UNIT I FUNDAMENDALS OF IOT

Definition and Characteristics of IoT, Sensors, Actuators, Physical Design of IoT – IoT Protocols, IoT communication models, IoT Communication APIs, IoT enabled Technologies – Wireless Sensor Networks, Cloud Computing, Embedded Systems, IoT Levels and Templates, Domain Specific IoTs – Home, City, Environment, Energy, Agriculture and Industry.

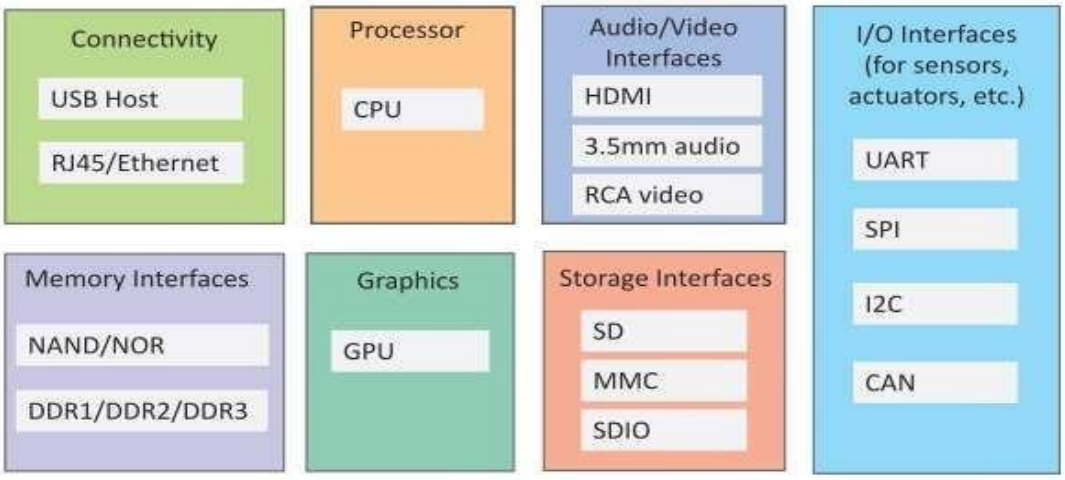
Physical Design of IoT

Things in IoT

The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing, Actuating and monitoring capabilities. IoT devices can

- Exchange data with other connected devices and applications (directly or indirectly), or
- Collect data from other devices and process the data locally or
- Send the data to Centralized servers or cloud-based applications back ends for processing the data or
- perform some tasks locally and other task within the IoT infrastructure, based on temporal and space constraints (ie: Memory, processing calibrators, communication latencies and speed and deadlines).

Figure : Generic block diagram of an IoT Device



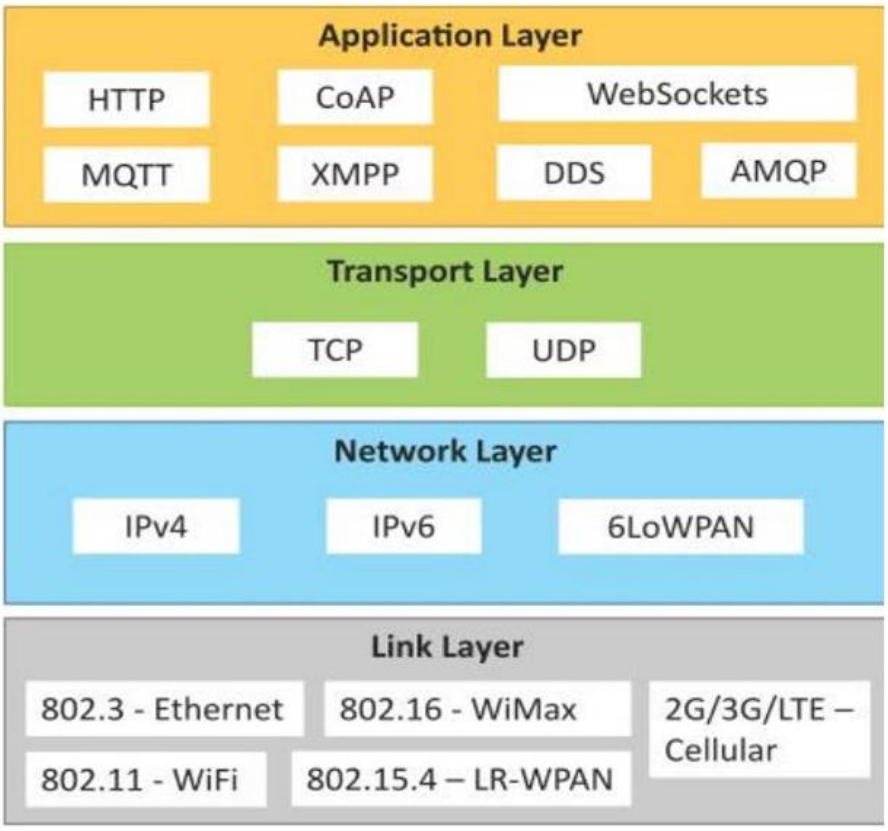
- An IoT device may consist of several interfaces' connections to other devices, both wired and

