Introduction to IOT

Industry 1.0 → late 18th Century
transition from manual labor to mechanized production using water and steam power, it introduced factories & ~~mass~~

Industry 2.0 → early 20th Century
adoption of electricity, leading to assembly lines & mass production. this period saw the rise of steel, oil and the automotive industries.

Industry 3.0 → early 1970's
Shift to automation, computers & electronics. introduced digital technology and use of IT systems in manufacturing

Industry 4.0 → early 21st century
Integration of advanced technologies like IOT, AI, big data and robotics to create intelligent,

Internet is global system of interconnected Computer networks that use internet protocol suite (TCP/IP) to link devices worldwide

it is network of networks that consists of private, public, academic, business and goverment networks of local to global scope, linked by broad array of electronic, wireless and optical ntw technologies

Evolution of Internet:

1. Connecting two Computers
2. Connecting large no. of Computers through world wide web
3. in www mobile devices got added, internet to mobile devices
4. people got Connected to world via Social n/w
5. now every day to day objects are also getting Connect to internet which is called as IOT.

IOT is about extending the power of the internet beyond Computers and Smartphones to a whole range of other things, processes & environments.

IOT is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a n/w without requiring human-to human or human-to-computer interaction.

a dynamic global n/w infrastructure with self Configuring Capabilities (can set themselv up & communicate using Common Communication rule). base on standard and interoperable Communication Protocol where physical & virtual things have identities, Physical attribute &. virtual personalites use intelligant interfaces and are seamlessly integrated into the info n/w often Communicate. data associated with users & their env.

abstract representation → in terms of diagram.

Sensors : Sensors are active devices that measure some variable of the nature or man made environment.

Actuators : an actuator is a mechanized device of various sizes that accomplishes a specified physical action

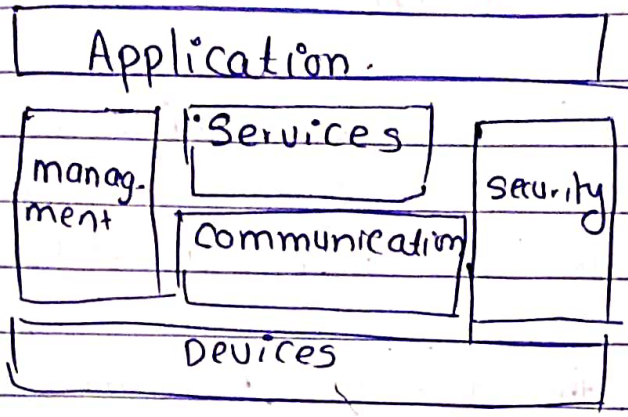
Things in IOT refers to devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities

Logical Design of IOT

logical design of an IOT system refers to an abstract representation of the entities and processes without going into low-level specifics of the implementation.

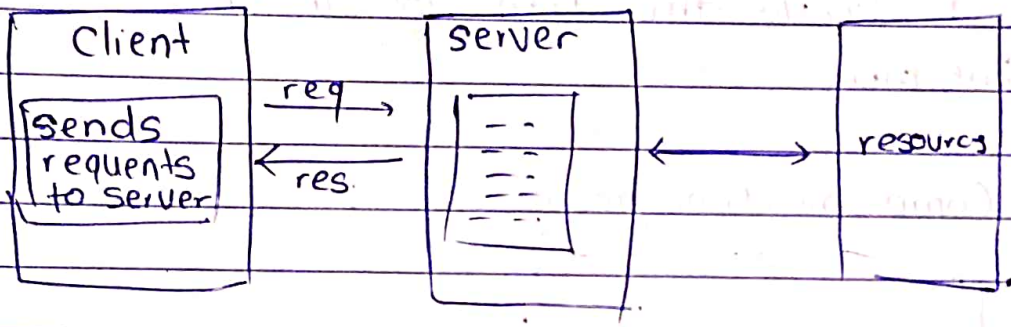
IOT system comprises of a no. of functional blocks that provide the system capabilities for identification, sensing, actuation, communication & managment.

IOT Functional Blocks



IOT Communication model

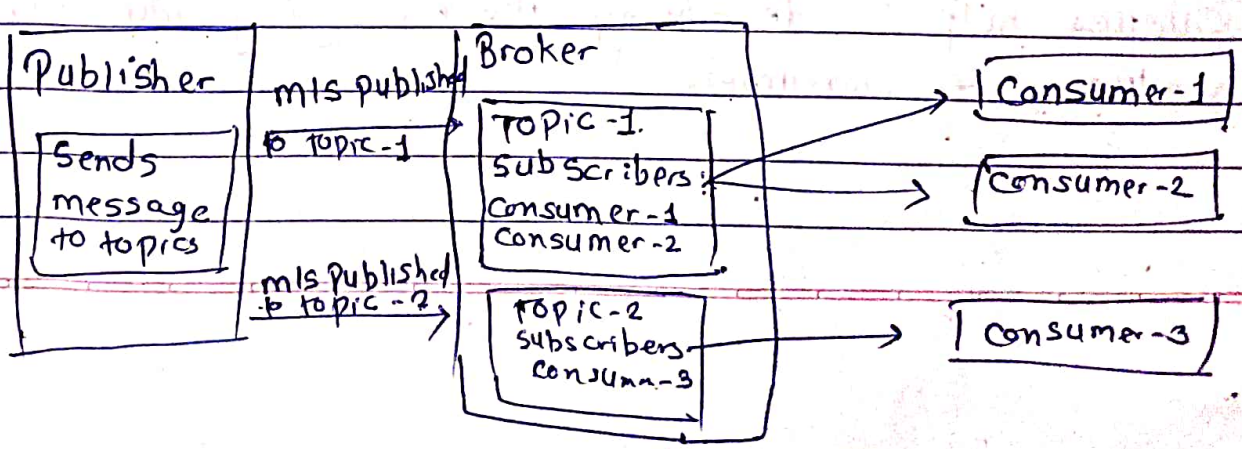
① Request-response model



request-response is a communication model in which client sends request to the server and the server responds to the request

the server receives a request, it decides how to respond, fetches the data, retrieves resource representation, prepare the response and the sends the response to the Client.

② Publish-Subscribe Communication model



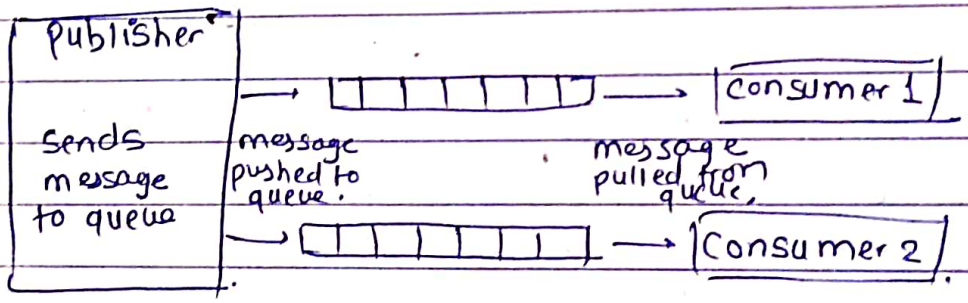
Publish-subscribe is a communication model that involves publishers, brokers & consumers

publishers are the source of data. publishers send the data to the topics which are managed by broker. publishers are not aware about consumers

Consumers subscribe to the topics which are managed by broker

when the broker receives data for a topic from the publisher it sends the data to all the subscribed consumers

③ Push-Pull Communication model.

