Unit I: Chapter 1 Introduction to Internet of Things

1.Definition and characteristics of IoT:Definition

A dynamic global network infrastructure with self – configuring based on standard and interoperable communication protocols where physical and virtual "things" have identified, physical attributes, and virtual personalities and use intelligent interfaces, oftencommunicate data associated with users and their environment

Characteristics

- Dynamic and self-Adapting:

IoT devices and systems may have the capability to dynamically adapt with the changingcontexts and take actions based on their operating condition.

Ex: Surveillance cameras can adapt their modes based on whether it is day or night.

- Self – Configuring:

IoT devices may have self-Configuring capability allowing a large number of devices to work together to provide certain functionality .

- Interoperable communication protocols:

IoT Devices may support a number of interoperable communication protocols and cancommunicate with other devices and also with the infrastructure.

- Unique Identity:

Each IoT devices has a unique identity and a unique identifier. (IPaddress, URI). IoT systems may have intelligent interfaces which adapt based on the context, allow communication with users and the environment contexts.

- Integrated into information network:

IoT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems.

2.Physical Design of IoT

Things of 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 exchangedata with other connected devices and applications (directly or indirectly), or collect datafrom 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 from some task locally and other task within the IoT infrastructure, based on temporal and space constraints (ie : Memory, processing calibrators, communication latencies and speed and deadlines).

An IoT device may consist of several interfaces connections to other devices, both wired and wireless. These include I)IoT interfaces for sensors II) interfaces for internet connectivity III) memory and storage interfaces IV) audio video interfaces. An IoT Devicecan collect various types of data from the onboard or attached sensors, such as temperature e , 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 Usefulinformation to guide further actions locally or remotely.

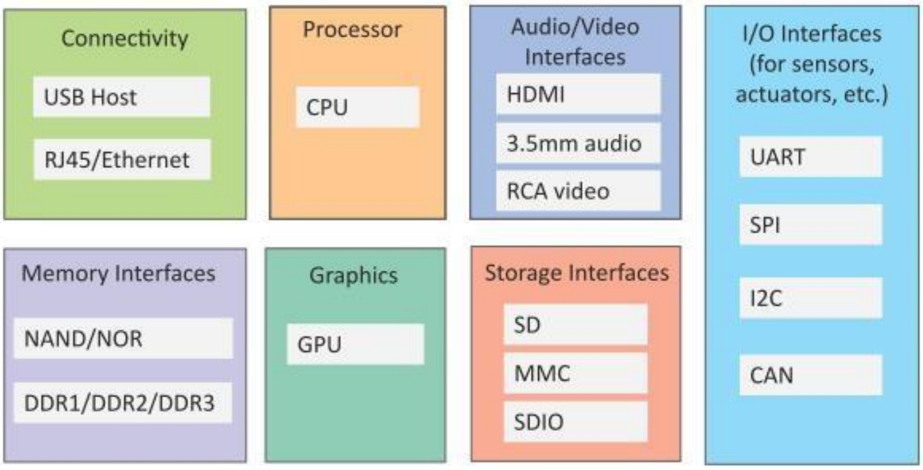


Fig: Generic Block Diagram of IOT Devices

3.IoT Protocol

Link Layer:

Link Layer protocols determine how the data is physically sent over the networks physicallayer or medium(example copper wire, electrical cable, or radio wave). The Scope of TheLink 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 themedium to which the host is attached.

802.3 Ethernet:

802.3 is a collections 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 10BASET Ethernet over copper twisted pair connection, Standards provide data rates from10 Mb/s to 40 gigabits per second and the higher. The shared medium in Ethernet can bea 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 collections of wireless Local area network.(WLAN) communication standards, including extensive descriptions of the link layer. For example 802.11a operatein 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 wirless broadband and Standards, including extensive descriptions for the link layer also called WiMAX wimax standard provides a data rates from 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 collections of standard for low rate wireless personal area network(LR-WPAN).These standard form 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 secondgeneration (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 tothe destination network. This layer Performs the host addressing and packet routing. The datagrams contains a source and destination address which are used to route them from thesource 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 usinga hierarchy latest schemes. 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 hassucceeded 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 operate in the 2.4 GHz frequency range and provide the data transfer rate off to 50 kb/s.

Transport layer :

The Transport layer protocols provides end-to-end message transfer capability independent of the underlying network. The message transfer capability can be set up onconnections, 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 deductioncapability 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 nowto too to 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 smalldata 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 define 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 enable 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 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 UDPinstead 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 connections for sending message between client and server. Websocket is based on TCP and Allows streams of messages to be sent back and forth betweenthe 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 forward 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 powerswide 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 modelwhere 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 overconnections to consumers publishers publish the message to exchange which thendistribute message copies to queues.

