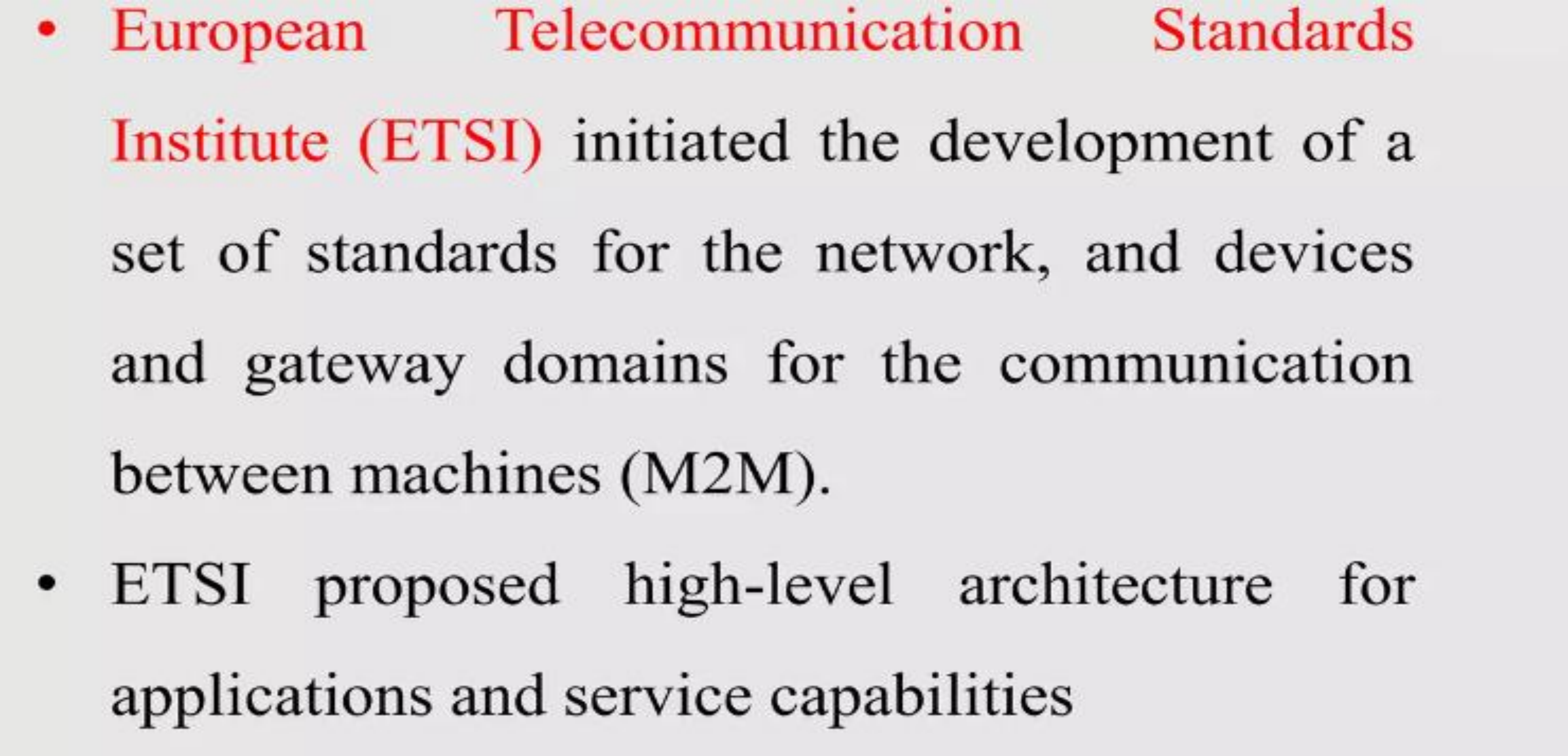
- IETF suggests the specifications for the layers, and the engineering aspects for the IoT communication, networks and applications.

