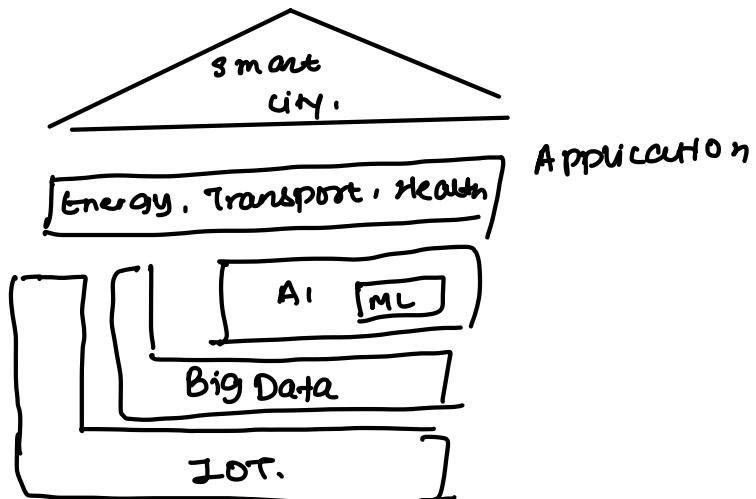


## Revision.

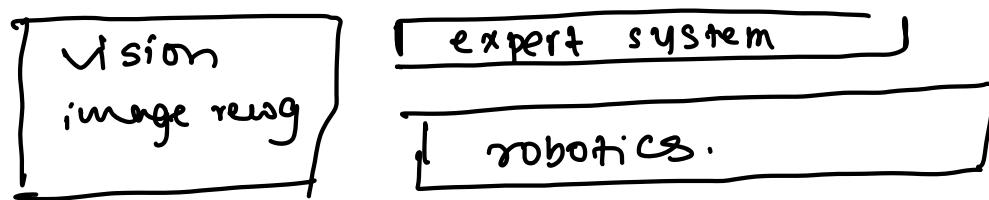
Smart city - To improve, city must become smart & intelligent.

Healthcare - Healthcare has improved Govt. since adoption of AI after epidemic in 2019.

Smart city Architecture -



Categorisation of AI in smart city.



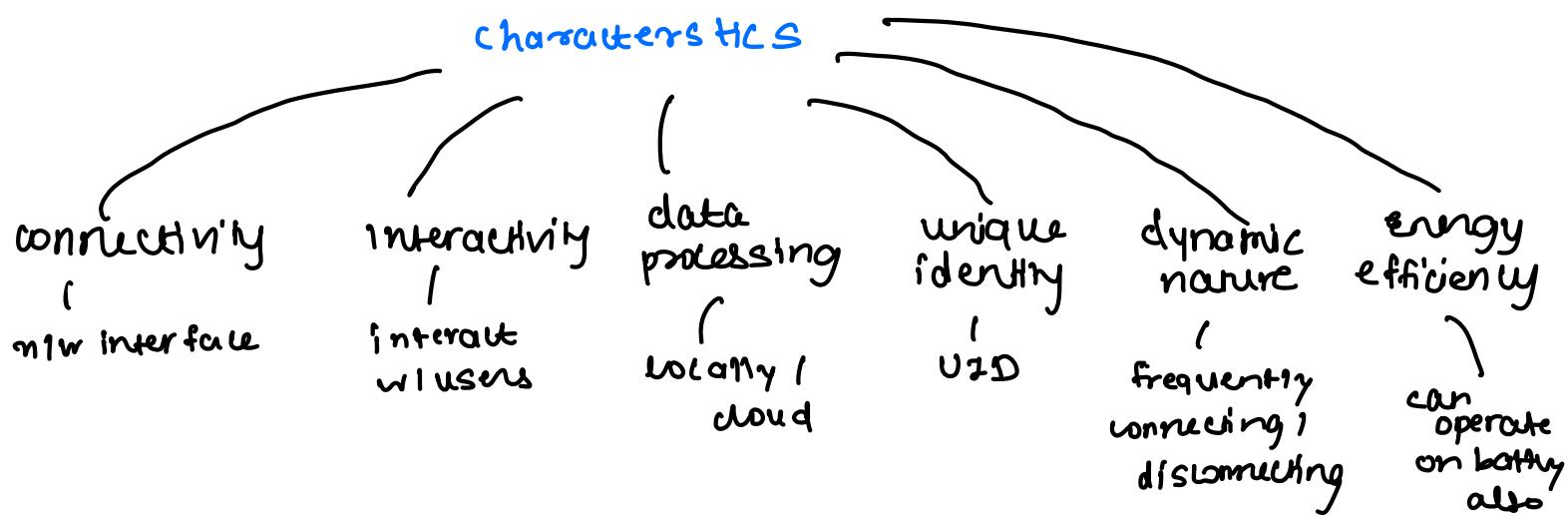
## AI implementation.

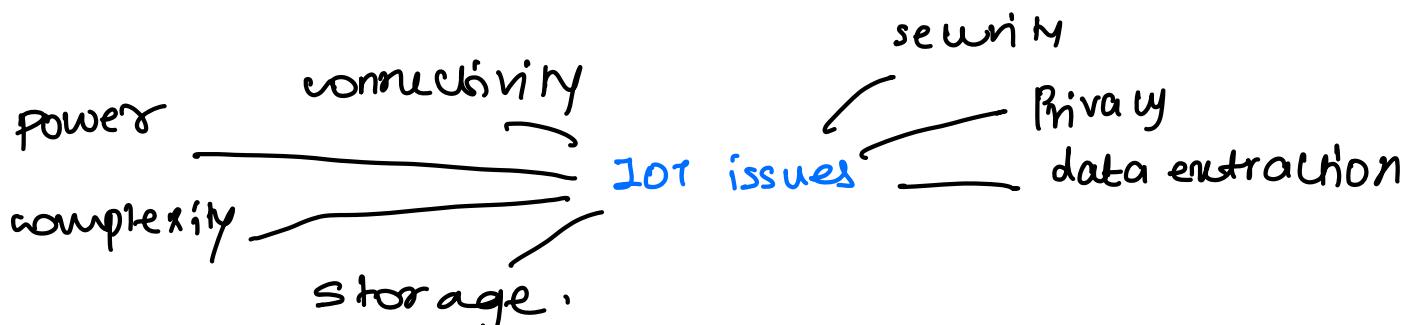
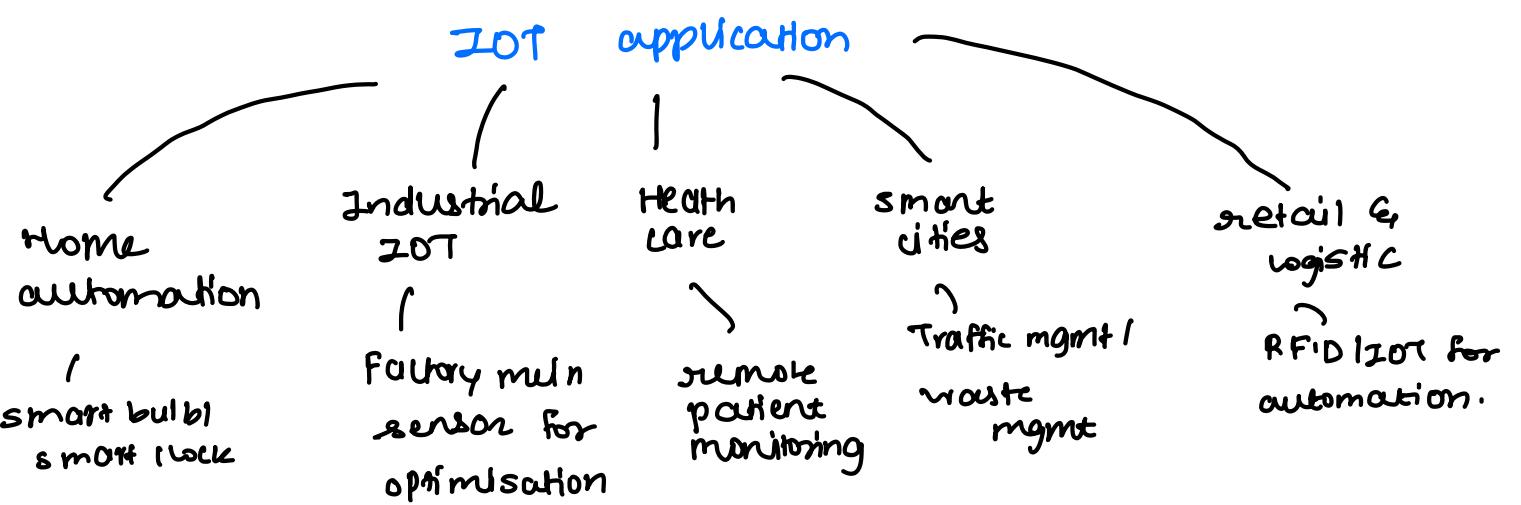
- 1) smart mobility  
Traffic management.  
(Intelligent Transportation)  
learning paradigm for digital native gen
- 2) Education.  
(smart class, VR-based)  
wearable Tech
- 3) Healthcare  
integrated sensor displays
- 4) Environment  
improve decision-making.
- 5) Governance  
improve QoL.
- 6) living & Infrastructure.  
Tech innovation.
- 7) Economy.  
(smart shopping)