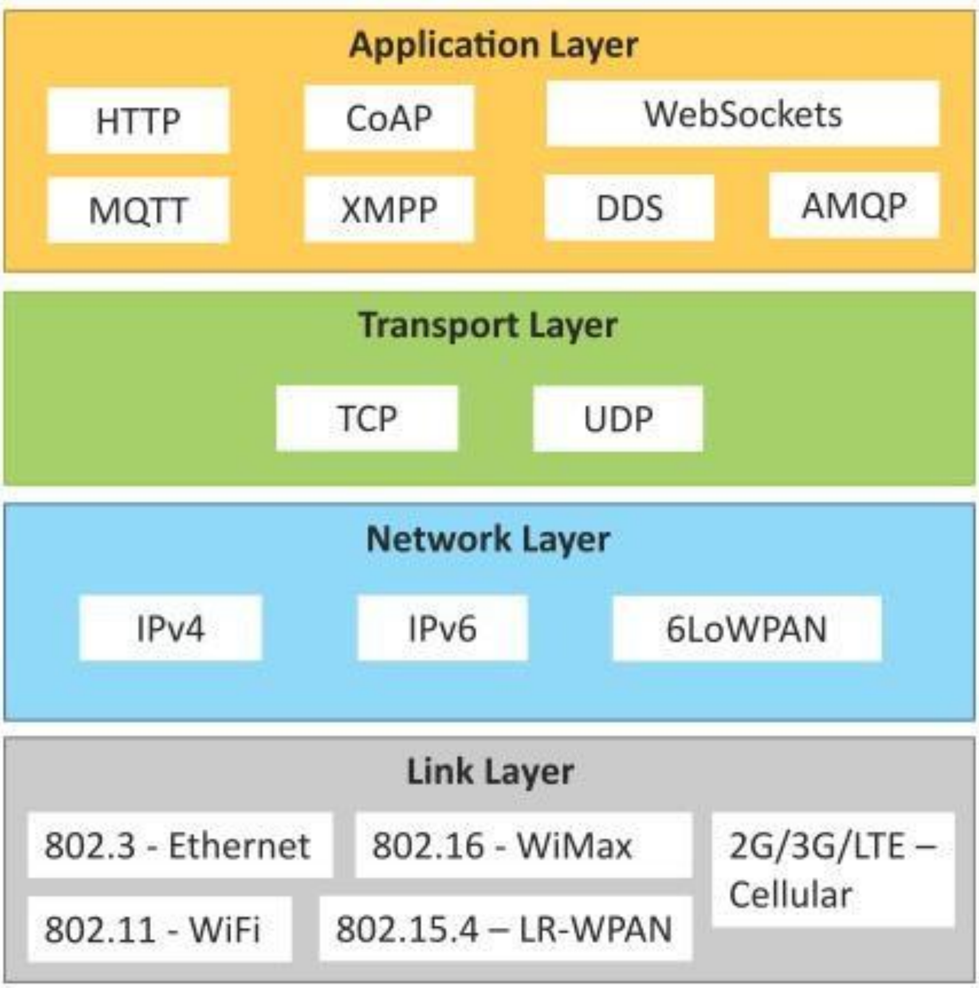


Fig: IOT Protocols

4.IoT communication model

- **Request response:** Request-response is a Communications model in which the client sendsrequest to the server and the server responds to the requests. when the server receives a request it decides how to respond, if it shows the data retrieved resources definitions for the response , and then send the response to the client. Access to response model is a stateless communication model and each request response per is independent of others thecrime and server interactions in the request response model.

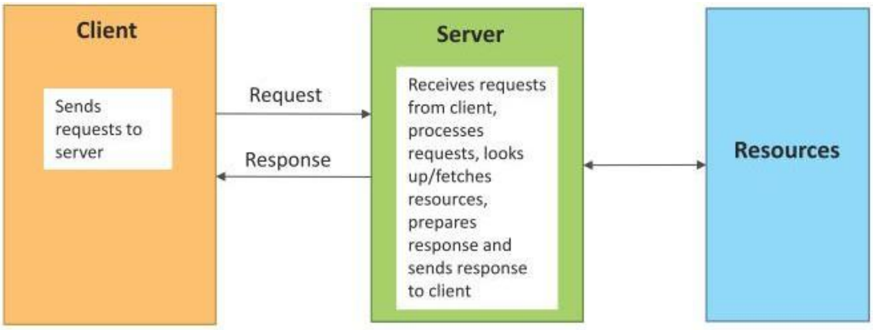

Client
Sends requests to server
Request
Response
Server
Receives requests from client, processes requests, looks up/fetches resources, prepares response and sends response to client
Resources

Fig: Request Response Communication Model

- **Publish - Subscribe:** Respect is a communication model that involve Publishers brokers and consumers. Publishers are the source of data. Publishers send the data to the topics which is managed by the broker. Publishers are not aware of the consumer. Consumers Subscribe to the topic which are managed by the broker. When the broker receives the datafor a topic from the publisher, it send the data to all the subscribed consumers.