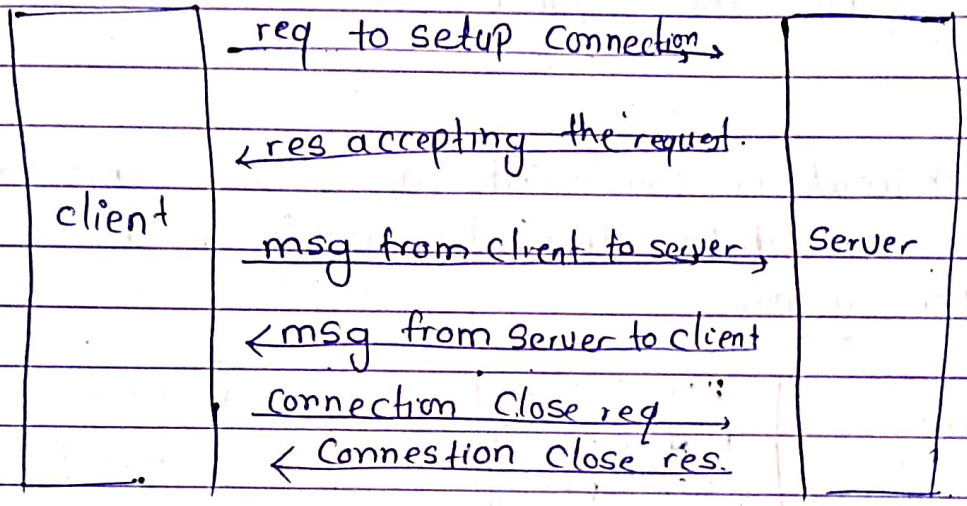


Push-Pull is a communication model in which the data producers push the data to queue and consumers pull the data from the queue. producers do not need to be aware of the consumers.

queues help in decoupling the messaging b/w the producers & consumers

Queues also act as buffer which helps in situation when there is a mismatch b/w the rate at which the producers push data and the rate at which the consumers pull data.

④ Exclusive pair Communication model.



exclusive pair is a bidirectional, fully duplex Communication model that uses a persistant Connection b/w the client and server.

Once the Connection is setup it remains open until the client sends a request to close Connection.

Client & server can send message to each other after Connection setup.

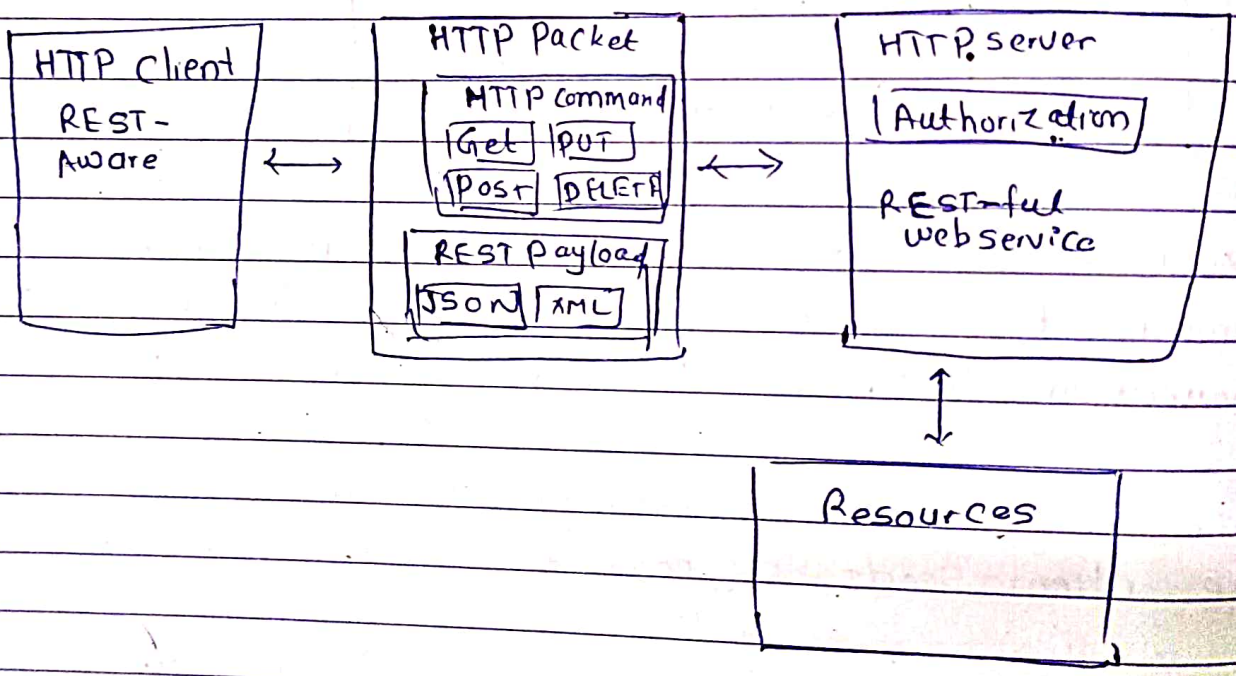
IOT Communication APIs

① REST based Communication

Representational state transfer is a set of architectural principle by which you can design web services & web APIs that focus on system's resources and how resource state are addressed and transferred.

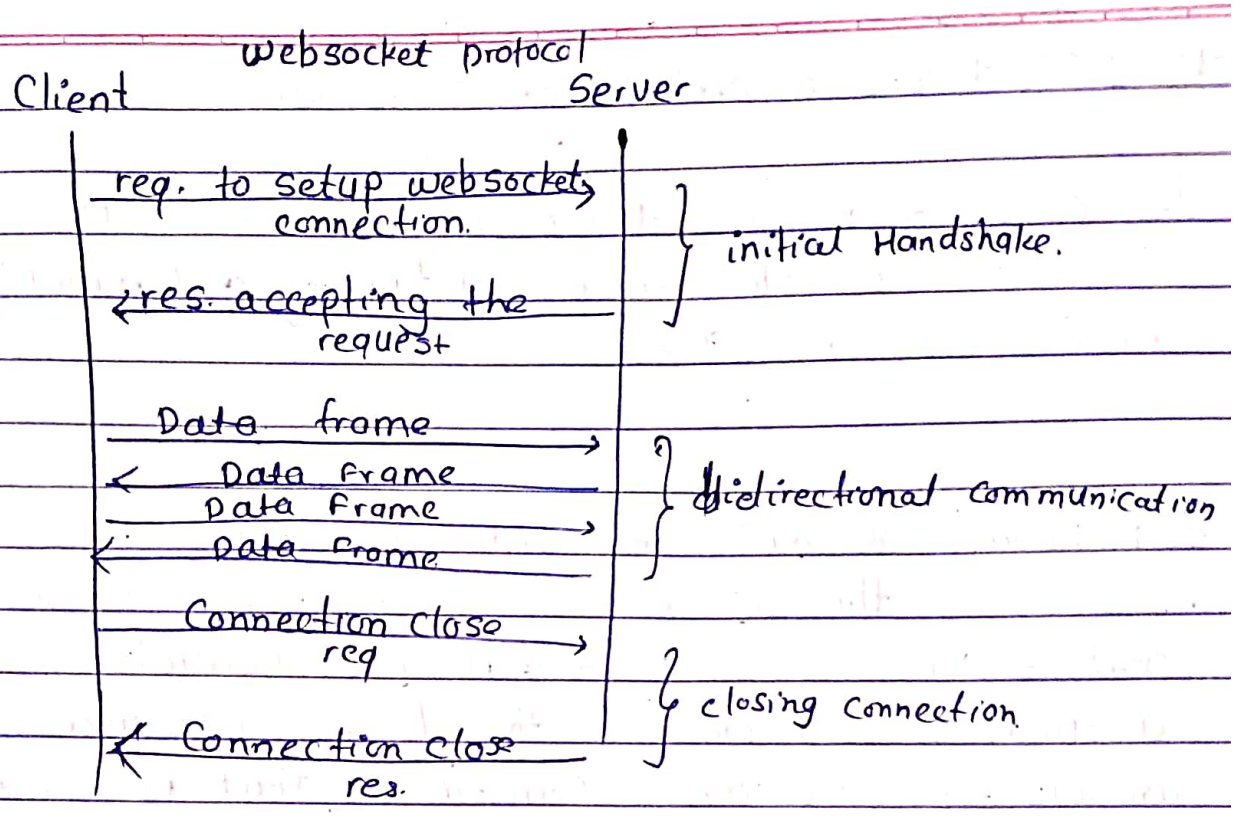
Rest-API follow the request-response communication model

