Architecture of IOT

The architecture four layers.

(1) Sensing layer - first layer.
→ includes sensors and actuators and responsible for collecting data.
→ These are placed in env to gather inform about temp, humidity, light sound
→ wired and wireless protocols connect these devices to network layer

(2) Network layer - provides communication and connectivity b/w devices in IOT
→ includes protocols like HTTP & MQTT that enable devices connect with each other
e.g. wifi, zigbee, cellular network.
→ includes gateways and routers that acts as intermediate b/w devices and wider internet

(3) Data processing layer - refers to the software & hardware component that are responsible for collecting, analyzing and interpreting data from IOT devices.
→ This layer receives raw data, process it and make it available for further analysis.
→ This layer use a variety of tools & tech which also include ML algorithms

Eg. tech used in data processing is data lake, which is a centralized repo for storing raw data.

(4) Application layer - topmost layer that interacts with end user

→ provides user-friendly interface enable user to access & control devices

→ software & applications including such as mobile ~~devices~~ apps, web portals

IoT Dashboard -

IoT dashboard is the user interface that enables user to interact, monitor with connected devices through buttons, charts other UI elements.

(1) Data enhancement - enhances data with additional contextual info like location, time, weather

(2) Data summary - summarise vast data in charts, plots, diagrams etc. Makes complex data easier to understand

(3) Data sharing - share imp. IOT data with partners & stakeholders. This enhances collaboration, coopration (real time data sharing

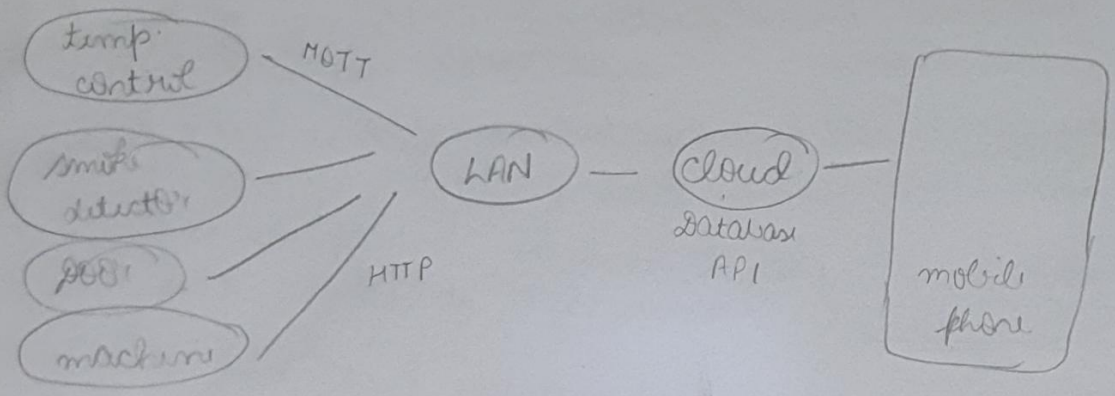
(4) Remote access - dashboards hosted in cloud can be accessed from anywhere.

→ monitor IOT devices & system remotely, enable users to stay connected when not physically present

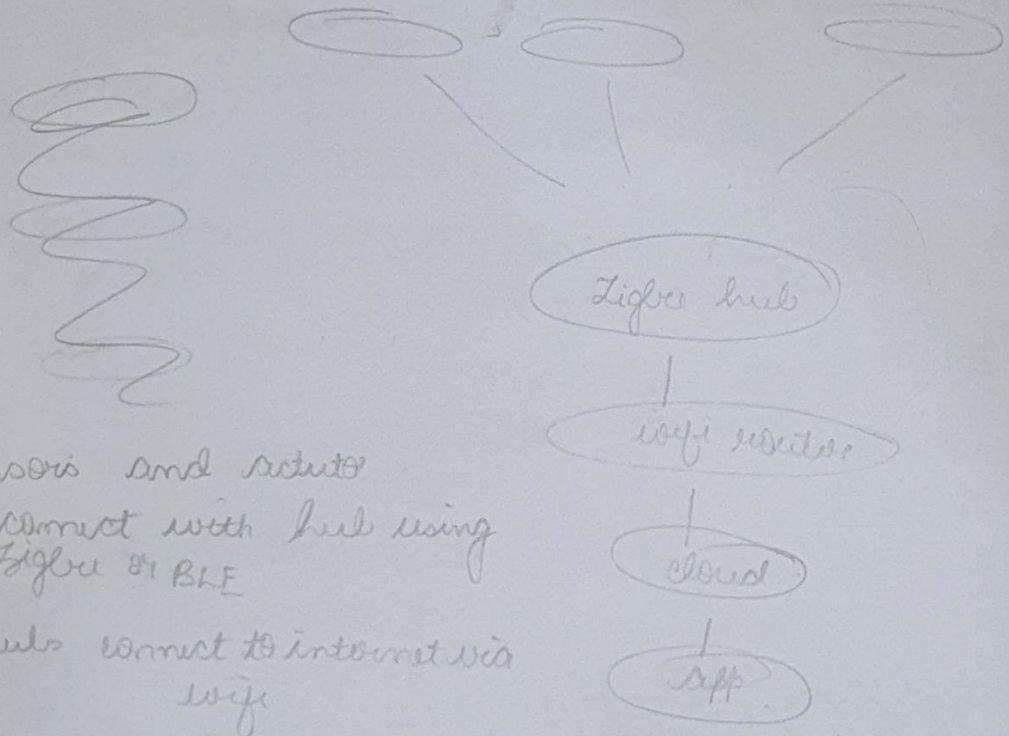
(5) Enhanced decision making - empower business & users to make data driven decisions optimize operations

1.