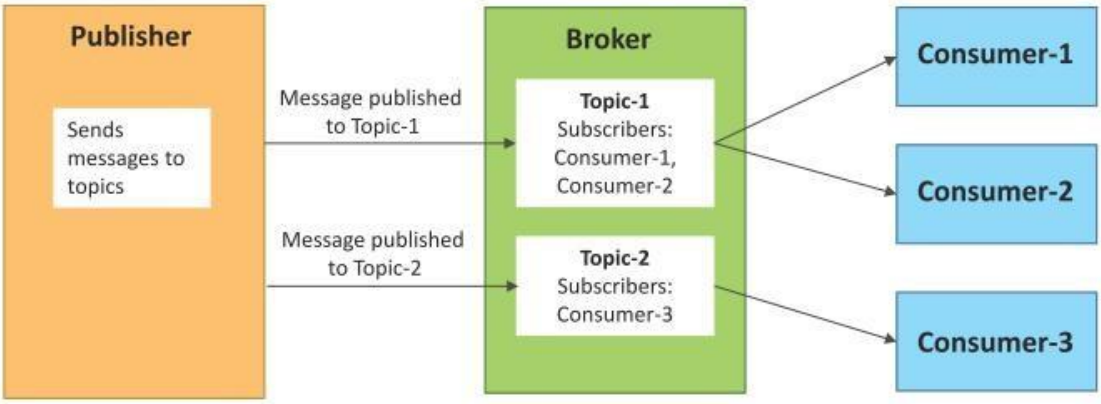


Fig: Publish-Subscribe communication model

- **Push pull:** Push pull is communication model in which the data producers push the data toqueues and the consumers pull the data from the queues. Producers do not need to be awareof the consumer. Queues help in decoupling the messaging between the Producers and Consumers . It also act as a buffer which helps in situations when there is a mismatch between the rate at which the produces push data and the rate at which the consumers fullthe data

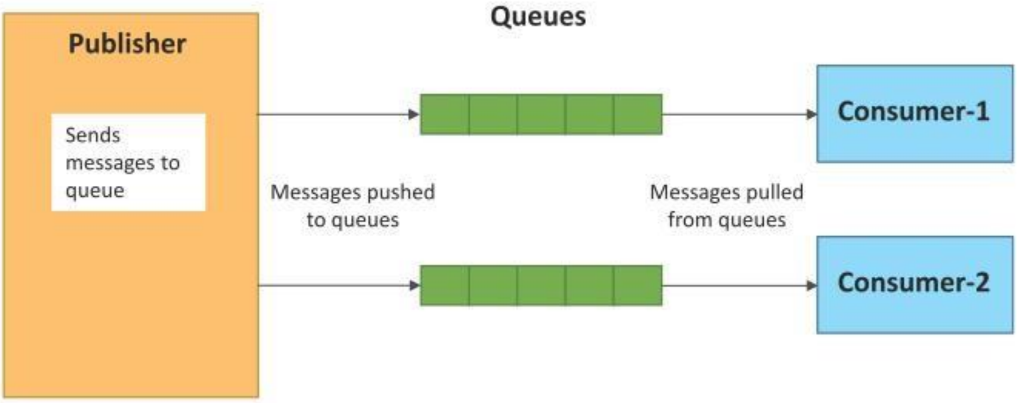


Fig: Push-Pull communication model

- **Exclusive pair:** Exclusive pair is a bi directional, fully duplex communication model that uses a persistent connections between the client and the server. once the condition is setupit remains open until the client sends a request to close the connection. client and server can send messages to each other after connection setup. Exclusive pair is a stateful Communications model and the server is aware of all the open connections.

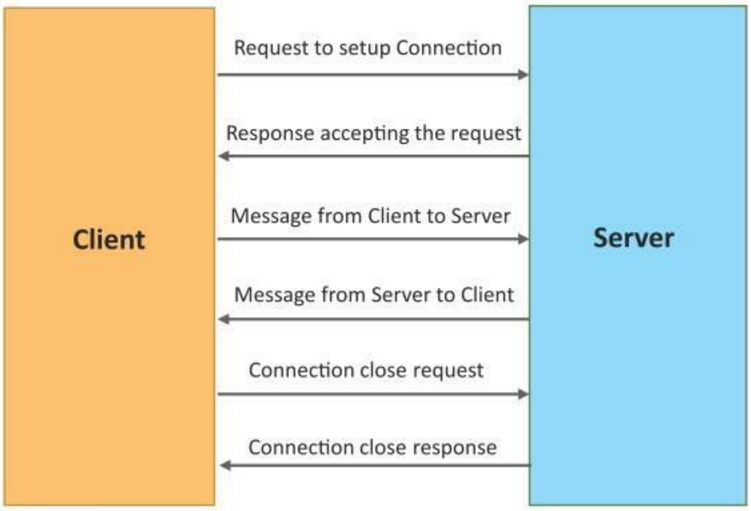

Client
Server
Request to setup Connection
Response accepting the request
Message from Client to Server
Message from Server to Client
Connection close request
Connection close response

Fig: Exclusive Pair Communication model

5.IoT communication APIs:

REST- based communication API:

Representational state transfer is a set of architectural principles by which you can designweb service and Web API that focus on a system resources and how resources states and addressed the transferred. REST API follow the request- response communication model.

The REST architectural constraints apply to the components, connectors, and data elements .