REST architectural constraints apply the components, connectors and data elements within a distributed hypermedia system



② Web Based Communication APIs

- websocket APIs allow bidirectional, full duplex communication blw clients and servers
- websocket API follow the exclusive pair communication model



IOT Enabling Technologies

IOT is enabled by several technologies including wireless Sensor nlw, cloud computing, Big data analytics, embedded systems, security protocols & architectures, Communication protocals, web services, mobile internet & Semantic Search engines

Embedded systems: Embedded system is a Computer system that has Computer hardware and Software embedded to perform Specific task. embedded System range from low Cost miniaturized devices such as digital watches to devices such as digital Cameras, pos terminal, Vending machines, appliances etc.

① Device ② Resource ③ Controller service ④ Data Base.
⑤ Web service ⑥ Analysis Component ⑦ Application

IOT levels & Deployment Templates

① Device - an IOT device allows identification, remote sensing, actuating and remote monitoring capabilities

② Resource : Resource are software components on the IOT device for accessing, processing and storing sensor information or controlling actuators connected to the device. Resources also include the software components that enable nlw access for the device

③ Controller service : Controller service is a native service that runs on the device and interacts with the web services. Controller service sends data from the device to the web service and receives commands from the application (via web services) for controlling the device.

④ Data base : Database can be either local or in the Clould and stores the data generated by the IOT devices.

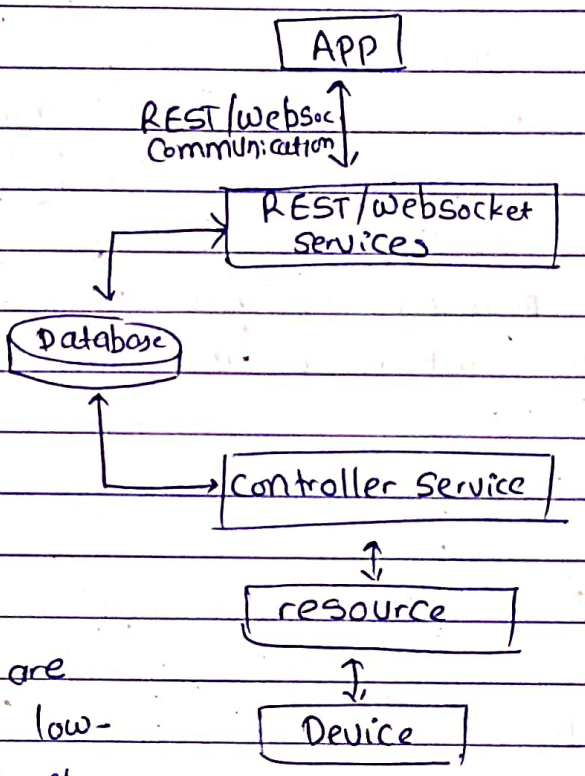
⑤ Web Service : Serves as a link blw IOT device, application, database and analysis components. Web services can be either implemented using HTTP & REST principle or using websocket.

⑥ Analysis Component - responsible for analyzing the IOT data and generate results in a form which are easy for the user to understand.

⑦ Application : Provide an interface that the users can use to control and monitor various aspects of the IOT system. applications also allow users to view the system status & view the processed data.

IOT Level-1

level-1 IOT system has a single node that performs sensing and actuation stores data, performs analysis and hosts the application.



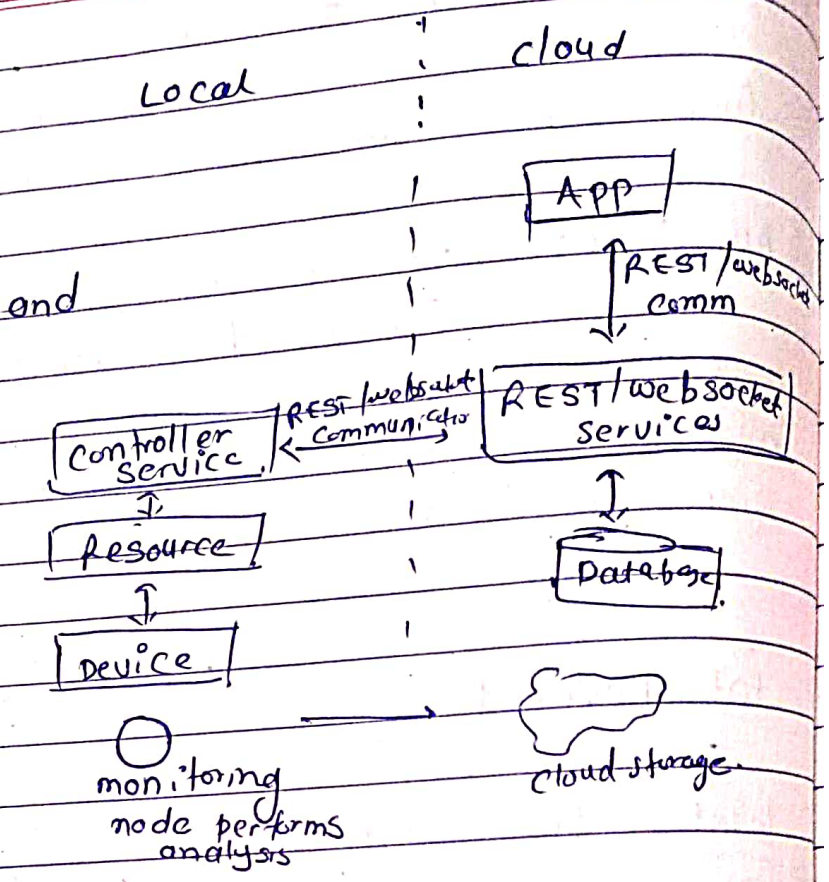
level-1 IOT systems are suitable for modeling low-cost and low-complexity solutions where the data involved is not big and the analysis requirements are not Computationally intensive

IOT level 2

Level-2 IOT system has a single node that performs sensing/actuation and local analysis.

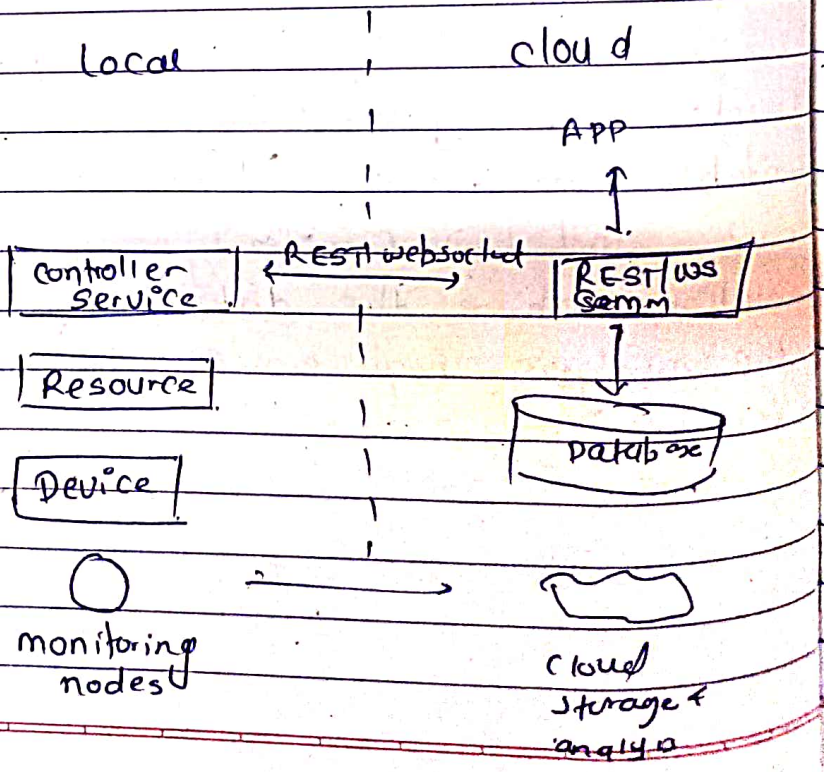
Data is stored in cloud and application is usually cloud-based

level-2 IOT systems are suitable for solutions where the data involved is big however the primary analysis requirement is not computationally intensive and can be done locally itself.