IoT/M2M Systems Layers and Design Standardization



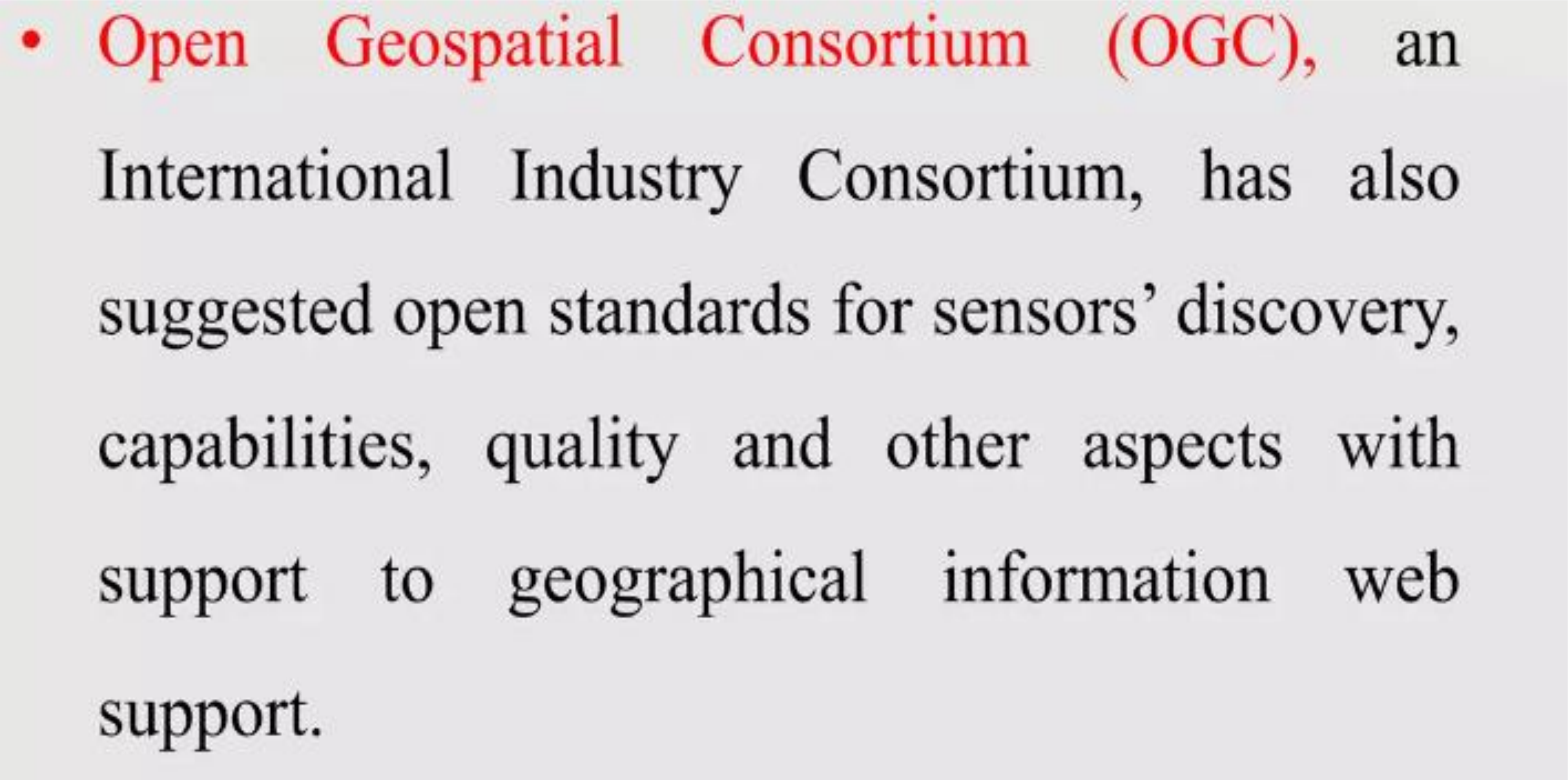
- International Telecommunication Union for Telecommunication (ITU-T) suggested a reference model for IoT domain, network and transport capabilities for the IoT services and the applications.