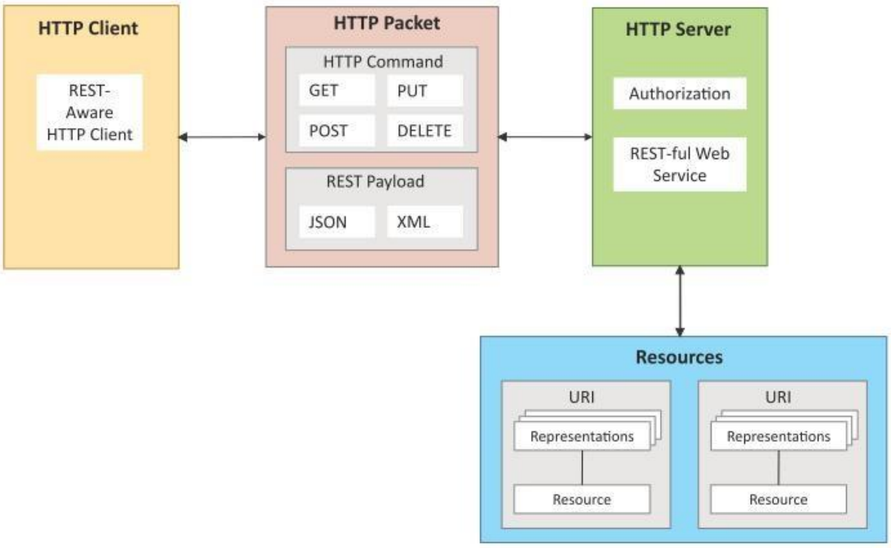


Fig: Communication with REST APIs

- **Client server:**

The principle behind the client-server conference separations of concerns for example client should not be concerned with the storage of data which is their concern of the server.Similarly the server should not be concerned about the user interface which is a concern of the client. separation allows client and server to be independently deployed and updated.

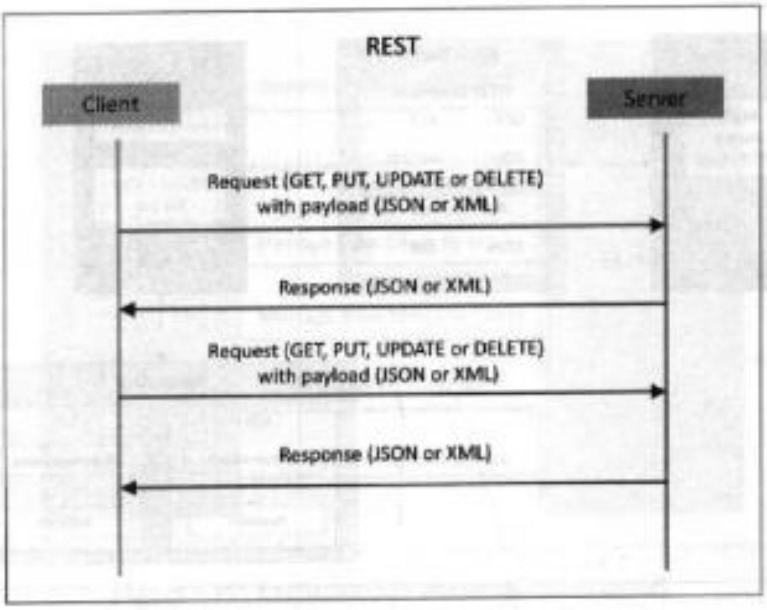

REST
Client
Server
Request (GET, PUT, UPDATE or DELETE) with payload (JSON or XML)
Response (JSON or XML)
Request (GET, PUT, UPDATE or DELETE) with payload (JSON or XML)
Response (JSON or XML)

Figure 1.12: Request-response model used by REST

- **Stateless:** Each request from client to server must contain all the information necessary to understand the request , and cannot take advantage of any stored context on the server .
- **Catchable:** Catch constrain requires that the data within the response to a request be implicitly or explicitly labeled as catchable or non-catchable. Then a client cache is giventhe right to reuse that response data for later, equivalent requests. completely eliminate some attractions and improve efficiency and scalability.
- **Layered system:**

System constraint come off constraints, constrains the behavior of components such that each component cannot see beyond the immediate layer with which they are interacting. Example client cannot tell whether it is connected directly to the end server or to an intermediary along the way system scalability can be improved allowing intermediaries torespond to request instead of tender server.

- **Uniform interface:**

Uniform interface constraints requires that the method of communication between clientand server must be uniform. Resources are identified in the request and separate from therepresentation of the resource that are returned to the client. When climbing holds a representation of your resource it has all the information required to update or delete the resource

- **Code on demand :** Service can provide executable code script for clients to execute in theircontext.

WebSocket based communication API:

WebSocket API allow bi directional, full duplex communication between client and server. Unlike request-response API allow full duplex communication and do not requirenew connection to be set up for each message to be sent. Websocket communication beginswith connection setup request send by the client to the server. The request is sent over httpand the server interprets it as an upgrade request. If the server support protocol response to the website handshake response after the connection setup the client and the server cansend data or messages to each other in full duplex model. WebSocket API reduce network traffic and latency as there is no overhead for connection setup and determination recordsto each message.