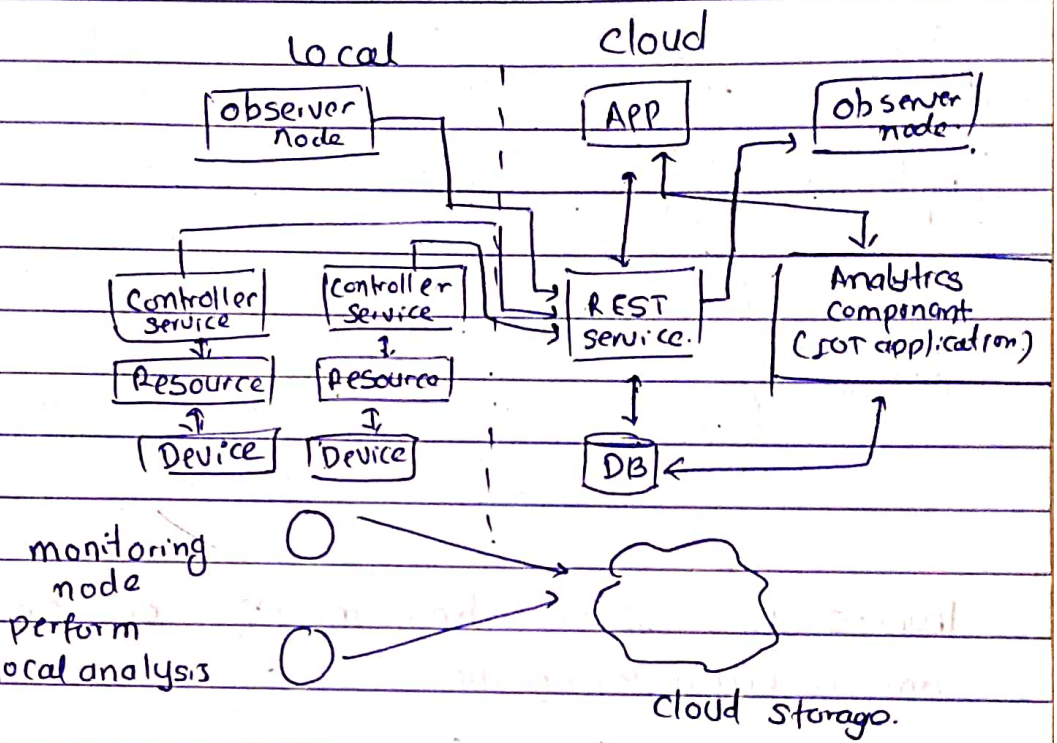
IOT level 3

a level-3 IOT system has a single node. Data is stored and analyzed in clould and application is cloud-based.



level-3 IOT systems are suitable for solutions where the data involved is big and the analysis requirements are computationally intensive.

IOT level-4

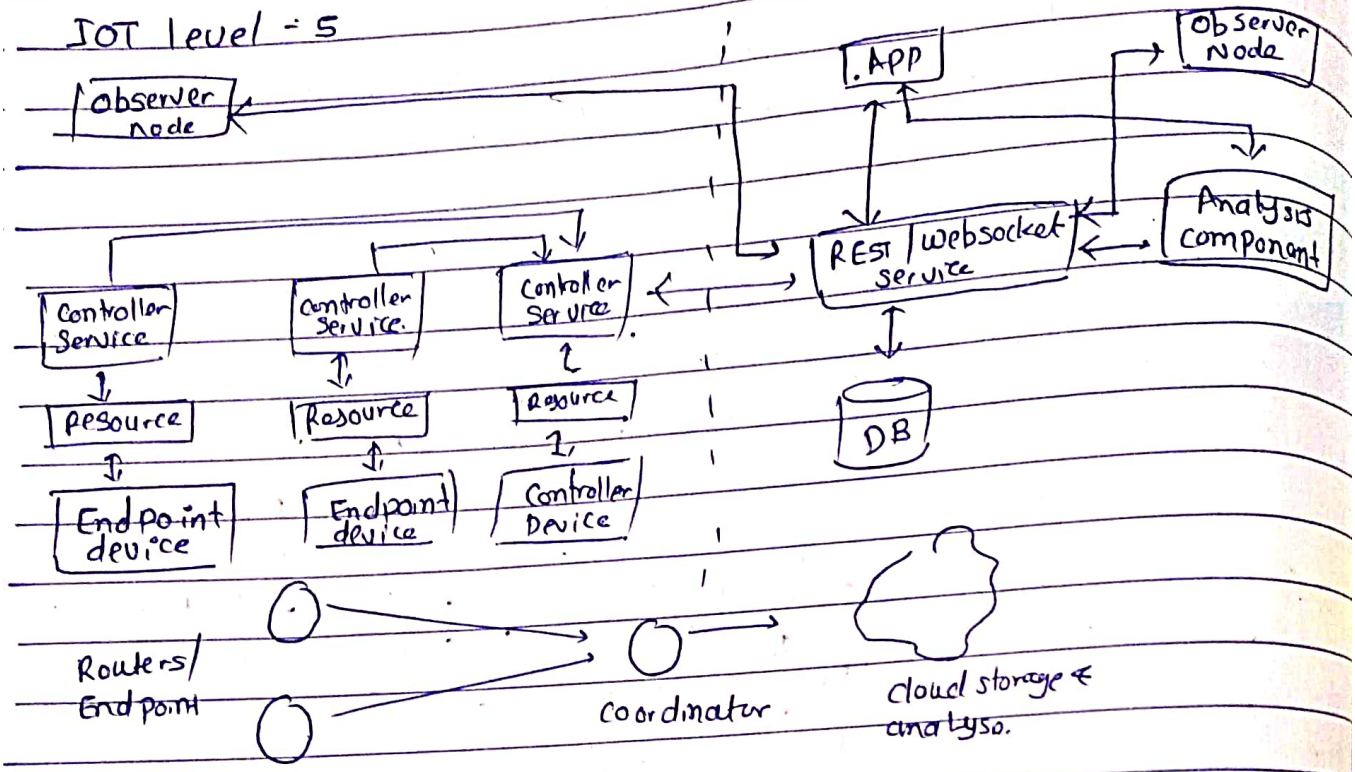


A level-4 IOT system has multiple nodes that perform local analysis. Data is stored in cloud and application is cloud based

level-4 contains local & cloud-based observer nodes which can subscribe to and receive information collected in the cloud from IOT devices

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.