S E N T G L E

## Unit - I

IOT - physical devices with sensor, SW & network connectivity

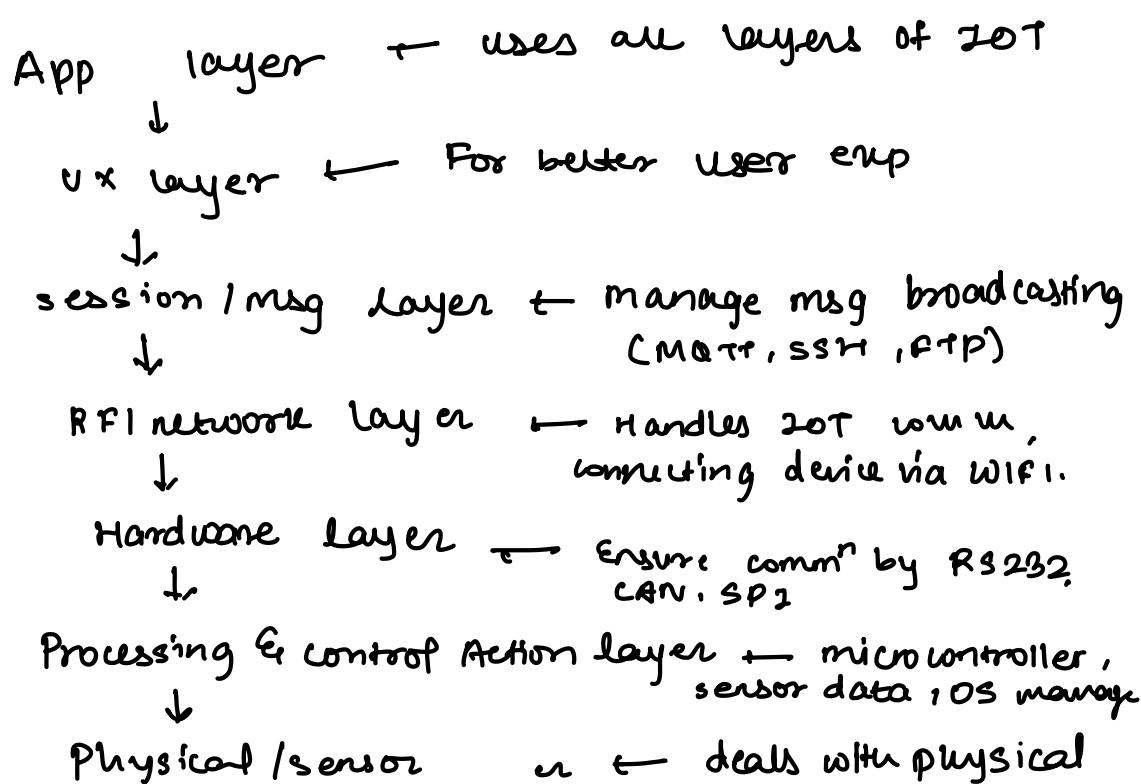




**sensor**

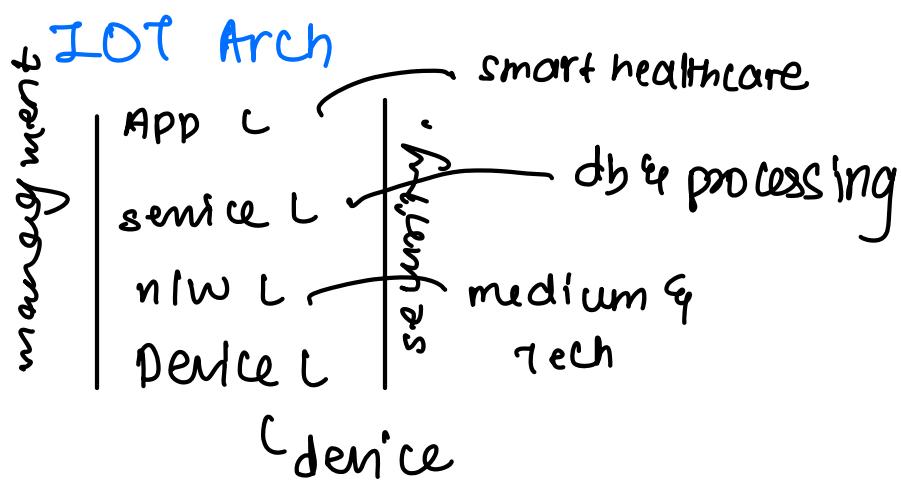
- active - Jo which emit wave & use detect wave e.g. Object detection (RADAR)
- passive - Jo which emit no wave & only detect incoming signal e.g. Thermal light sensor

## IOT stack layer:



# Recommendation on IoT research

- ① Security & Privacy
- ② Energy efficient IoT
- ③ 5G & IoT encryption
- ④ Edge computing & AI in IoT.
- ⑤ Standardization & Interoperability.



functional block of IoT Arch.