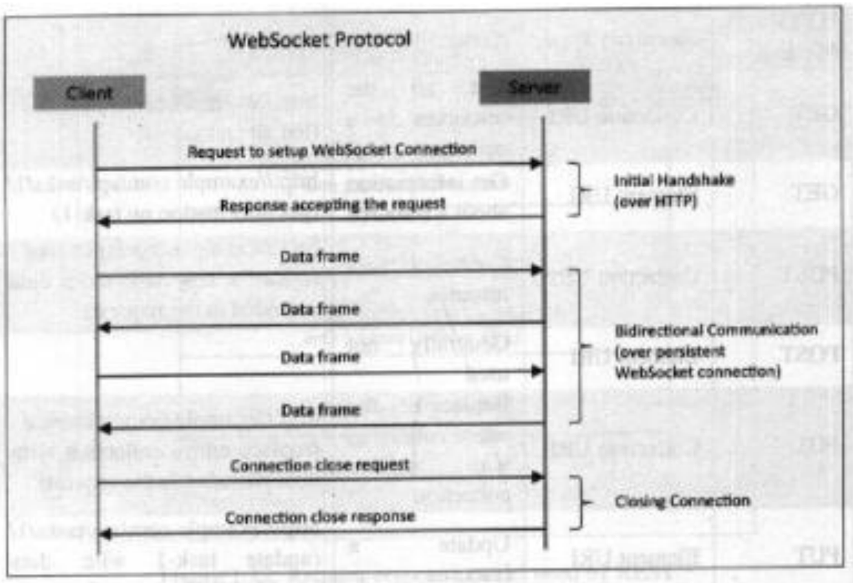

WebSocket Protocol
Client
Server
Request to setup WebSocket Connection
Response accepting the request
Initial Handshake (over HTTP)
Data frame
Data frame
Data frame
Data frame
Bidirectional Communication (over persistent WebSocket connection)
Connection close request
Connection close response
Closing Connection

Figure 1.13: Exclusive pair model used by WebSocket APIs

6.Communications protocol

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. Otherfunction of the protocol include sequence control flow control and transmissions of Lostpacket.

7.Embedded systems

An Embedded system is computer system that has computer hardware and software embedded perform specific task. 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.

8.IoT levels and Deployment Templates

In this section we define various levels of IoT systems with increasing completely. IoT system comprises of the following components:

1. **Device :** An IoT device allow identification, remote sensing, actuating and remote monitoring capabilities.
2. **Resources :** Resources are software components on the device for accessing and storing information for controlling actuator connected to the device also include software components that enable network access for the device .
3. **controller service:** Controller Service is a native service that runs on the device and interactwith the web services. Controller service sends data from the device to the web service receive command from the application from controlling the device.
4. **Database:** Database can be either local or in the cloud and stores the data generated by theIoT device.
5. **Web service:** Serve as a link between the device, application database and analysis components. Web Services can be implemented using HTTP and REST principles or usingwebsite protocol.

A comparison of restaurant website is provided below:

Stateless/stateful: Rest services stateless in nature. Each request contain all the informationneeded to process it. Request are independent of each other. Website on the other hand isstateful in nature where the server maintains the state and is aware of all the open connections.

Directional / Bi- directional: REST service operate over http and unidirectional. Request is always sent by a client and the server response to the request. And other hand website is a bi directional product server to send message to each other

Request response / full duplex: REST service follower request response Communicationsmodel where the client sends request and the server response to the request. Website and the other hand Allow full-duplex Communications between the client and server, it meansboth client and server can send messages to can independently.

TCP connections: For REST Service each http request involves setting up in a new TCP connections Websocket on the other hand involves a single TCP connection over which the client and server communicate in a full duplex mode.

Headache Overhead: REST service operate over http , and each request is independent ofothers . Thus each request carries http header which is an overhead. Due to the overhead of http headers, REST is not suitable for real time applications left hand does not involveoverhead of headers. After the initial handshake the client and server exchange messages with minimal frame information.

Scalability: Scalability is easier in this case of the REST services of request are independent And no state information needs to be maintained by the server. Thus both horizontal out and vertical scaling solutions are possible for REST services. For webSockets horizontal scaling can be cumbersome due to stateful nature of the communication. Since the server maintains the state of our connection, vertical scaling iseasier for Websocket than horizontal scaling.

Analysis component: The analysis component is responsible for analyzing the IoT data and generate results in the form which are easy for the user to understand. Analysis of IoT data can be performed either locally or in the cloud. Analyzed results are stored in the localor cloud database.

Application: IoT applications provide an interface that the user can use to control and monitor various aspects of the IoT system. Applications also allow user to view the systemstatus and view the processed data.

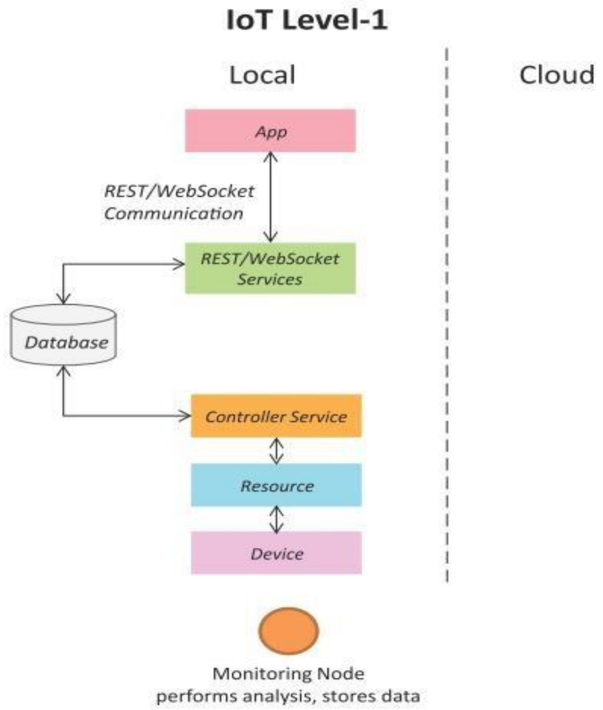
IoT level 1:

Level One IoT system has a single node / device that performs sensing and/or actuation, stores data, reforms analysis and the host to the application. Level 1 IoT systems are suitable for modeling low cost and low complexity solutions where the data involving is not big and the analysis requirements are not computationally intensive.