IOT level - 5



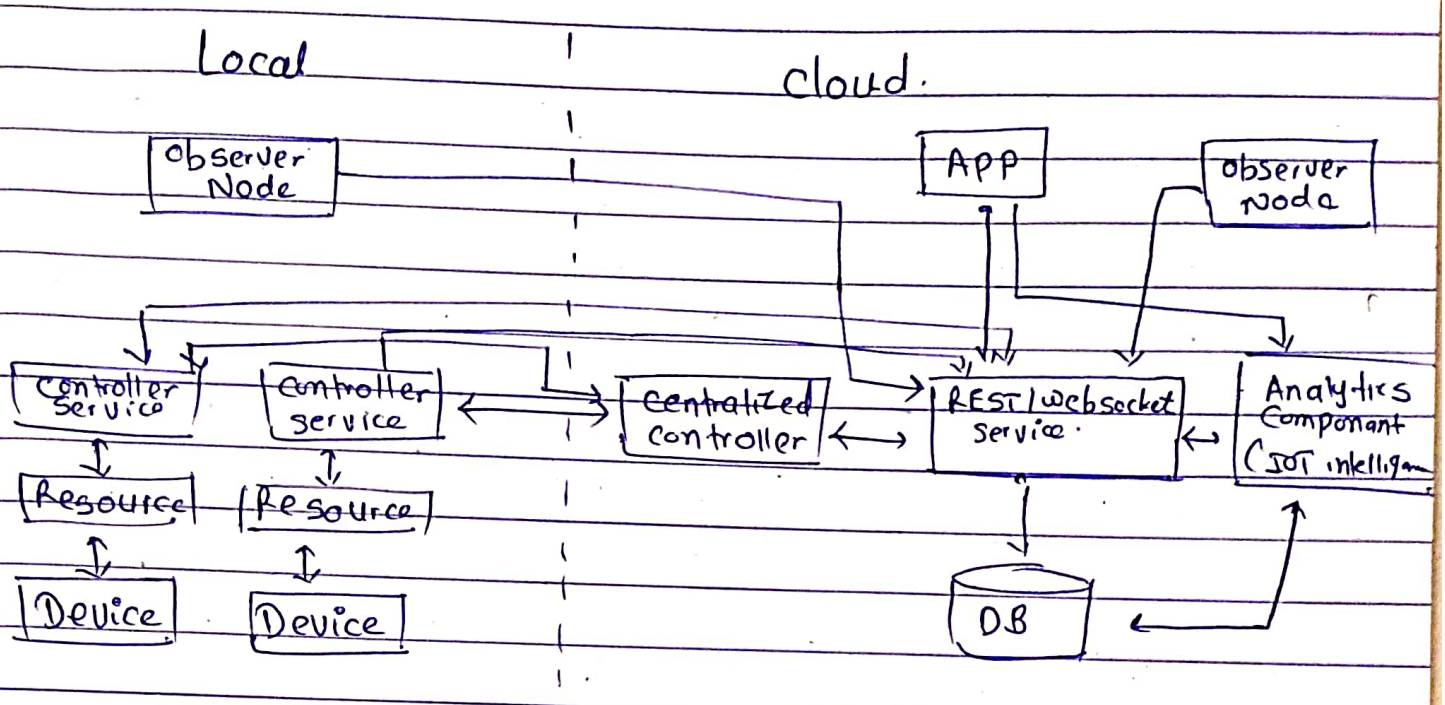
level-5 IOT system has multiple end nodes and one co-ordinator node

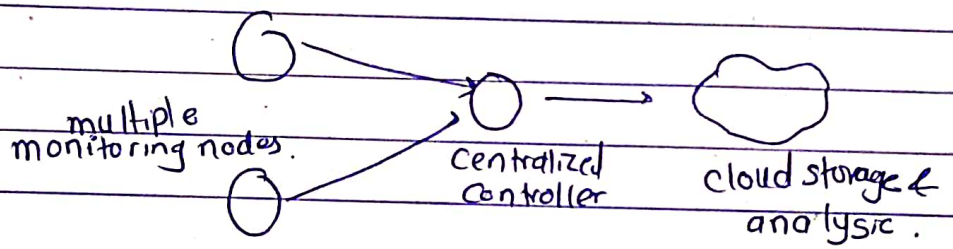
end nodes that perform sensing and actuation coordinator node collects data from end nodes and sends to the cloud

Data is stored and analyzed in the cloud and application is cloud based

level-5 IOT systems are suitable for solutions based on wireless sensor networks in which the data involved is big and the analysis requirements are computationally intensive

IOT level-6





level 6 IOT system has multiple independent end nodes that perform sensing and actuation and send data to the cloud.

Data is stored in cloud and application is cloud based

The analytics component analyzes the data and stores the results in cloud database

The results are visualized with the cloud base application

Centralized Controller is aware of the status of all the end nodes and sends control commands to the nodes.

IOT n/w Architecture and Design

challenge

① Scale

The scale of IOT endpoints such as sensors & devices, is vastly greater than that of traditional IT n/w. this explosion in the no. of connected devices is due to the diverse and widespread deployment of sensors and other IOT devices in industries like manufacturing, healthcare, transportation and smart cities.

IPV4 address space has reached exhaustion and is unable to meet IOT's scalability requirements. IT networks still rely on IPV4 to cope with limitation of IPV4 NAT (N/w address Translation) techniques are used but NAT introduce complexity

IPV6 is essential for IOT

② Security

Physical Exposure of IOT Devices

IOT devices, deployed on wireless sensor n/w (WSNs) are installed in location that are physically exposed physical exposure makes them vulnerable to various security threats

Device-level authentication → must be able to authenticate itself to the n/w to ensure that only authorized devices are permitted to connect

Link encryption - Data transmitted b/w IOT devices and the n/w should be encrypted to protect it from being intercepted or altered

zero touch deployment - this approach allows devices to be automatically configured and securly integrated into the n/w without manual intervention.

③ Devices and nlw Constraints

IOT devices and nlw are often limited by various resource constraints such as power, CPU, memory and link speed Considering the massive scale of IOT IOT nlw are lossy and can only support minimal data rates

New last-mile wireless technologies are needed to support constrained IOT devices over long distances nlw is constrained, modifications need to be made to traditional nlw layer transport mechanisms

④ Massive volume of data generated

Sensors generate a massive amount of data on a daily basis, causing nlw bottlenecks and slow analytics in the cloud

Data analytics capabilities need to be distributed throughout the IOT nlw from the edge to the cloud