App ↗ cloud & App  
| connect sensor  
Gateway ↗ n/w to Internet  
Processor ↗ Brain of IoT  
Sensor ↗ non-electrical  
to elect for processing

## IoT Enabling tech

Tech that help in acquiring data - **sensor**

Tech that help in analysing data - **cloud computing**

Tech that help in taking decision - **Big data analytic**

Tech that help in enhancing privacy - **comms protoc.**

## IoT Physical design

Hardware (sensor, actuator)

middleware

(on-demand storage & computing data)

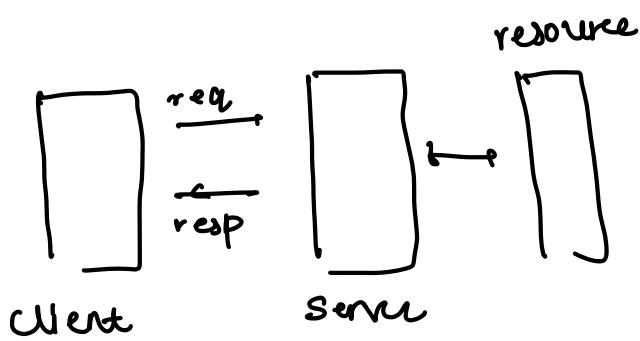
Presentation

(offer visualisation

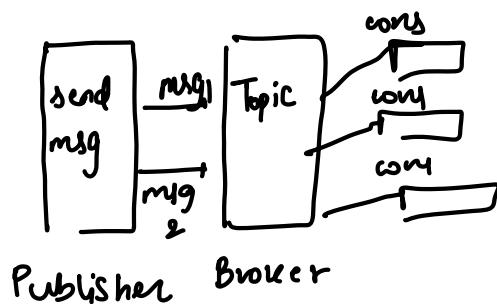
& interpretation)

# logical model of IoT

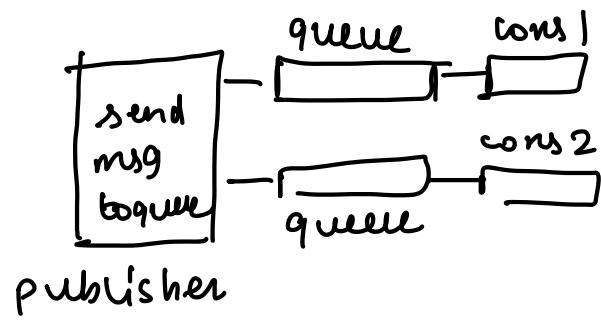
## Request-response



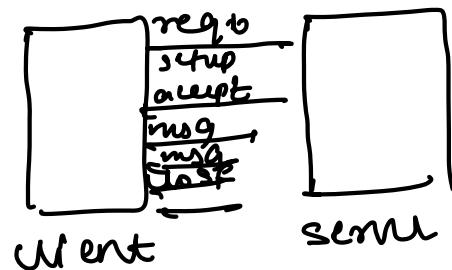
## Publish-subscribe



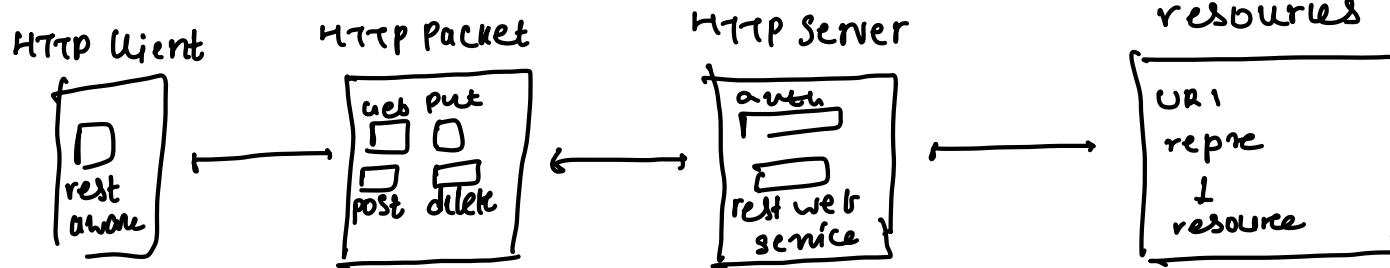
## Push-pull



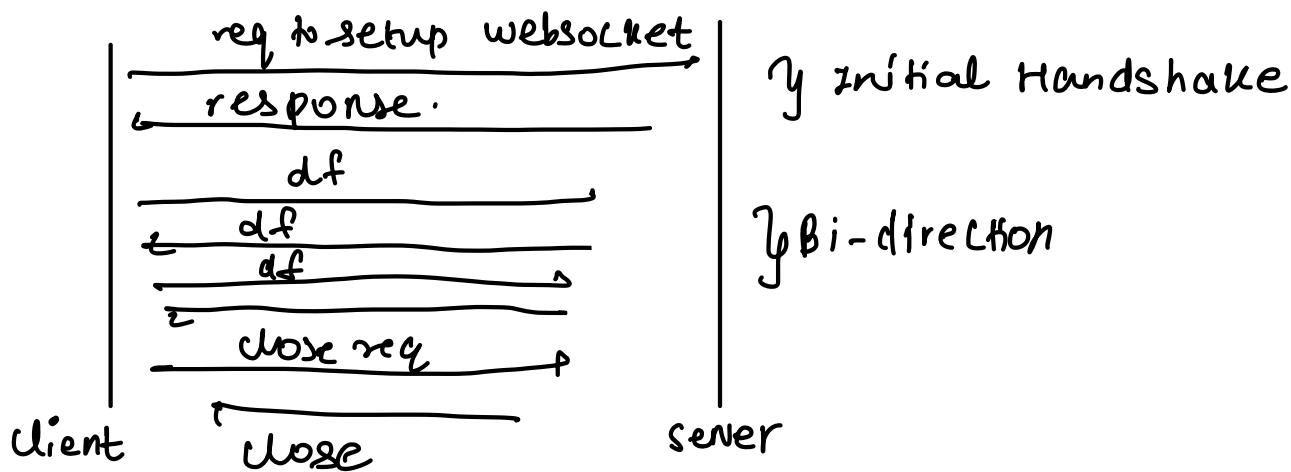
## Exclusive pair



## rest based API



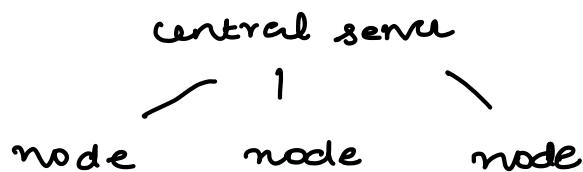
## websocket



## Urvil of IOT:

- 1 - minimal complexity → one sensor → data local
- 2 - slightly more complex → data → cloud → freq of ↑ → Analysis local sensing → storage cloud
- 3 - same as 2 but analysis also cloud → controlled by cloud
- 4 - more data due to more nodes → node upload data to cloud
- 5 - Even more, more nodes → complex more data → entirely cloud

## WSN (wireless sensor netw)



## RFID

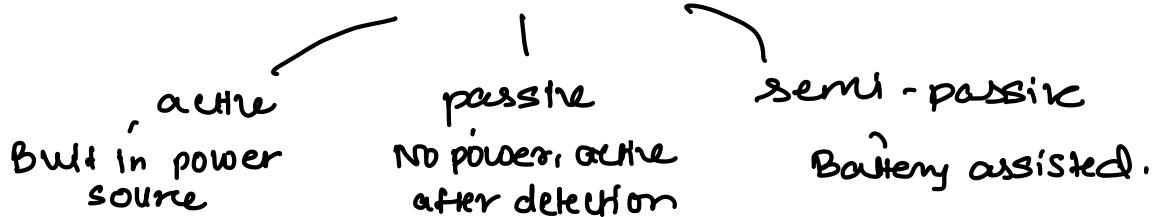
RFID reader

]]]  
radio wave

radio freq. identification

- contains product info
- reader collects data.
- Antenna detect nearby RFID tag.
- data sent to db.

## Types



## component

Microchip

- unique ID
- small amt of memory.
- passive

Antenna

- made of conductive material
- transmit data when read by antenna
- converts waves into readable signal.