Let us now consider done example of Level 1 IoT system for home automation. This system consists of the single node that allows controlling the lights and appliances inyour home remotely . The device used in this system interface with their lights and appliances using electronic relay switches.

The status information of each light or appliance is maintained in a local database. RESTservice deployed locally Allow retrieving and updating the state of the each light or appliances in the status database.

The controller service continuously monitor the state of each light or appliance and triggersthe relay switches accordingly. The applications which is deployed locally has a user interface for controlling the lights or appliances. since the device is connected to the internet, the application can be accessed remotely as well.

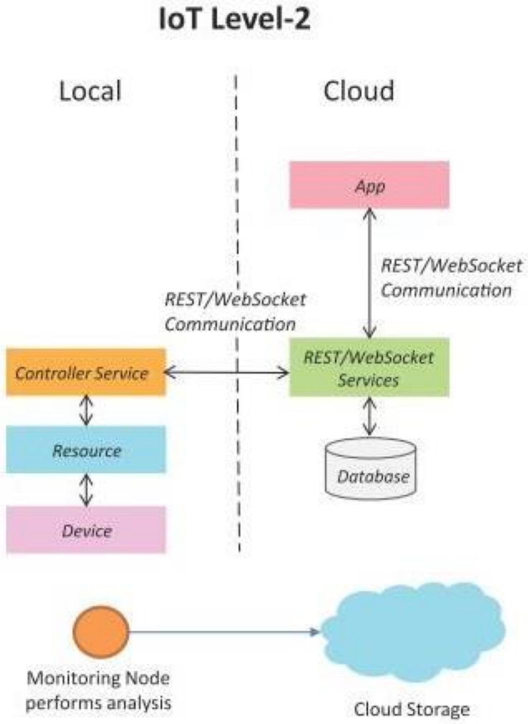


IoT level 2:

Level 2 IoT system has a single node that performs sensing and/or actuation and local analysis. Data is stored in the cloud and application is usually cloud based systems are suitable for solutions where the data in world is big, however the primary analysis requirement is not computationally intensive and can be done local itself.

Construct an example of Level 2 IoT system for smart irrigation.

The system consists of the single node that monitor the soil moisture level and control segregation system. The device used in this system collect soil moisture data from sensorthe controller service continuously monitor the moisture level. If the monster level drops below a threshold t , the irrigation system is turned on. For controlling the irrigation system actuators such as solenoid valve can be used.. Rest Web Services is used for storingand retrieving data which is stored in the cloud database. A cloud based application is usedfor visualizing the moisture level over a period of time, which can help in making decisionsabout irrigation schedules.



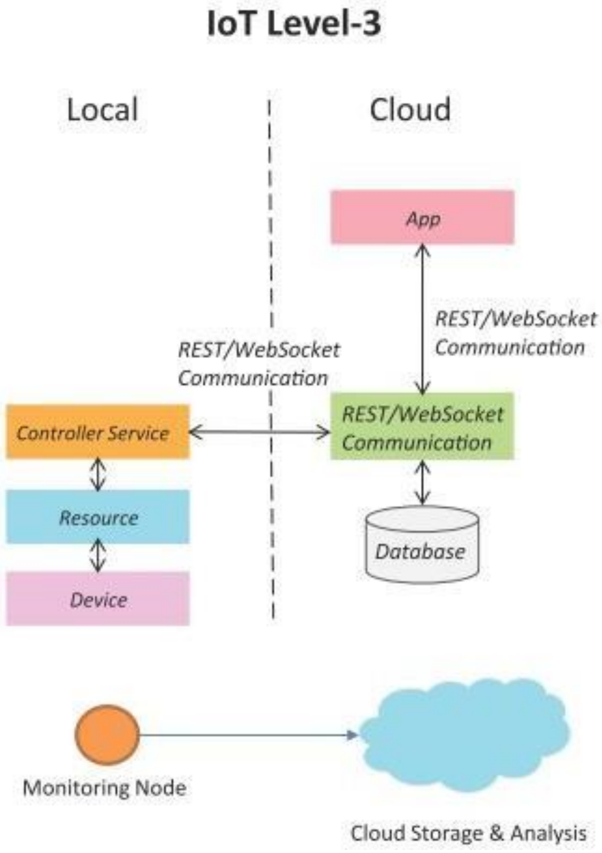
IoT Level 3:

Level 3 system has a single node . Data is stored and analyzed in the cloud application is cloud-based. Level 3 IoT system suitable for solutions where the data involved is big and analysis requirements computationally intensive.

Let us considered example of Level 3 IoT system tracking package handling. The systemconsists of a single node that monitors the vibration level for package being shipped.

The device in the system uses accelerometer and gyroscope sensor for monitoring vibration levels. The controller service send sensor data to the cloud in real time using a website service. The data is stored in the cloud and also visualized using a cloud based application.