⑤ Support for legacy devices

⑥ The need for data to be analyzed in real time

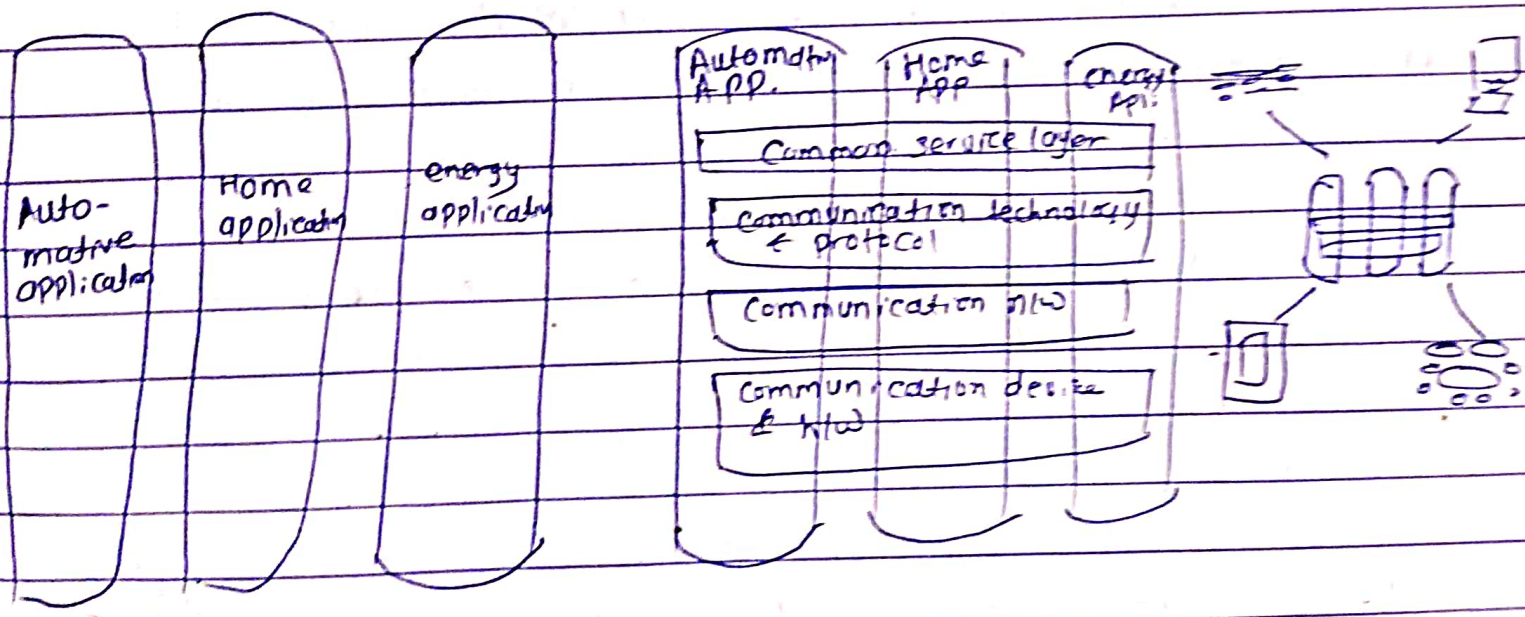
Traditional IT n/w performs scheduled batch processing of data. IOT data needs to be analyzed and responded to in real-time

Analytics software needs to be positioned closer to the edge and should support real-time streaming analytics

Comparing IOT architectures

① One M2M architecture

One M2M is like a translator that allows different systems to communicate smoothly over an IOT n/w. it uses a set of rules (RESTful APIs) to ensure that these diffrent systems can talk to each other in a Consistent and standardized way



three major domains

① Application layer

One M2M architecture gives major attention to Connectivity b/w devices and their application

This domain includes the application-layer protocol and attempts to standardize northbound API defination for interaction with business intelligence (BI) system

② Service layer

This layer includes the physical n/w that the IOT application run on, the underlying management protocols & the hardware

eg

backhaul Communication via cellular transmitting data from small n/w to large or main internet

it provides some common services

Conceptual layer adds APIs & middleware supporting third party services & applications

③ n/w layer

This is the Communication domain for the IOT device & endpoints

includes the devices themselves & the Communication n/w that links them

→ Application layer

end-users interacts with the IoT systems.
it includes the software applications that provide specific service.

this layer includes user interfaces, dashboard, mobile apps & web applications that display data collected from IoT devices

eg in smart home application layer include app on your mobile.

Service layer

it's middleware blw application layer & service layer provides servite like data storage, processing and managment this layer ensures that data is accessible, interpretable and useful for application layer.

includes data managment services, APIs, database, cloud computing platforms and analytics engines.

eg in smart city, this layer includes cloud on which all data stored

Network layer

responsible for connecting IoT devices to each other and to the internet manages the communication blw devices and infrastructure needed to support it.

includes commonication protocols, gateways & nlw infrastructure like routers and base station

eg wearable fitness tracker, nlw layer would be responsible for transmitting data from the device to smartphone app via bluthooth.

7 level IOT reference model by IOT world Forum

⑦ Collaboration & processes
(involving people & Business process)

⑥ Application
(reporting, analytics, control)

⑤ Data abstraction (aggregation & access)

④ Data accumulation (storage)

③ Edge Computing (Data element analysis & transformation)

② Connectivity (communication & processing units)

① Physical devices & Controllers (Things in IOT)

① Physical device & controllers layer
The various endpoint devices and sensors that send & receive information
Size of these things can range from almost microscopic sensors to giant machine in a factory
primary function is generating data and being capable of being queried / controlled over n/w

② Connectivity layer
reliablity & transmission of data are imp function, more specific transmission of data b/w layer 1 and n/w and b/w n/w and information processing that occurs at layer 3, switching & routing, translation b/w protocols.

③ Edge Computing
→ also called as Fog layer
→ Focus on data reduction and converting nlw data flows into information that is ready for storage and processing by higher layers
→ Information processing is initiated as early and as close to the edge of the nlw as possible, processing starts where data generated, early processing helps to take quick decision and real time analysis
→ filtering and aggregation of data is performed
→ data to be reformatted or decoded making further analysis easis.

④ layer 4 : Data accumulation layer
Captures data and stores it so it is usable by applications when necessary, Convert event based to query based processing (event based → trigger or action happen after a perticular activity) (query-based → data is stored, computation or analyze happen when user fires a query)

⑤ layer 5 : Data obstraction layer
Simplifies and organizes data from different sources so that it all work together smoothly.
→ takes data from diffrent format and convert into common
→ make sure all uses same terminology or labels
→ check if necessary data is present & ntg imp missing
→ brings all data together, even if it is at diffrent ~~layer~~ location with the help of virtualization it present all data at same place.

⑤ Application layer

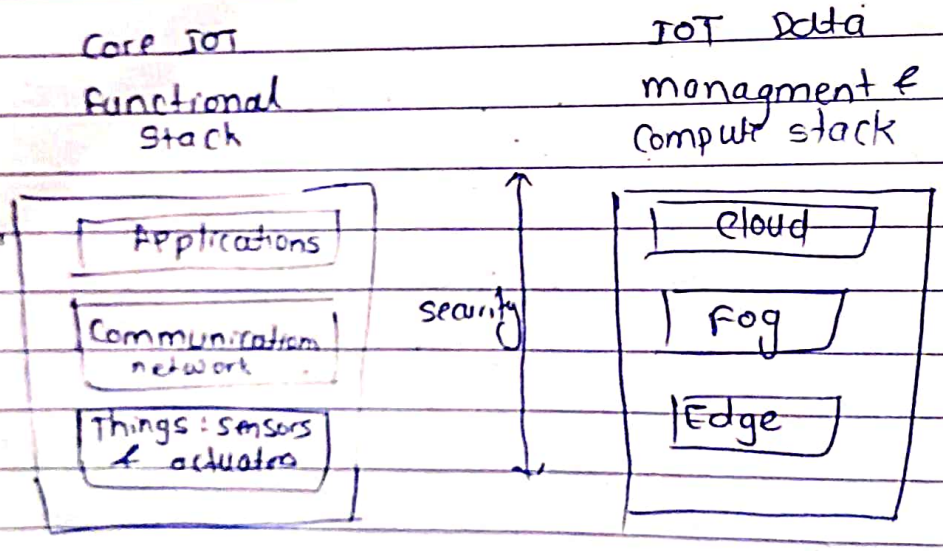
Interprets data using software applications, applications may monitor, control and provide reports based on the analysis of the data

④ Collaboration & processes layer

Consumes & shares the application information. Collaborating on & communication IOT information often require multiple steps, it makes IOT useful.