wireless. These include

- IoT interfaces for sensors
- interfaces for internet connectivity
- memory and storage interfaces
- audio video interfaces.

An IoT Device can collect various types of data from the onboard or attached sensors, such as temperature, humidity, light intensity. IoT devices can also be varied types, for instance, wearable sensors, smart watches, LED light automobiles and industrial machines. Almost all I would advise generate data in Some form or the other which when processed by Data Analytics systems leads to Useful information to guide further actions locally or remotely.

IoT Protocol



Link Layer:

Link Layer protocols determine how the data is physically sent over the networks physical layer or medium (example copper wire, electrical cable, or radio wave). The Scope of The Link Layer is the Last Local

Network connections to which host is attached. Host on the same link exchange data packets over the link layer using the link layer protocol. Link layer determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached.

802.3 Ethernet:

802.3 is a collection of wired Ethernet standards for the link layer. For example, 802.3 10BASE5 Ethernet that uses coaxial cable as a shared medium, 802.3.i is standard for 10 BASET Ethernet over copper twisted pair connection, Standards provide data rates from 10 Mb/s to 40 gigabits per second and the higher. The shared medium in Ethernet can be a coaxial cable, twisted pair wire or and Optical fiber. Shared medium carries the communication for all the devices on the network.

802.1- WI-FI:

IEEE 802.3 is a collection of wireless Local area network. (WLAN) communication standards, including extensive descriptions of the link layer. For example, 802.11a operate in the 5 GHz band, 802.11b and 802.11g operate in the 2.4 GHz band. 802.11ac operates in the 5G hertz band.

802.16 WiMAX:

IEEE 802.16 is a collection of wireless broadband and Standards, including extensive descriptions for the link layer also called WiMAX standard provides a data rates from 1.5 Mb/s to 1Gb/s the recent update provides data rates of hundred megabits per second for mobile station.

802.15.4 LR-WPAN:

IEEE 802.1 5.4 is a collection of standards for low-rate wireless personal area network (LR WPAN). These standard forms the basis of specifications for high level communication Zigbee. LR WPAN standards provide data rates from 40 k b/ s. These standards provide low cost and low speed Communications for power constrained devices.

2G / 3G / 4G mobile communications:

These are the different generations of mobile communication standards including second generation (2G including GSM and CDMA). 3rd Generation (3G including UMTS and CDMA2000) and 4th generation 4G including LTE.

Network / internet layer:

The network layer are responsible for sending of IP datagrams from the source network to the destination network. This layer Performs the host addressing and packet routing. The datagrams contain a source and destination address which are used to route them from the source to the destination across multiple

networks. Host Identification is done using the hierarchy IP addressing schemes such as ipv4 or IPv6.

IPV4:

Internet protocol versions for open parents close (IPV4) is there most deployed internet protocol that is used to identify the device is on a network using a hierarchy latest scheme. It uses 32-bit addresses scheme that allows total of 2 32 address. As more and more devices got connected to the internet. The Ipv4 has succeeded by IPv6.