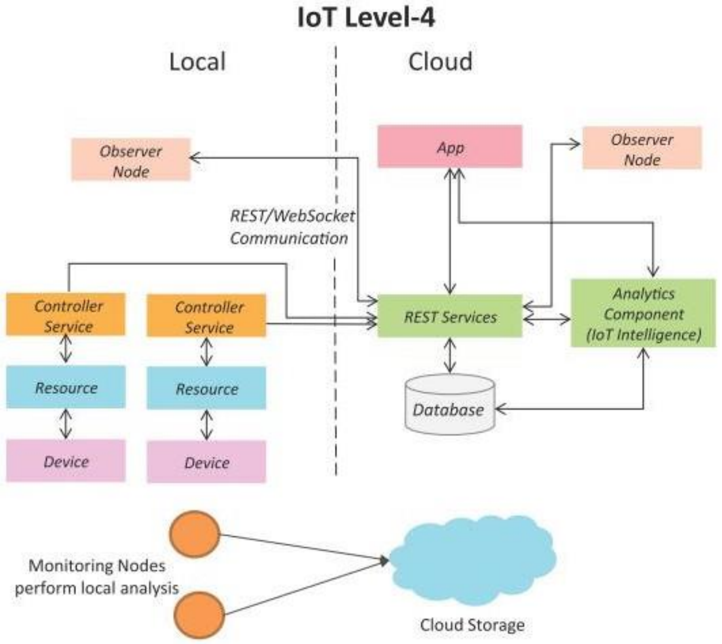
The analysis component in the cloud can Trigger alert the vibration level become greater than threshold. The benefit of using websocket service instead of the REST service this example the sensor data can be sent in real-time to the cloud. Cloud based application cansubscribe to the sensor data feeds for you in the real-time data.



IoT level 4:

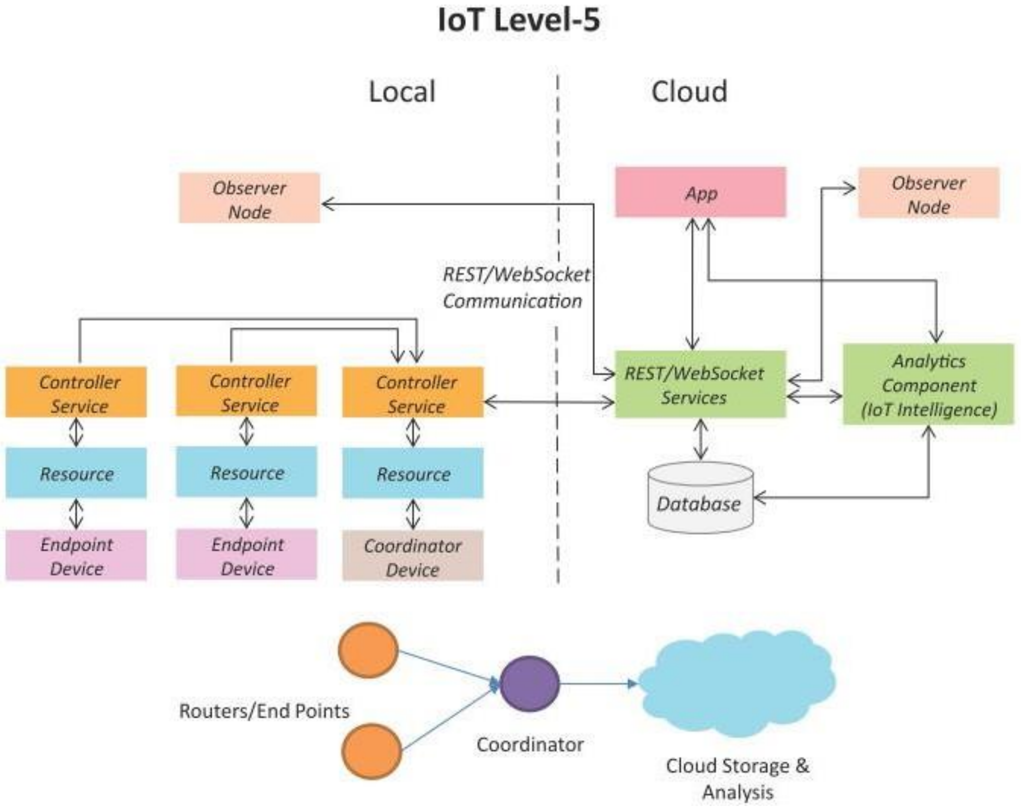
A level 4 IoT system has multiple notes that perform local analysis. Data is stored in the cloud and application is cloud based, level 4 contains local and cloud based observer noteswhich can subscribe to and receive information collected in the cloud from IoT devices. Observer node can process information and use it for various applications, however observer notes do not perform any control function. level 4 IoT systems are suitable for solutions where multiple nodes are required the data involved is big and the analysis requirements are computationally intensive.

let us consider an example of level four IoT system for noise monitoring. The system consists of multiple notes placed in different locations for monitoring noise level in an area. In this example with sound sensor. Nodes are independent of each other each node runs in one controller service that sends the data to the cloud. The data is stored in a clouddatabase the analysis of the data collected from a number of notes is done in the cloud



IoT Level 5:

IoT system has multiple end nodes and one coordinator notes and notes that perform sensing and / or actuation. Coordinator node collects data from the entry and send to the cloud. Data is stored and analyzed in the cloud and applications is cloud based. Level 5 IoT system are suitable for forest fire detection. The system consists of multiple nodes placed in different locations for monitoring temperature, humidity and carbon dioxide levels in a forest. The endnotes in this example are equipped with various sensors such astemperature humidity and to CO2. The coordinator node collects the data from the end nodes and act as a Gateway that provides internet connectivity to the IoT system. The controller service on the coordinator device sends the collected data to the cloud .The data is stored in the cloud database. The analysis of the data is done in the computing cloudto aggregate the data and make prediction.