Simplified IOT architecture

presented by two parallel stacks



The nlw Communication layer of the IOT stack itself involves a significant amount of details and vast technologies.

there is hetogeneity in IOT devices, still nlw communication layer bring them together, provide gateway and back haul technologies and

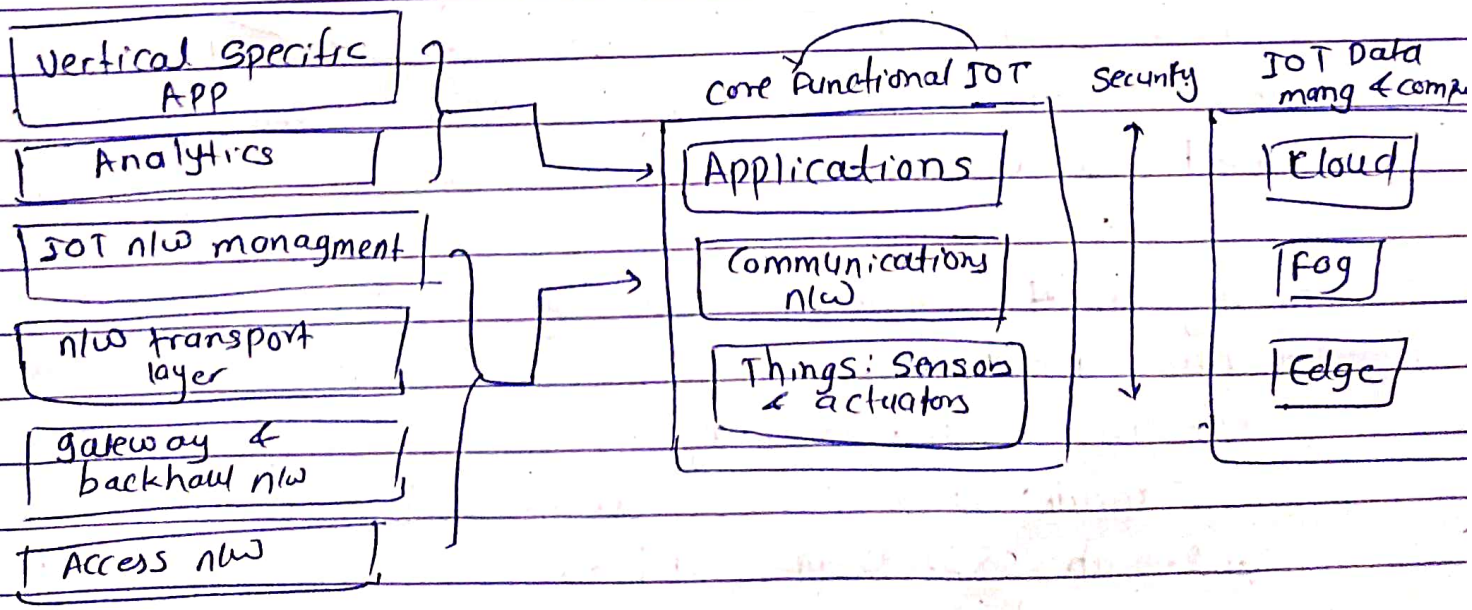
ultimately bring data back to a central location

n/w btw gateway and the data centre is composed of traditional technologies which include tunneling, VPN, IP-based quality of service (QOS), conventional layer 3 routing protocols etc

unlike IT systems, IOT systems often need to analyze and manage data at multiple levels not just in the Cloud or a central data center. at the starting and at cloud too. this tiered approach is necessary because IOT systems often deal with large amount of data

Three data managment layers are
① edge layer (data mana. within the sensor)
② Fog layer (data manag. in the gateway & transd n/w)
③ Cloud layer (data manag. in the cloud or central data)

Expanded view of the simplified IOT Architecuture



Core IOT Functional stack

IOT nlw is build around "Things" i.e Smart objects they are called smart because they use a Combination of Contextual information and configured goals to perform actions

Smart objects does not rely on external systems for its actions. but things interact with external System to report information that the smart object Collects

Several Componants have to work together for an IOT nlw to be operational

"Things" layer

physical devices need to be fit the constraints of the environment in which they are deployed and provide information needed

"Communications nlw layer"

when smart objects are not self-contained (depends on external system for action) they need to communicate with the external system

mostly used wireless technology

it has 4 sublayers

① access nlw sub layer

made up of wireless technologies such as 802.11ah, 802.15.4g and LoRa

sensors Connected to the access nlw may be also wired

(ii) Gateways & backhaul nlw sub layer:

gateways communicates directly with smart objects.

the role of gateway is to forward the collected information through a longer range medium (called the backhaul) to a headend central station where the information is processed

(iii) Network transport sub layer

For communication to be successful, nlw and transport layer protocols such as IP and UDP must be implemented to support variety of devices to connect and media to use

(iv) IOT nlw managment sub layer

additional protocols must be in place to allow the headend applications to exchange data with sensors.

" Application & analytics layer.

→ upper layer, application analyze the data
→ controls the smart object → take the intelligent decision based on collected information, give instruction to analyzed systems, things to change behaviour or patterns according to analyzed condition

(See after edge computing)

Edge Computing

- Computing resides in the sensors & IOT devices
- new classes of IOT endpoints have enough Compute capabilities to perform least low-level analytic and filtering to make basic decision.

Layer 1: Things: Sensors & Actuators layer

① Battery-powered or power Connected → Sensors & actuators Can either be powered by batteries or Connected to a power source

② mobile or static

③ low or high reporting frequency

④ Simle or rich data → the data captured can range from simple (eg binary data, basic metric) to rich (complex datasets)

⑤ report range - distance over which sensor or actuator Can communicate or report data

⑥ object density per cell - no. of sensors/devices present in perticular area.

Layer 2 : Communication nlw layer

Physical env in which the IOT devices are deployed are diffrent from IT nlw

Sensors are manufactured in such way that they Can tolerate extreme conditions.

Sublayer

each technology was designed based on what to connect, where to connect, who much data to transport at which interval and over what distance

based on above, frequency band that was expected to be most suitable, the frame structure according to data pattern (packet size & commun. layer) and possible topologies

range blw smart object & information collector plays imp role in determing the access technology

PAN (personal area n/w)

→ Scale of few meters, personal space around person → bluetooth common wireless technology for this scale

HAN (home area n/w)
→ Scale of few ten of meters
→ common wireless technologies for IOT tech. ZigBee & bluetooth low energy (BLE)

NAN (neighborhood area n/w)
→ scale of few hundreds of meters
→ NAN is group of house unints from which data collected

FAN (Field area n/w)
→ scale of several ten meters to several 100 m
→ FAN outdoor area larger than single group of house units.
– group of NAN

LAN (local area n/w)
→ scale up to 100m

amount of data to carry over a given time period along with correlated power consumption (driving possible limitations in mobility & range) determines the wireless cell size & structure

point to point topologies
one point to communicate with another point

point to multipoint topologies
one point to communicate with more than one other point.
IOT technologies in which more than one gateways communicate with multiple smart objects are in this category.

When devices are connected & implement protocol stack functions they can form a peer-to-peer nlw

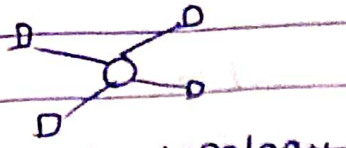
eg
- temperature sensors in each zone sends data to central point where temperature is displayed and controlled
- sensors donot communicate with another room sensor
- nlw forms a star topology
- In IEEE 802.15.4 standard, central point is called a coordinator for the nlw
- with this type of deployment, each sensor is not intended to do anything other than communicate with the co-ordinator in a master/slave type of relationship

→ sensor can implement a subset of protocol functions to perform just specialized part (communication with the co-ordinator)
→ such a device called a reduced-function device (RFD), it can't be coordinator
cannot implement direct communications to another RFD

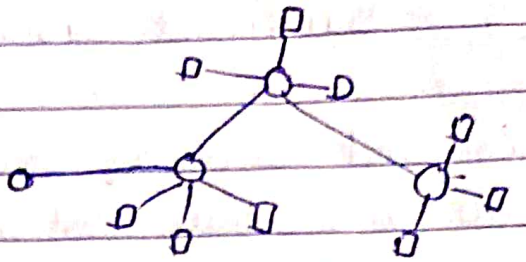
→ Co-ordinator that implements the full nlw functions is called. by contrast a full function device (FFD)

→ an FFD can communicate directly with another/multiple FFD forming peer-to-peer connection.