IPv6:

It is the newest versions of internet protocol and successor to IPv4. IPv6 uses 128-bit address schemes that are lost total of 2 128 are 3.4* 10 38 address.

6LoWPAN:

IPv6 over low power wireless personal area networks brings IP protocol to the low power device which have limited processing capability it operates in the 2.4 GHz frequency range and provide the data transfer rate off to 50 kb/s.

Transport layer:

The Transport layer protocols provide end-to-end message transfer capability independent of the underlying network. The message transfer capability can be set up on connections, either using handshake or without handshake acknowledgements. Provides functions such as error control, segmentation, flow control and congestion control. TCP: Transmission control protocol is the most widely used to transport layer protocol that is used by the web browsers along with HTTP, HTTPS application layer protocols email program (SMTP application layer protocol) and file transfer protocol. TCP is a connection Oriented and stateful protocol while IP protocol deals with sending packets, TCP ensures reliable transmissions of packets in order. TCP also provide error deduction capability so that duplicate packets can be discarded and low packets are retransmitted. The flow control capability ensures that the rate at which the sender since the data is now too high for the receiver to process.

UDP:

unlike TCP, which requires carrying out an initial setup procedure, UDP is a connection less protocol. UDP is useful for time sensitive application they have very small data units to exchange and do not want the overhead of connection setup. UDP is a transactions oriented and stateless protocol. UDP does not provide guaranteed delivery, ordering of messages and duplicate eliminations.

Application layer:

Application layer protocol defines how the application interfaces with the lower layer protocols to send the data over the network. Data are typically in files, is encoded by the application layer protocol and encapsulated in the transport layer protocol. Application layer protocol enables process-to-process connection using ports.

Http:

Hypertext transfer protocol is the application layer protocol that forms the foundations of world wide web http includes, commands such as GET, PUT, POST, DELETE, HEAD, TRACE, OPTIONS etc. The protocol follows a request response model where are client sends request to server using the http, commands. Http is a stateless protocol and each http request is independent father request and http client can be a browser or an application running on the client example and application running on an IoT device, mobile applications or other software.

CoAP:

Constrained application protocol is an application layer protocol for machine-to-machine application M2M meant for constrained environment with constrained devices and constrained networks. Like http CoAP is a web transfer protocol and uses a request- response model, however it runs on the top of the UDP instead of TC CoAP uses a client –server architecture where client communicate with server using connectionless datagrams. It is designed to easily interface with http like http, CoAP supports method such as GET, PUT, DELETE.

WebSocket:

WebSocket protocol allows full duplex communication over a single socket connection for sending message between client and server. WebSocket is based on TCP and Allows streams of messages to be sent back and forth between the client and server while keeping the TCP connection open. The client can be a browser, a mobile application and IoT device

MQTT:

Message Queue Telemetry Transport it is a lightweight message protocol based on public subscribe model MQTT uses a client server Architecture by the clients such as an IoT device connect to the server also called the MQTT broker and publishers' message to topic on the server. The broker forwards the message to the clients subscribed to topic MQTT is well suited for constrained and environments

XMPP:

Extensible Messaging and Presence Protocol it is a protocol for real-time communication and streaming XML data between network entities XMPP powers wide range of applications including messaging, presence, data syndication, gaming multiparty chat and voice / voice calls. XMPP Allows sending small chunks of XML data from one network entity to another in real time. XMPP supports both client to server and server –client communication path.

DDS:

Data distribution service is the date centric middleware standard for device to-device machine to machine communication DDS uses a publish subscribe model where publisher example device that generate data create topics to which subscribers per can subscribe publisher is an object responsible for data distributions and the subscriber responsible for receiving published data. DDS provide quality of service (QoS) control and configurable reliability.

AMQP:

Advanced Message Queuing protocols. it is an open application layer protocol for business messaging. AMQP support point to point and publish - subscribe model routing and queuing. AMQP broker receive message from publishers' example devices or applications that generate data and about them over connections to consumers publishers publish the message to exchange which then distribute message copies to queues.