Range

low  
High  
Ultra-high

1-10cm

10cm-1m

upto 12m

speed

low

low → mod

mod.

common uses.

animal tracking

contactless payment

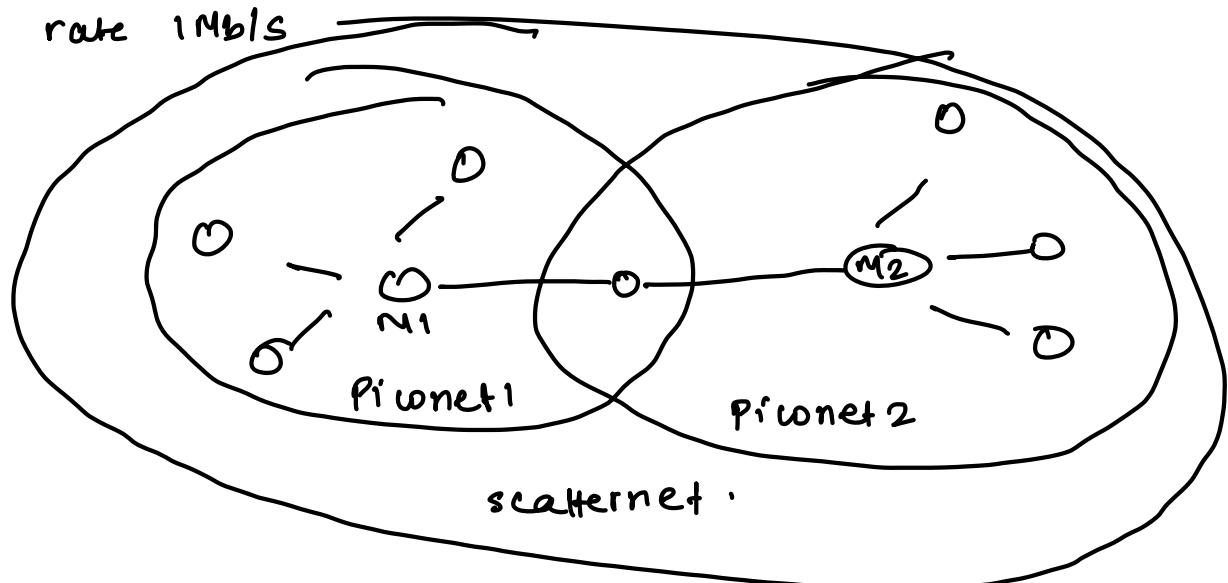
supply chain

magnet.

## Bluetooth

- low power tech
- short range 2.4GHz
- support data rate 1Mbps

Arch \*



## Pico

- 1 master mode
- communication only b/w master & slave
- range - 10m

## Scatternet

- made up of multiple piconet
- slave in pico can be master in scatternet
- node cannot be master in 2 nets.

## Attacks

- 1) Bluejacking - sending unauthorised msg to nearby devices.
- 2) Bluesnarfing - unauthorised access into info like contact, emails.
- 3) Bluebugging - Take control over a phone.

WIFI - Vic Hayes (Baap).

- wireless fidelity / that allows mobile / laptop to access networks.
- also known as WLAN.
- fast transfer rate / long range.
- use more power
- 2.5 GHz & 5GHz are used.
- WiFi (802.11 IEEE used).
- Use TCP/IP transport, High Bandwidth.