IoT/M2M Systems Layers and Design Standardization



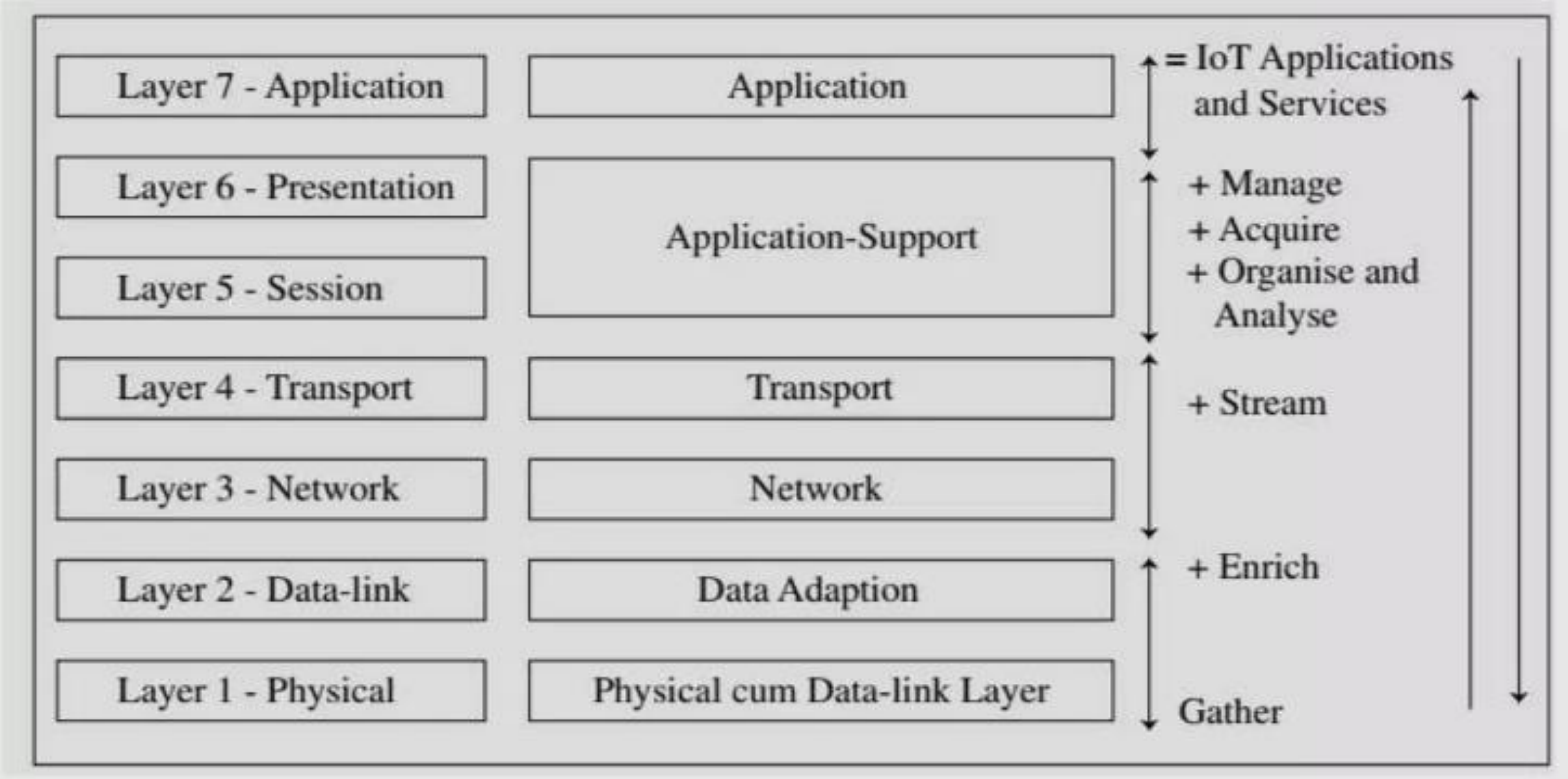
- European Telecommunication Standards Institute (ETSI) initiated the development of a set of standards for the network, and devices and gateway domains for the communication between machines (M2M).
- ETSI proposed high-level architecture for applications and service capabilities

IoT/M2M Systems Layers and Design Standardization



- Open Geospatial Consortium (OGC), an International Industry Consortium, has also suggested open standards for sensors' discovery, capabilities, quality and other aspects with support to geographical information web support.