IOT



(1)



→ sensors and actuators connect with hub using Zigbee or BLE

→ hubs connect to internet via wifi

→ MQTT msg passing b/w devices & hub.

→ app communicate with hub using HTTP/S

→ cloud with hub via https.

Protocols –

(1) wifi – hub to internet, used in high bandwidth devices like security camera
→ wide availability, long range

(2) zigbee – used for sensors & actuators.
low power consumption

(3) BLE
short close range devices
low power consump, battery saving

(4) MQTT – device & hub.
lightweigh protocol, low bandwidth devices

(5) HTTP / HTTPS – user cloud interface
standard web protocol

(3) of first VAPT

(1) Physical vulnerability –

a. unauth physical access
vuln - tampering
mitigation – camera, biometric, access control

b. Env hazards extreme temp, humidity, electromagnetic
use EMI shields

(2) Network

a. wireless signals can be intercepted
use strong encryption

Symmetric – eg. AES.

Asymmetric – eg. RSA

many IOT devices have power and memory hence symmet

→ trasmits small packets of data

→ for large network managing unique key pair

→ allow periodic by rotation

3.

(1) Device hardening - ensuring that the devices are secure from the moment they are manufactured by tamper evident seals, secure packaging and hardened firmware

(2) access control - authentication protocol and secure credential management.

(3) Surveillance - motion sensors, cameras

(4) Regular audit

TLS is a protocol that implemented on transport layer to encrypt data transmitted via HTTP, FTP

IOT devices often transmit highly sensitive data over internet & this is often encrypted

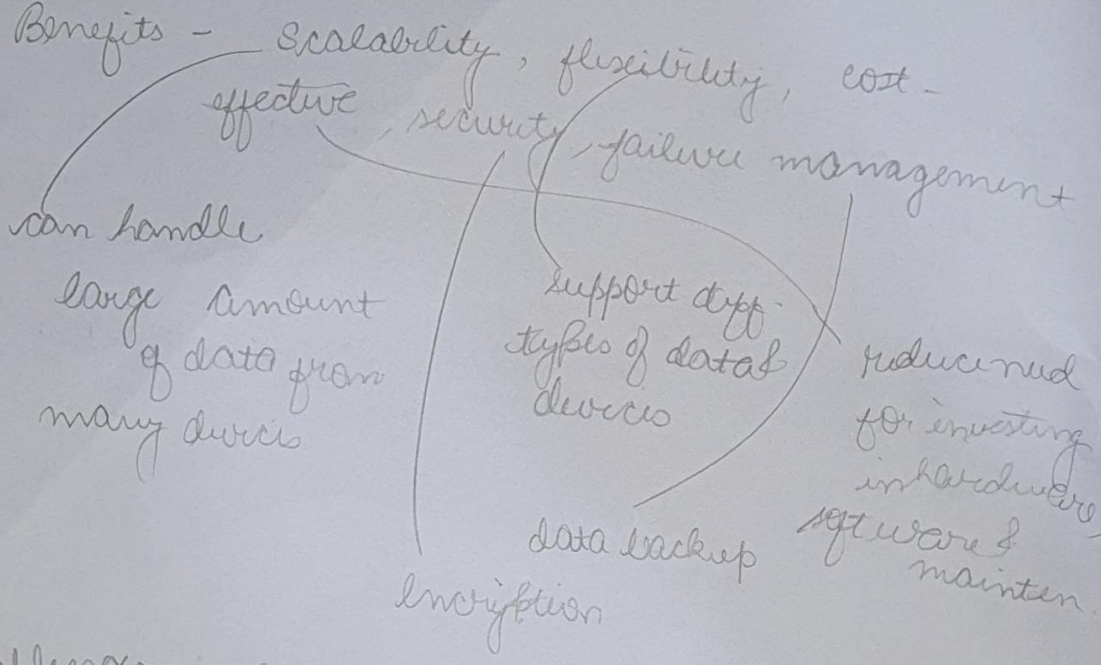
TLS is used to achieve confidentiality of application protocol MQTT, HTTP & web socket

(3)
→ Data from sensor is encrypted before transmission to a central server.

→ access to central server is restricted to authenticated healthcare provider

→ Digital sign are used to verify the integrity of data received

6.



7. RBAC.

→ works on principle of least privilege
→ helpful for larger enterprise where admin can create user group & assign them roles & responsibilities.

Admin - full control over all devices
User - limited control such as turning light
guest - very limited access.

(b)

(1) Scalability - as no of devices ↑ managing access control normally becomes impractical

group similar roles & permissions together

(2) Device heterogeneity — consist of devices from various manufacture with diff capabilities

adopt industry standards & protocols e.g. MQTT, CoAP

(3) Security & privacy
encryption

(4) latency
efficient algo
load balancing

8. first ensure your device have necessary ~~protocol~~ sensors & establish secure connection using protocol like MQTT

→ choose cloud platform
→ real time processing tool such as Apache Kafka

9
(1) User need analysis, include security, energy efficiency, convenience
(2) Scope and feature - camera, smart door
(3) Choose compatible devices - communi protocol like wifi, zigbee, Z-wave
(4) Network connection
(5) integrate the devices into chosen IOT platform
(6)

10 Over the air device management-

.recieve and install updates on software without the need for physical access to devices.

Convenience -

Security - patch software

Scalability - easily manage a large fleet of devices

Consistency - run on same software

feature enhancement - new features without disrupting device operation