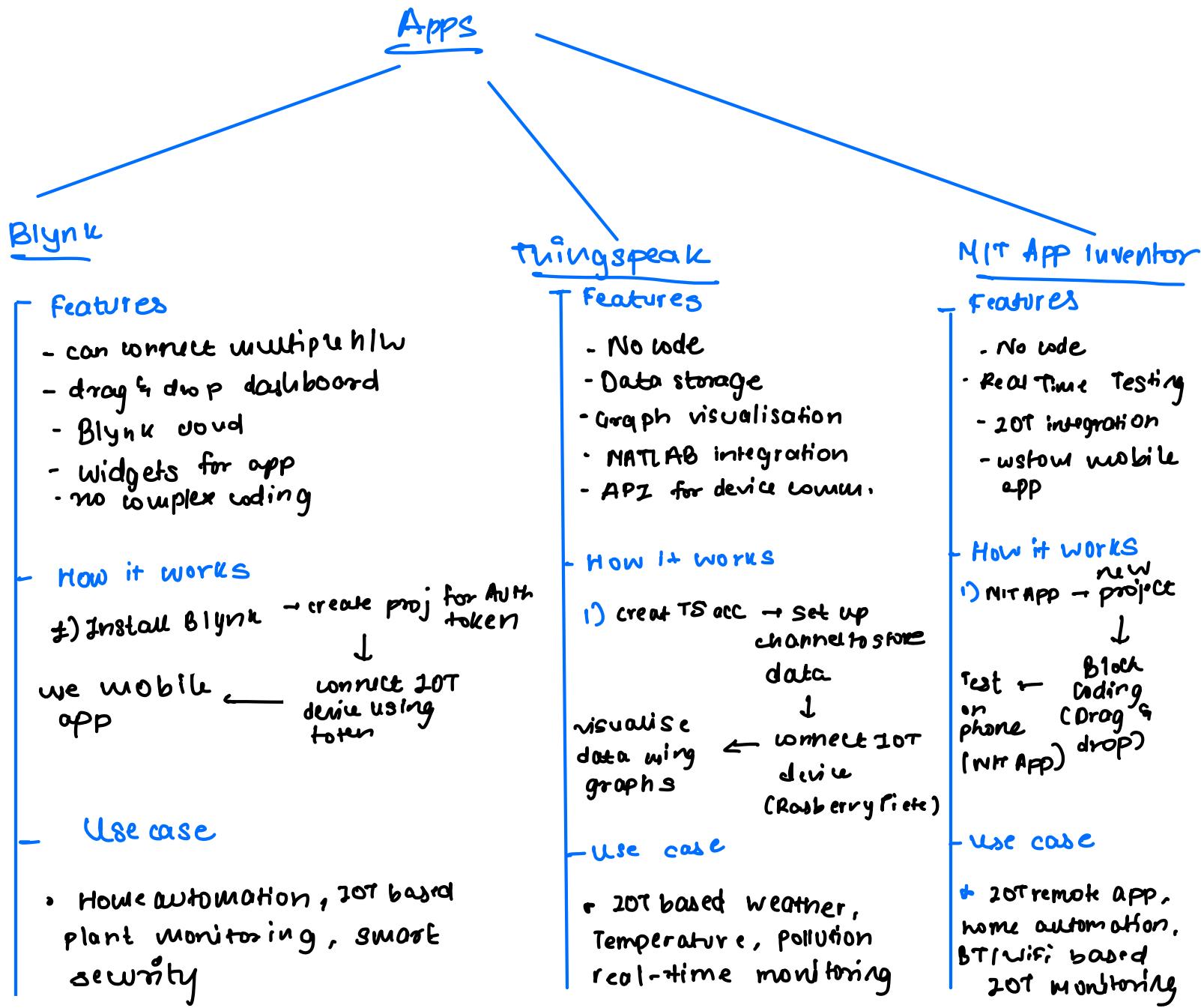
# Midsem

## Summary.

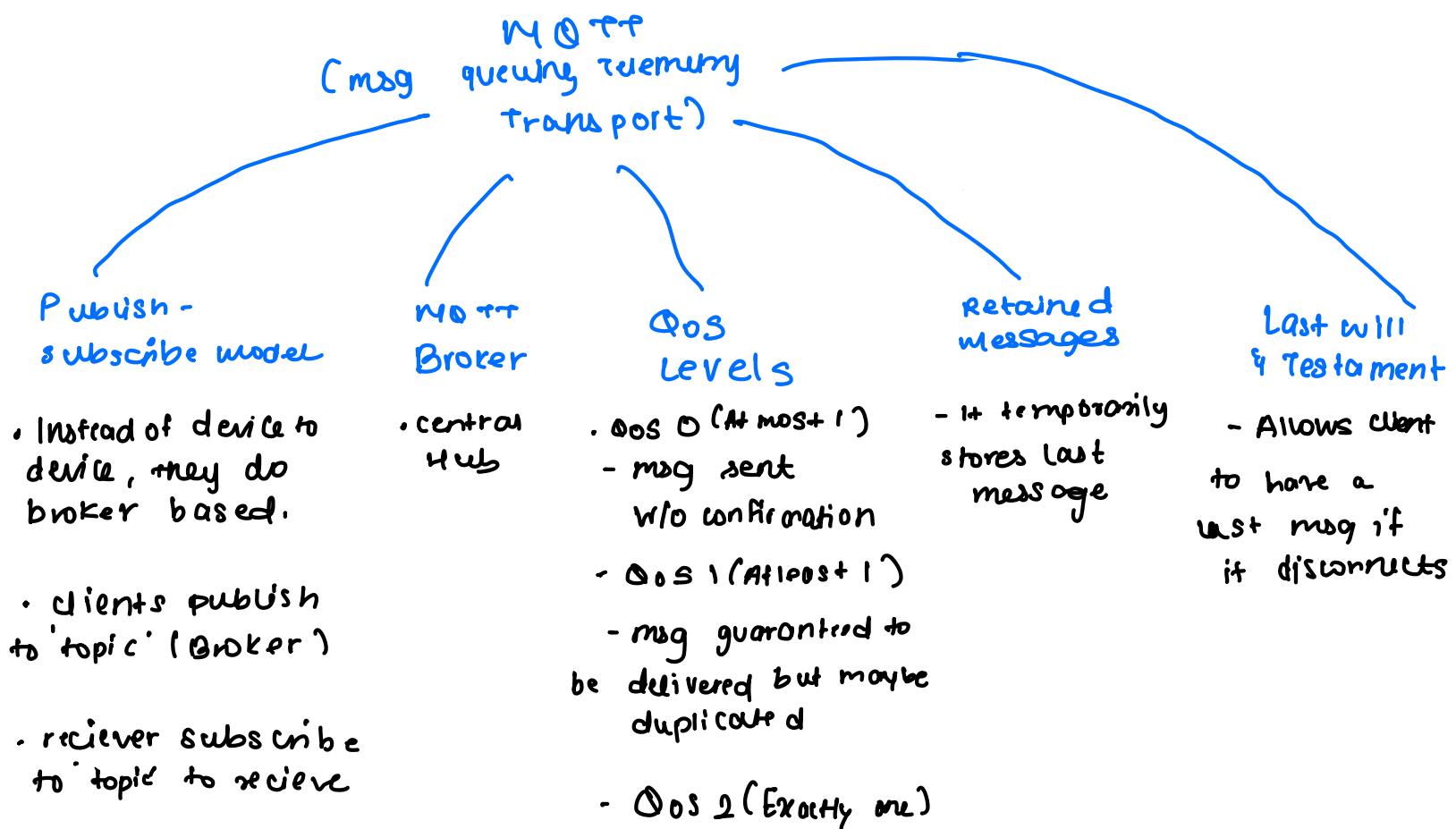
Blynk - ready made IoT App

Thingspeak - store & analyse IoT data

MIT app inventor - custom mobile app to interact w/IoT devices



## unit - 2



## use cases

- Smart home automation , Industrial IoT , Healthcare

## Quality of Life in IoT.

### Healthcare

- Wearable health device (fitness band)
- Remote patient monitoring

### Smart Home

- voice assistant
- fall detection sys

### Environment monitoring

- Air Quality sensor
- smart water quality monitoring

### smart infra

- traffic mgmt.
- waste mgmt

### Disaster Management

- early warning system

## Impact of IoT on QoL

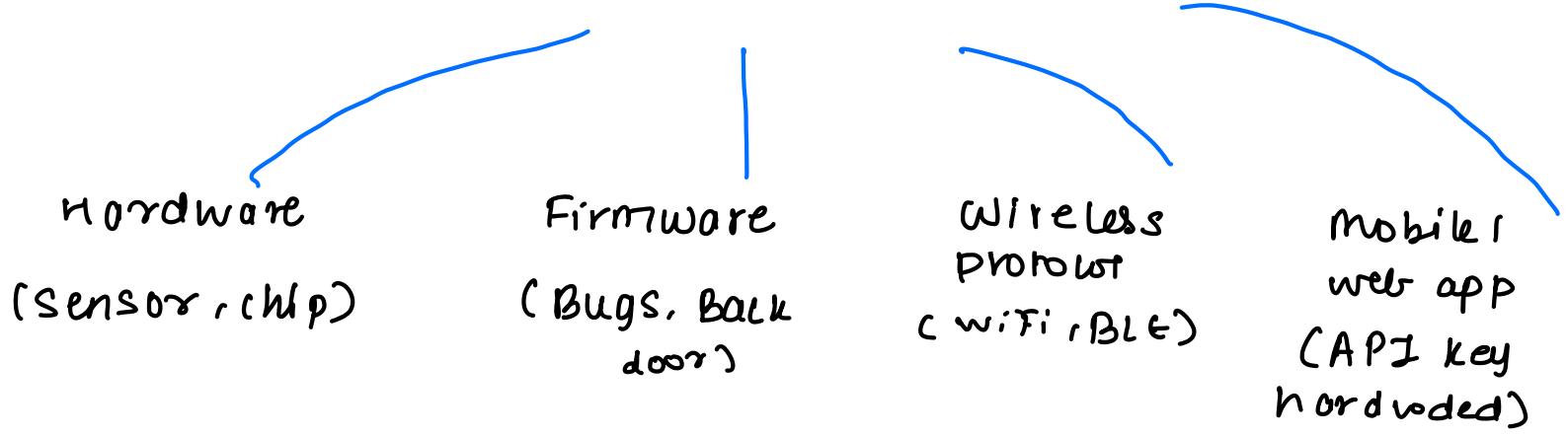
- Increased safety
- Better healthcare
- Energy efficiency
- Enhanced accessibility.

## Unit-5

**IOT security** - IOT yani everyday devices which are connected to the Internet. They send & collect data unkto protect karna.

- It focuses on C.I.A.

**Attack surface** - All the diff points where attacker can enter the system.



## OWASP Top 10

1. Weak Password
2. Insecure n/w
3. Insecure ecosystem
4. lack of secure update
5. Insecure/std component
6. Insuff. privacy
7. Insecure data Transf.
8. Lack of device Manag.
9. Insecure default sett.
10. Lack of Physical Hardening.

## Case study - Dyn Botnet (Mirai)

- many IOT device were hacked by Mirai in 2016.  
 in devices ko bots  
bara diya. → inse DDOS korva  
diya.

stages.