Modified OSI Stack for the IOT/M2M Systems



Layer 7 - Application

Layer 6 - Presentation

Layer 5 - Session

Layer 4 - Transport

Layer 3 - Network

Layer 2 - Data-link

Layer 1 - Physical

Application

Application-Support

Transport

Network

Data Adaption

Physical cum Data-link Layer

= IoT Applications and Services

+ Manage

+ Acquire

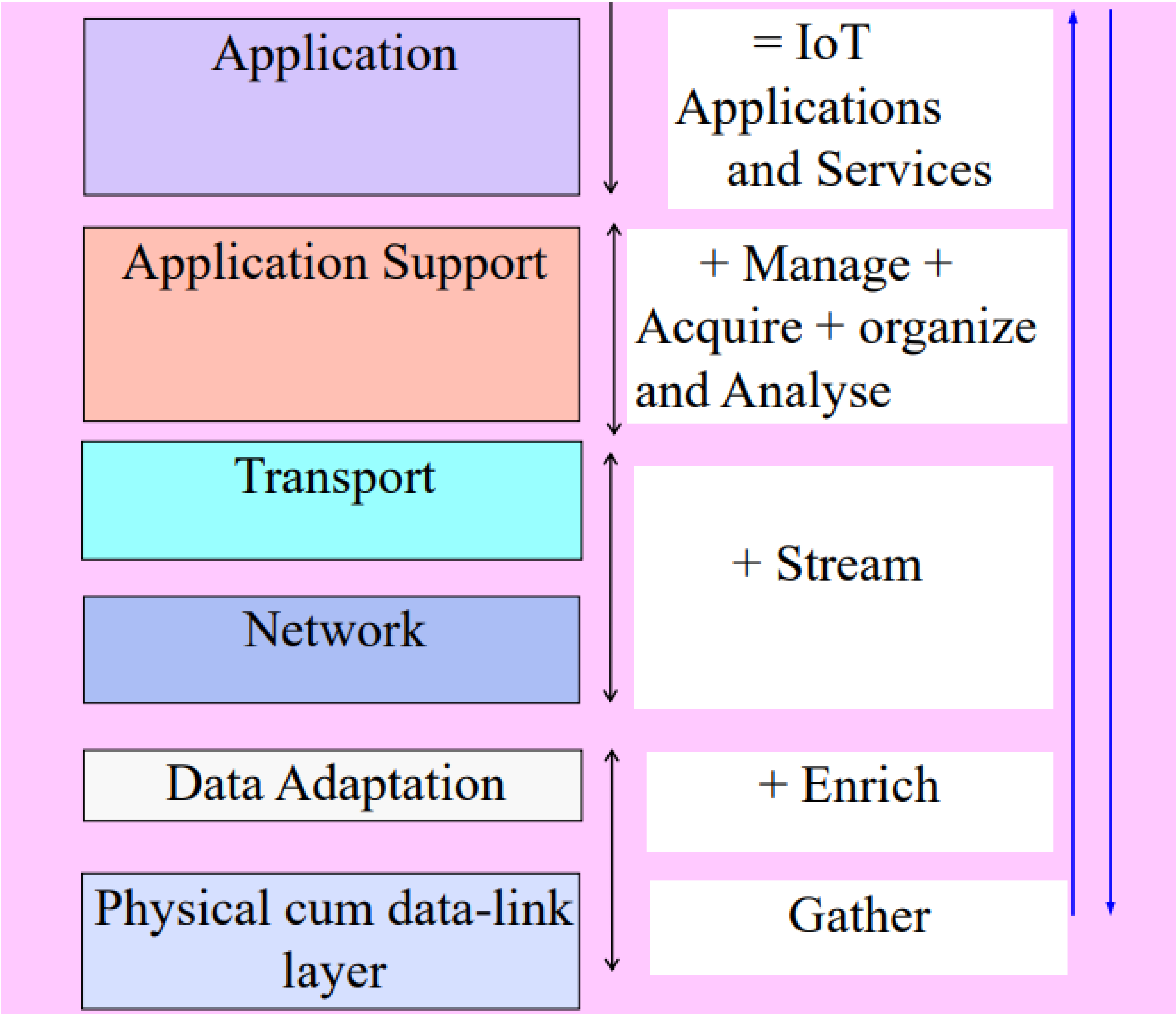
+ Organise and Analyse

+ Stream

+ Enrich

Gather

6 Layered Architecture



Application
= IoT Applications and Services
Application Support
+ Manage + Acquire + organize and Analyse
Transport
Network
+ Stream
Data Adaptation
+ Enrich
Physical cum data-link layer
Gather