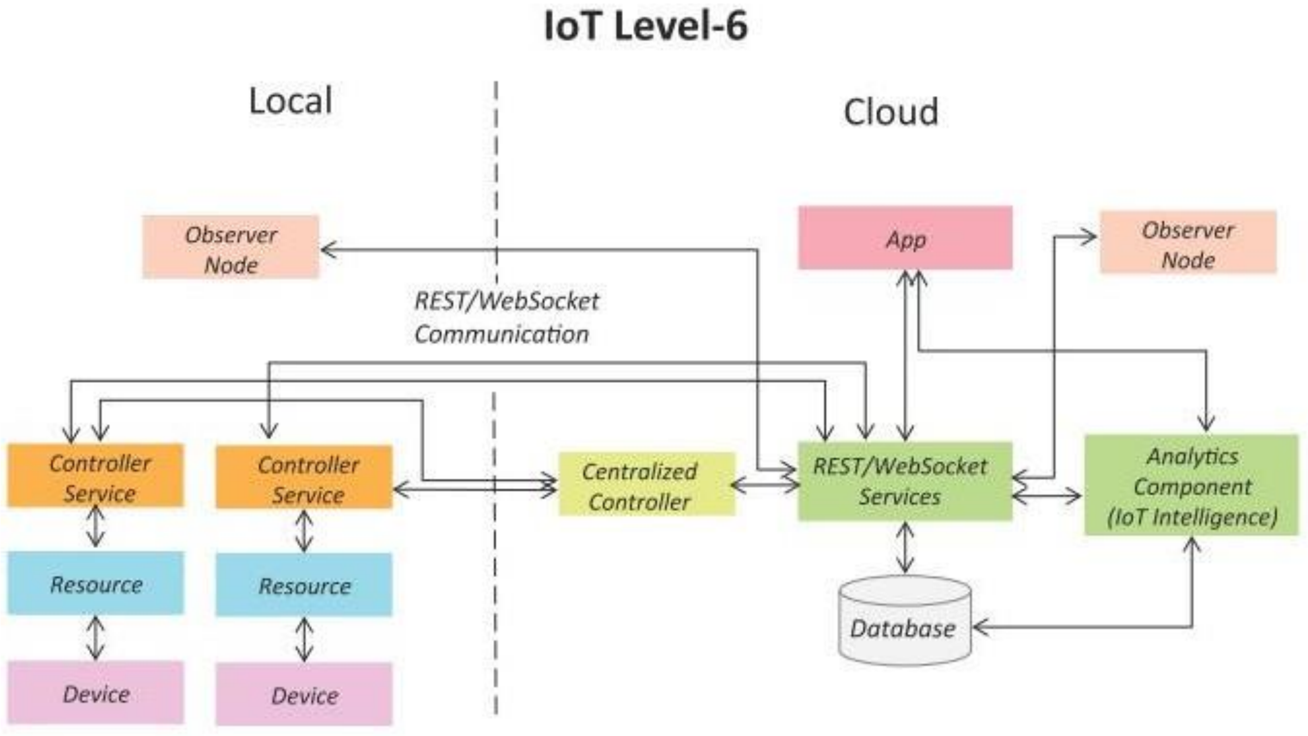


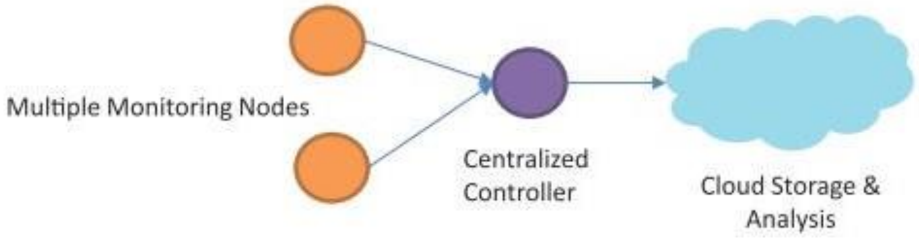
IoT Level 6:

IoT Level 6 system has multiple Independent and nodes that perform sensing and / or actuations and send data to the cloud. Data is stored in the cloud and applications is cloudbased .

The analytics component analyze the data and store the results in the cloud database. Theresults are visualized with the cloud based application. The centralized controller is awareof the status of all the end notes and send control commands to the notes.

Let us consider an example of the level 6 IoT system for weather monitoring. The systemconsists of multiple nodes placed in different location for monitoring temperature, humidity and pressure in an area. The end nodes are equipped with various sensors such as temperature ,pressure and humidity. The end nodes send the data to the cloud in real time using a websocket service .The data is stored in a cloud database. The analysis of thedata is done in the cloud to aggregate the data and make predictions. A cloud based applications is used for visualizing the data.


IoT Level-6
Local
Cloud
Observer Node
REST/WebSocket Communication
App
Observer Node
Controller Service
Controller Service
Centralized Controller
REST/WebSocket Services
Analytics Component (IoT Intelligence)
Resource
Resource
Database
Device
Device


Multiple Monitoring Nodes
Centralized Controller
Cloud Storage & Analysis