- 1) Infect devices

- 2) Protect itself
- 3) Launch attack

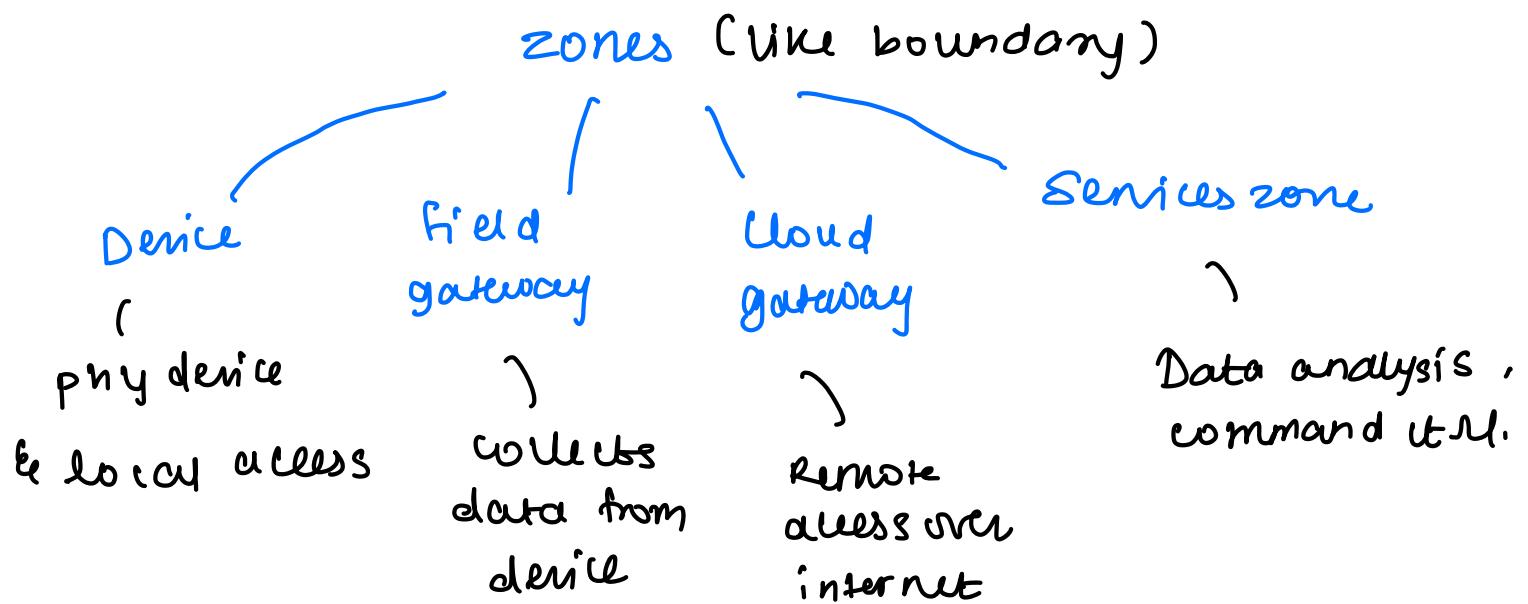
## IOT Pentesting approaches.

( NIW - black/whitebox  
 wireless - appin security  
 Phy - social eng)

Areas to test	Tools used
• Hardware / firmware	• HailKF / IDA Pro
• Radio comm'	• sniff (zigbee / BLE)
• Mobile / Web app	• XSS, SQLi vul.
• Cloud Interface	• weak MQTT

## Threat Modelling in IOT.

(we plan in future to stop attacks).

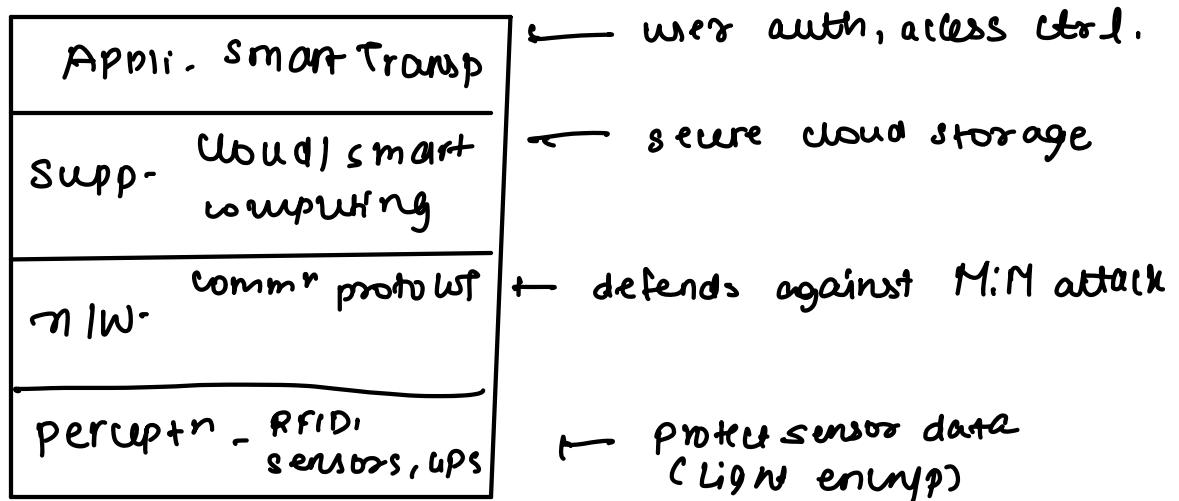


To stop this, we use STRIDE model.

S - spoofing

- + - Tampering
- R - Repudiation
- I - Info disclosure
- D - Denial of Service
- E - Elevation of privilege.

## IV IoT Security Architecture.



## IoT Security Requirements

Authentication - confirm identity of devices

Confidentiality - encrypt sensitive data

Integrity - ensure data isn't tampered.

Cloud security - strong encryp., multi party computation

Appl<sup>n</sup> security - safe data sharing & access ctrl.

# \* Challenges in IoT Sec

## Challenges

• Encryption

What it is?

Devices have low processing power

Solution.

Light encryption Algo

• Authentication

Devices need strong verification

Certificates, two-factor auth.

• Firewall update

Hard to update all devices

OTA updates

• WMM<sup>n</sup> channel

Data can be intercepted

TLS, secure protocol.

• Data Integrity

Data can be modified during transmission

Signature, checksum

• Application security

Apps can be vulnerable

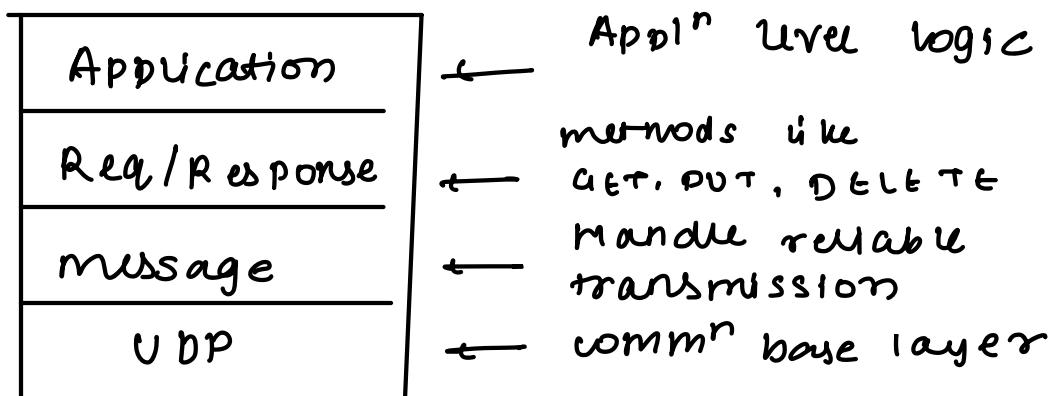
Secure coding practice

## Unit 2

### CoAP (constrained Appl<sup>n</sup> Protocol)

- light weight protocol designed by IETF for constrained devices
- connectionless (runs over UDP, not TCP)
- Based on RESTful Arch.
- Good for low power, memory devices.