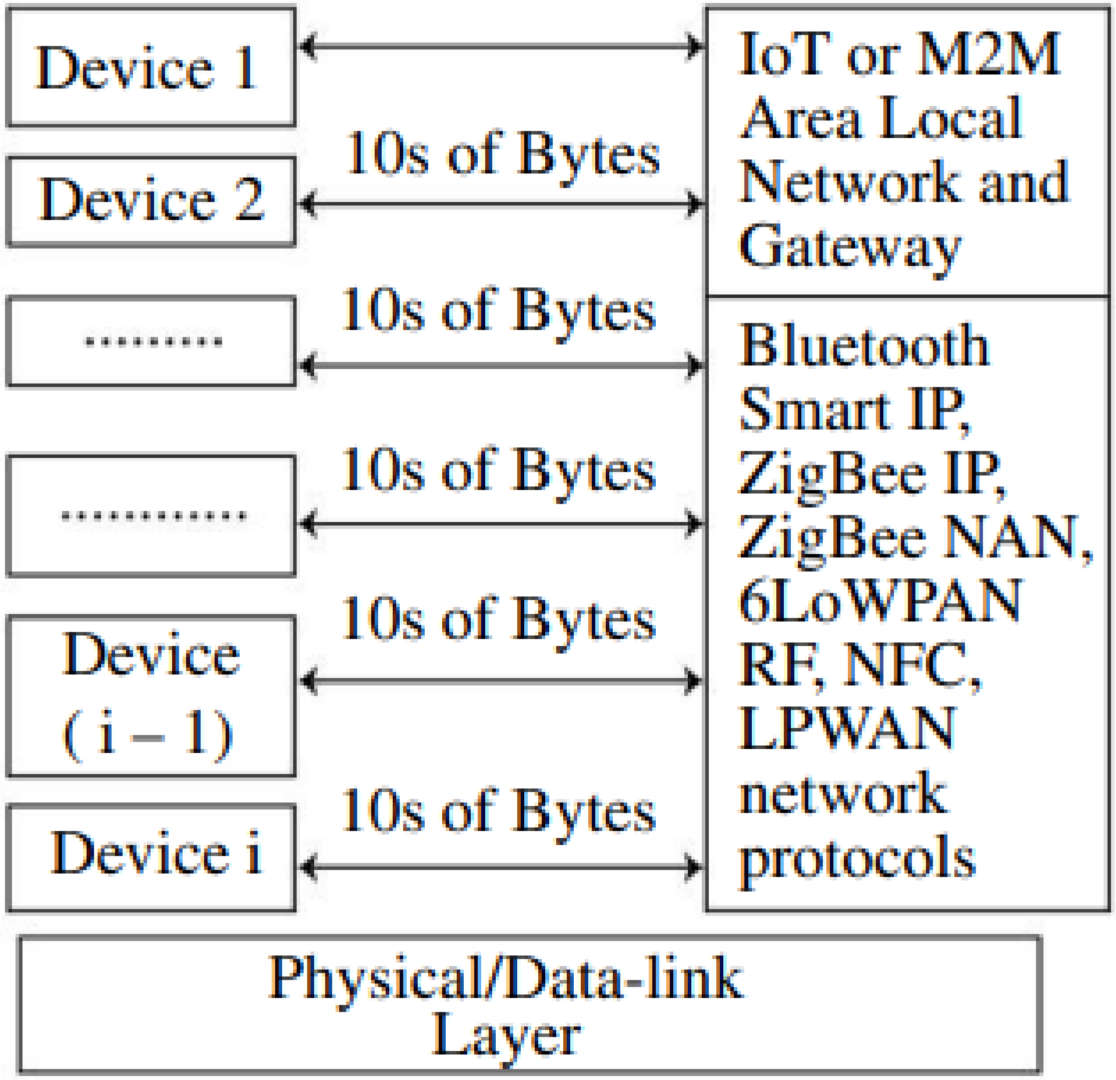
Data Interchange in Streetlight Example

- Layer 1: smart sensing and data-link circuit with each streetlight for transferring the sensed data to the layer 2
- Layer 2
- Group controller controls a group of streetlights as per the program commands from a Central station
- Layer 2: Data Adaptation the group controller receives data of each group through Bluetooth or ZigBee, then aggregates and compacts the data for communication to Internet
- Layer 3: Network stream on the Internet to next layer
- Layer 4: Transport layer for device identity management, identity registry and data routing to next layer
- Layer 5: Application support by data managing, acquiring, organising and analysing
- Layer 6: Application a remotely stored service program which issues the commands or programs the firmware at the service controllers
- Service controllers switch on-off, and monitor each group of streetlights in whole of the city

COMMUNICATION TECHNOLOGIES

- Connected devices 1st to ith connected to the local network and gateway using the WPAN or LPWAN network protocols
- The figure shows the local area network of devices.
- The connectivity between the devices (left-hand side) is by using RF, Bluetooth Smart Energy, ZigBee IP, ZigBee NAN(neighbourhood area network), NFC or 6LoWPAN or mobile.
- Tens of bytes communicate at an instance between the device and local devices network.

Bluetooth (Low Energy), ZigBee IP, NFC, RF link (Wireless Technologies), and I^2C, SPI, UART (Wired Technologies)



Device 1

Device 2

....

....