→ Topologies where each FFD has a unique path to another FFD are called cluster tree topologies



star topology



clusterd stars

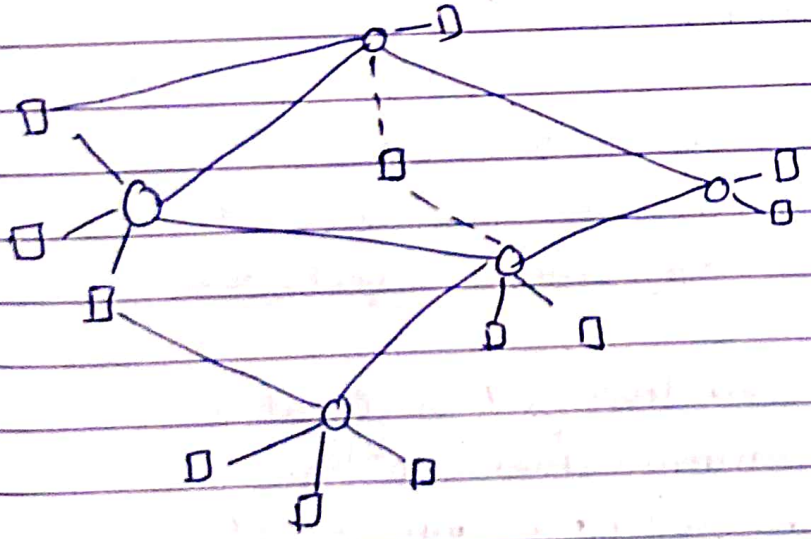
○ → FFD

□ → RFD

point-to-multipoint technologies allow a node to communicate more than one node / more than one paths to another nodes forming mesh topology.

these links can be used to exchange information blw nodes or to extend the range of the communication link.

mesh nlw are redundant, disappearance of one node does not necessarily interupt nlw communication.



Gateways & Backhaul Sublayer

→ Data collected from a smart object may need to fwd to a Central station where it is processed
→ Stations are at diffrent location from the smart object, through a access technology needs to be forworded to another medium (backhaul) & transported to the central station
→ gatway is incharge of intermediate Communication
→ Smart obj are static or mobile at some range
→ Dedicated short-range Communication (DSRC) allows vechicle-to-vehicle & vehicle to infrastructure Communication
→ if env is stable (factory, oil & gas fields) than ethernet backhaul is used else wireless technology

Nlw Transport layer

IoT nlw managment sublayer

- IP, TCP & UDP brings Connectivity to IoT nlw
- upper layer protocols need to take care of data transmission blw the smart objects & other systems
- multiple protocols have been leveraged or Created to solve IoT data Communication problems.
- Some nlw rely on Push model or Pull model.

- HTTP is also suggested for data transfer phase
- Sensors could use client side for establishing connection to the IOT central application
- but HTTP was not designed to operate in constrained environments with low memory, low power & low bandwidth

- websocket is HTML5 specification, provides a simple bidirectional connection over a single connection
- Some IOT solutions use websocket to manage the connection blw smart object & external application.

- Extensible Messaging & presence protocal (XMPP)
- based on instant messaging & presence
- allows the exchange of data blw two or more systems and supports presence and contact list maintenance
- handle publish/subscribe, because of this distribution of information to multiple device becomes easy

- Constrained Application protocal (COAP)
- COAp uses some methods similar to those of HTTP (get, post, put & Delete) but implements a shorter list, this limiting the size of the header
- COAp also runs on UDP
- COAp adds the feature of observation, observation allows the streaming of state change as they occur, without requiring the receiver to query for these changes.

- Message Queue Telemetry Transport (MQTT)
- MQTT use broker based architecture.
- Sensor can be set to be an MQTT publisher (publishes a piece of information), application that needs to receive the information can be set as the MQTT subscriber and any intermediary system can be set as broker to relay information b/w the publisher & the subscriber(s)
- MQTT runs over TCP

(back ufrom where came)

Fog Computing

- Fog Services are typically accomplished very close to the edge device, sitting as close to the IOT endpoints as possible

- Fog nodes have contextual awarness of the sensors it is managing because of its geographic proximity to those sensors
analysis the message received from sensors and send only the relevant information over the backhaul n/w to the cloud

because of Fog layer devices can be monitored, controlled & analyzed in real time without the need to wait for communication from the central analytics & application servers in the cloud

Hierarchy of Edge, Fog & cloud

- Edge & Fog Computing cannot replace the cloud
- this model suggests a hierarchical organization of nlw, compute & data storage resource.
- at each stage data is collected, analyzed & responded to when necessary, according to the capabilites of the resources to each layer
-

Analytic vs Control applications

① Analytic applications

this type of application collects data from multiple smart objects, process it & display the results.

results derived cannot be obtained from solely looking at information displayed by a single smart objects

② Control Applications

Controls the behaviour of smart objects or the objects related to smart objects

Control applications are very useful for controlling complex aspects of IOT nlw with a logic that cannot be programmed inside single IOT object.

Data vs nlw analytics

① Data analytics

examining the data gathered from smart devices to offer useful insights

eg dashbord display alarm when wt sensor delects that the shelf is empty in store

② nlw analytics

IOT systems are built around smart objects connected to the nlw

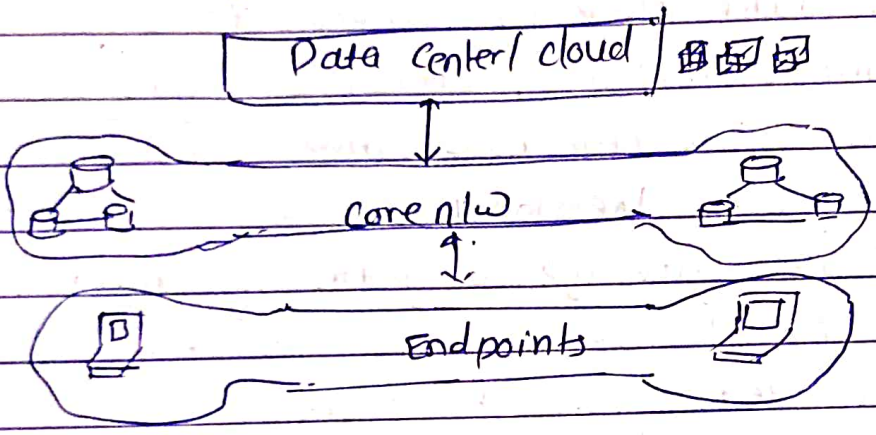
a loss or degradation in connectivity affect efficiency of system.

IOT Data managment & compute stack

data generated by sensors is unstructured and very little use on its own.

Processing location is outside smart object generally it is cloud

Smart objects need to connect to cloud and data processing is centralized



IOT issues to be addressed

1. Bandwidth in last-mile IOT n/w is very limited
2. latency can be very high
3. n/w backhaul from the gateways can be unreliable and often depends on 3G/LTE or even satellite links
4. volume of data transmitted over the backhaul. Can be high
5. Big data is getting bigger.

Fog Computing

→ to solve the problems distribute data managment throughout the IOT systems as close to the edge of the IP nlw as possible

→ any device with Computing, storage and nlw Connectivity Can be a fog node

→ analyzing IOT data close to where it is collected minimizes latency, offloads gigabytes of nlw traffic from the core nlw, keep sensitive data inside the local nlw

→ fog node allows intelligence gathering and control from the closest possible point while doing so performance increases

Characteristics

① Contextual location awareness and low latency
② Geographic distribution
③ Deployment near IOT endpoints
④ wireless Communication blw the fog and the IOT endpoints
⑤ real time interaction