### Arch



### Message types

#### 1) confirmable (CON)

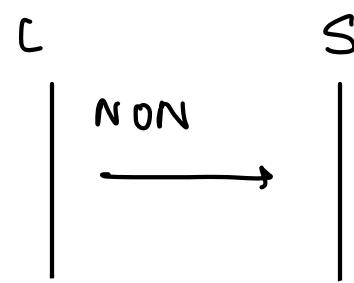
- Reliable, ACK needed

(response mfg if not  
ACK, RST)



## 2) Non confirmable (CON)

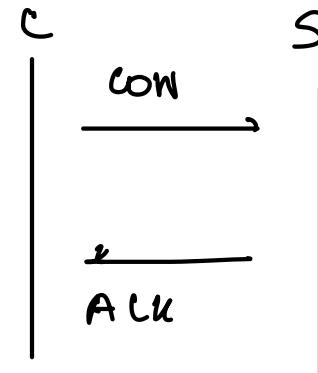
- unreliable, no guarantee of delivery



## 3) Acknowledgement (ACK)

- server confirms msg is received

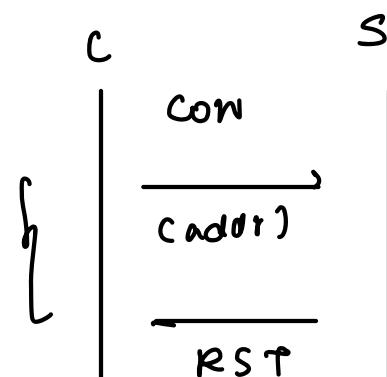
(like regular handshake)



## 4) Reset (RST)

- server indicates error in comm'

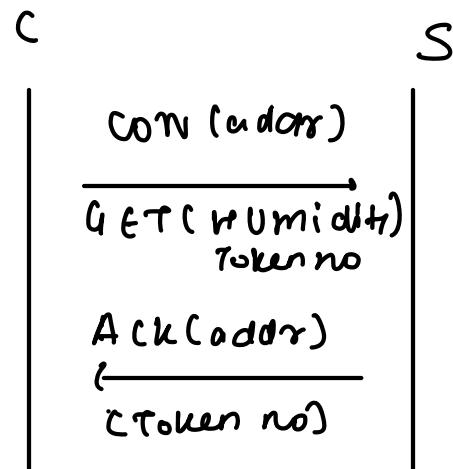
Time out



## CoAP Req-Response Modes.

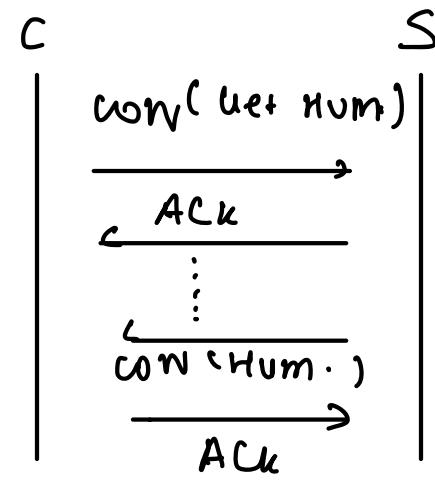
### 1) Piggyback

- ACK + response is sent immediately.



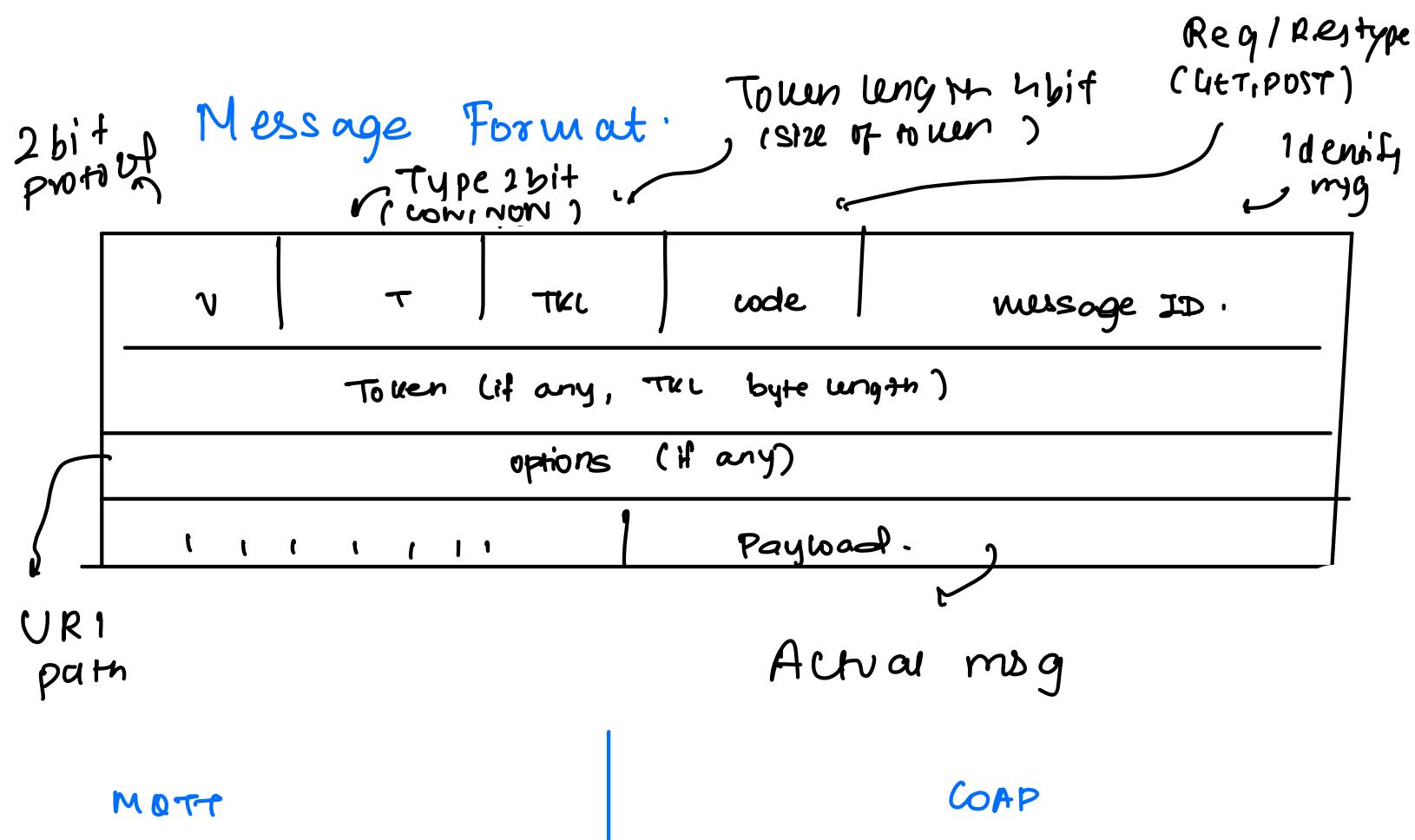
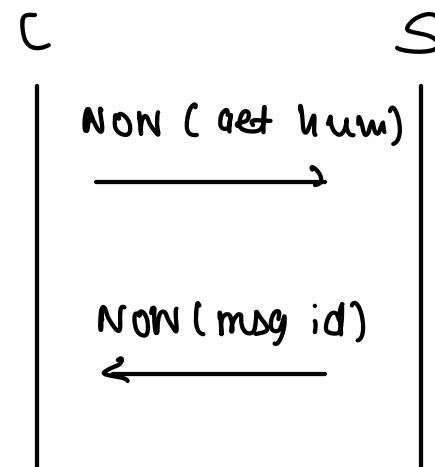
## a) Separate response

- Pehele empty ACK  
response badme



## b) Non-confirmable

- no acknowledgement
- Agar hum toh response nahi toh kuch nahi  
(no strings attached types).