Device (i – 1)

Device i

10s of Bytes

10s of Bytes

10s of Bytes

10s of Bytes

10s of Bytes

IoT or M2M Area Local Network and Gateway

Bluetooth Smart IP, ZigBee IP, ZigBee NAN, 6LoWPAN RF, NFC, LPWAN network protocols

Physical/Data-link Layer

Wireless Communication Technology

Near-Field Communication

Near-Field communication (NFC) is an enhancement of ISO/IEC2 14443 standard for contact-less proximity-card.

- NFC is a short distance (20 cm) wireless communication technology.
- It enables data exchange between cards in proximity and other devices.
- Examples of applications of NFC are:
- proximity-card reader/RFID/IoT/M2M/mobile device, mobile payment wallet, electronic keys for car, house, office entry keys and biometric passport readers.

Radio Frequency Identification (RFID)

- Radio Frequency Identification (RFID) is an automatic identification method.
- RFIDs usethe Internet.
- RFID usage is, therefore, in remote storage and retrieval of data is done at the RFID tags.
- An RFID device functions as a tag or label, which may be placed on an object.
- The object can then be tracked for the movements. The object may be a parcel, person, bird or an animal.

Bluetooth(BT)

- Bluetooth devices follow IEEE 802.15.1 standard protocol for L1 (physical cum data-link layer).
- BT devices form a WPAN devices network.
- Two types of modes for the devices are
- Bluetooth BR/EDR (Basic Rate 1 Mbps/Enhanced Data Rate 2 Mbps and 3 Mbps) and
- Bluetooth low energy (BT LE 1Mbps). A latest version is Bluetooth v4.2. BT LE is also called Bluetooth Smart.
- Bluetooth v5, released in June 2016, has increased the broadcast capacity by 800%, quadrupled the range and doubled the speed.

Wi-Fi

- Wi-Fi is an interface technology that uses IEEE 802.11 protocol and enables the Wireless Local Area Networks (WLANs).
- Wi-Fi devices connect enterprises, universities and offices through home AP/public hotspots.
- Wi-Fi connects distributed WLAN networks using the Internet.
- Automobiles, instruments, home networking, sensors, actuators, industrial device nodes, computers, tablets, mobiles, printers and many devices have Wi-Fi interface.
- They network using a Wi-Fi network.
- Wi-Fi interfaces connect within themselves or to an AP or wireless router using Wi-Fi, PCMCIA or PCI card or built-in circuit cards.

RF Transceivers and RF Modules

- RF transmitters, receivers, and transceivers are the simplest RF circuits.
- A transceiver transmits the RF from one end and receives the RF from the other end, but internally has an additional circuit, which separates the signals from both ends.
- An oscillator generates RF pulses of required active duty cycle and connects to a transmitter.
- BT(Bluetooth), ZigBee, and WiFi radios deploy ISM band transceivers, which have comparatively complex circuits.

Wireless USB

- Wireless USB is a wireless extension of USB 2.0 and it operates at ultra-wide band (UWB) 5.1 GHz to 10.6 GHz frequencies.
- It is for short-range personal area network (high speed 480 Mbps 3 m or 110 Mbps 10 m channel).
- FCC recommends a host wire adapter (HWA) and a device wire adapter (DWA), which provides wireless USB solution.
- Wireless USB also supports dual-role devices (DRDs).
- A device can be a USB device as well as limited capability host.

Wired Communication Technology

UART/USART Serial Communication

- A Universal Asynchronous Transmitter (UART) enables serial communication (transmission) of 8 bits serially with a start bit at the start of transmission of a byte on serial Transmitter Data (TxD) output line.
- Serial means present one after another at successive time intervals.

Serial Peripheral Interface

- Serial Peripheral Interface (SPI) is one of the widely used serial synchronous communication methods.
- Source of serial synchronous output or input is called master when it also controls the synchronising clock information to the receiver.
- A receiver of serial synchronous input or output is called a slave, when along with the serial data it also receives the synchronising clock information from the master.
- Four sets of signals, viz., SCLK, MISO, MOSI, and SS (slave select) are used on four wires.
- When SS is active, then the device functions as a slave.

I2C Bus

- A number of device integrated circuits for sensors, actuators, flash memory and touchscreens need data exchanges in a number of processes.
- ICs mutually networkthrough a common synchronous serial bus, called inter-integrated circuit (I2C).
- Four potential modes of operation (viz. master transmit, master receive, slave transmit and slave receive)

Wired USB

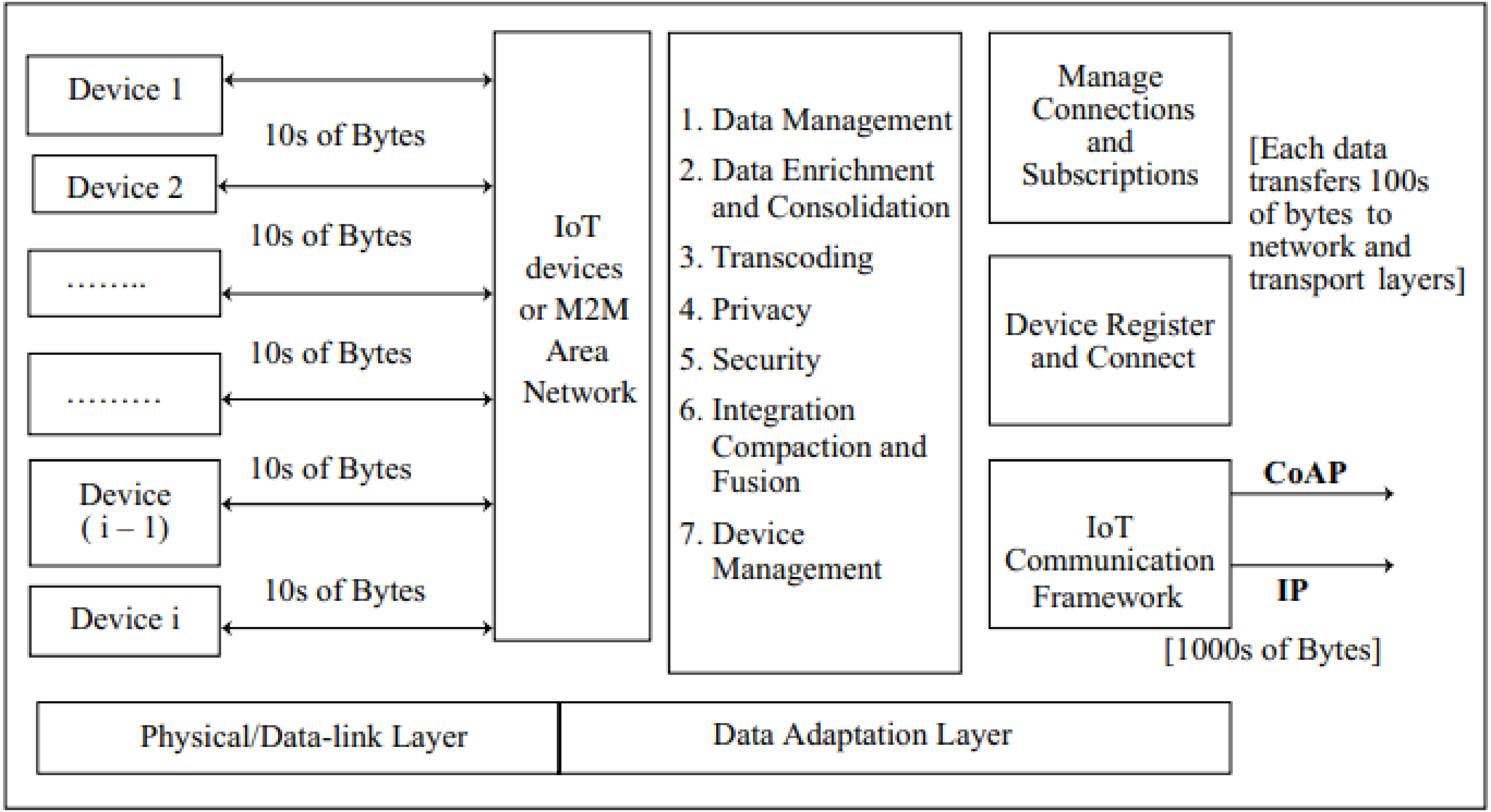
- Universal Serial Bus (USB) is for fast serial transmission and reception between the hosts, the embedded system and distributed serial devices;
- For example, like connecting a keyboard, printer or scanner.
- USB is a bus between the host system and a number of interconnected peripheral devices.
- Maximum 127 devices can connect with a host.
- USB standard provides a fast (up to 12 Mbps) as well as a low-speed (up to 1.5 Mbps) serial
- transmission and reception between the host and serial devices.
- Both the host and device can function in a system.
- USB three standards are USB 1.1 (1.5 and 12 Mbps), 2.0 (mini size connector) 480 Mbps, 3.0 (micro size connector) 5 Gbps and 3.1 (super speed 10 Gbps).