- 1) TCP  
(connection oriented)
- 2) Many to many
- 3) more power
- 4) Publisher / subscriber

- 1) UDP  
(connectionless)
- 2) one to one
- 3) lowest consumption of power.
- 4) request - response (RESTful).

can accommodate  
only change

msg in near  
time

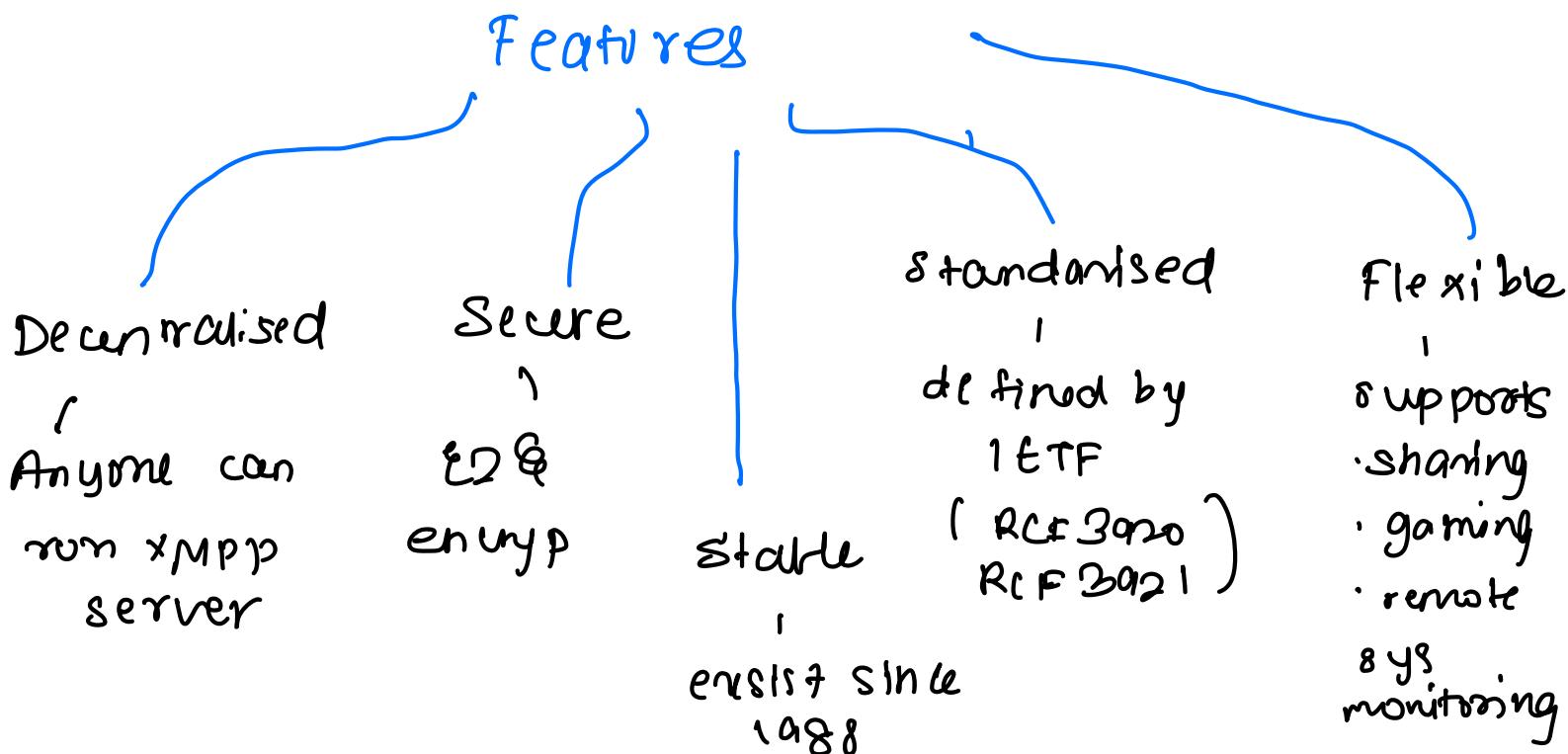
online/offline  
type

## Xmpp (Extensible messaging & Presence protocol).

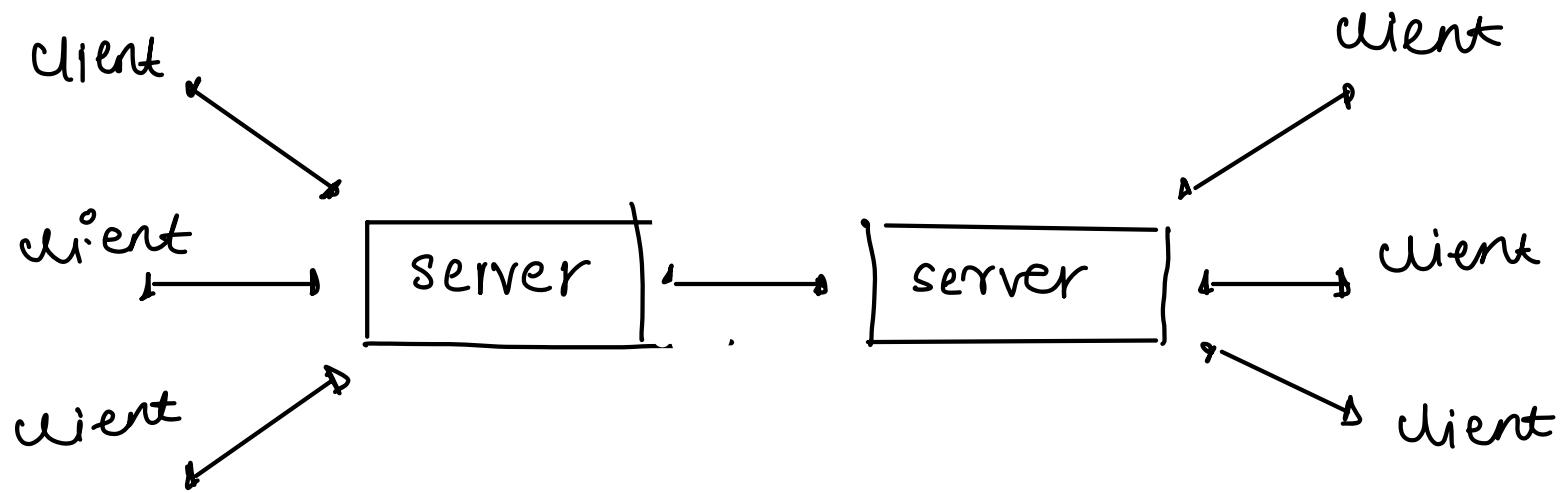
o set of rule & standard.

- Based on XML
- whatsapp use xmpp  
(msg, voice, video call)

- Previously  
known as Jabber.



# Architecture



- Client (S/IW, apps) connect an XMPP server
- Server can talk to other servers (Global n/w)
- Initially TCP based

Now, supports HTTP Polling  
Also, BOSH

(Bi-directional streams over Synchronous HTTP).

## Polling

- Client pulls (fetches) message from server

## Binding

- Server can push msg to client actively.