Ethernet

- Ethernet standard is IEEE 802.2 (ISO 8802.2) protocol for local area network of computers, workstations and device LANs.
- Each frame at a LAN consists of header.
- Ethernet enables the services of local device nodes, computers, systems and local resources, such as printers, hard disk space, software and data.

DATA ENRICHMENT, DATA CONSOLIDATION AND DEVICE MANAGEMENT AT GATEWAY

- A gateway at a data-adaptation layer has several functions.
- These are data privacy, data security, data enrichment, data consolidation, transformation and device management.
- The IoT or M2M gateway consists of data enrichment, consolidation and device management, and communication frameworks.
- The communication gateway enables the devices to communicate and network with the web.
- The communication gateway uses message transport protocols and web communication protocols for the Internet.


Device 1
Device 2
....
....
Device (i – 1)
Device i
10s of Bytes
10s of Bytes
10s of Bytes
10s of Bytes
10s of Bytes
IoT devices or M2M Area Network
1. Data Management
2. Data Enrichment and Consolidation
3. Transcoding
4. Privacy
5. Security
6. Integration Compaction and Fusion
7. Device Management
Manage Connections and Subscriptions
Device Register and Connect
IoT Communication Framework
[Each data transfers 100s of bytes to network and transport layers]
CoAP
IP
[1000s of Bytes]
Physical/Data-link Layer
Data Adaptation Layer

Data Management and Consolidation Gateway

- Gateway includes the provisions for one or more of the following functions:
  - Transcoding
  - Privacy, security
  - Integration
  - Compaction and fusion

Transcoding

- Transcoding means data adaptation, conversion and change of protocol, format or code using software.
- The gateway renders the web response and messages in formats and representations required and acceptable at an IoT device.
- Similarly, the IoT device requests are adapted, converted and changed into required formats acceptable at the server by the transcoding software.

Privacy

- Privacy is an aspect of data management and must be remembered while designing an application.
- Needed for: Data such as patient medical data, data for supplying goods in a company from and to different locations,
- Changes in inventories, may need privacy and protection from conscious or unconscious transfer to untrustworthy destinations using the Internet.
- A suitable encryption of identification of data source enforces privacy.
- Following are the components of the privacy model:

● Devices and applications identity-management

● Authentication

● Authorization

● Trust

● Reputation

Secure Data Access

- Access to data needs to be secure.
- The design ensures the authentication of a request for data and authorization for accessing a response or service.
- It may also include auditing of requests and accesses of the responses for accountability in future.
- In IOT a layer provides the confidentiality and authorization using AES-128 and CCM.
- End-to-end security is implied using a security protocol at each layer, physical, logical link and transport layers during communication at both ends in a network.

Data Gathering and Enrichment

- IoT/M2M applications involve actions such as data-gathering (acquisition), validation, storage, processing, reminiscence (retention) and analysis.
- Four modes of gathering data are:

  1. Polling refers to the data sought from a device by addressing the device; for example, waste container filling information in a waste management system.

  2. Event-based gathering refers to the data sought from the device on an event; for example, when the device reaches near an access point or a card reaches near the card reader or an initial data exchange for the setup of peer-to-peer or master-slave connection of BT device using NFC.

  3. Scheduled interval refers to the data sought from a device at select intervals; for example, data for ambient light condition in Internet of streetlights

  4. Continuous monitoring refers to the data sought from a device continuously; for example, data for traffic presence in a particular street.

- Data enrichment refers to adding value, security and usability of the data

Data Dissemination

- The three steps for data enrichment before the data disseminates to the network:
  - Aggregation,
  - Compaction And
  - Fusion.
- Aggregation refers to the process of joining together present and previously received data frames after removing redundant or duplicate data.
- Compaction means making information short without changing the meaning or context; for example, transmitting only the incremental data so that the information sent is short.
- Fusion means formatting the information received in parts through various data frames and several types of data (or data from several sources),
- removing redundancy in the received data and presenting the formatted information created from the information parts.
- Data fusion is used in cases when the individual records are not required and/or are not retrievable later.

EASE OF DESIGNING AND AFFORDABILITY

- Design for connected devices for IoT applications, services and business processes considers the ease in designing the devices' physical, data-link, adaption and gateway layer.
- Ensure availability of SDKs (software development kits), prototype development boards with smart sensors, actuators, controllers and IoT devices.
- They should be low in cost of hardware which it embeds and are preferably open source software components and protocols.
- Hardware should embed minimum number of components and
- Use ready solutions for ease in designing local devices personal area network and secure connectivity with the Internet.