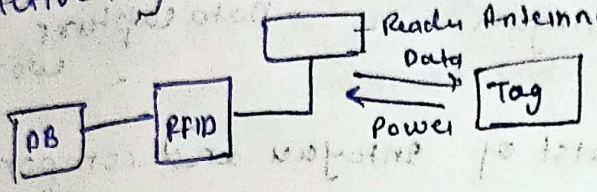
Internet of things

Radio frequency identification card - (RFID) Electronic tag, wireless radio frequency identification, inductive electronic chip and non contact card can identify target object and relevant data by radio frequency signal. can work in harsh env without human intervention.

Classification

- Passive tag - do not have power supply
- Active tag - built in battery.



Reader writer - device that capture and process RFID tag data made up of transceiver, microprocessor, memory, sensor.

controller - command center for operation of chip.

Reader Antenna - device that radiate Radio freq. signal as EM wave.

characteristic - fast scan
Miniature chapi
Reliable
Penetration unbarrier reading.
memory to store data.

Advantages

Disadvantage - Not technologically mature
high cost
Technical standard are not uniform.

EPCIS - Electronic Product code information Service.

It is a global GS standard for creating and share visibility event data to gain view of physical or digital object.

Object — Physical object — trade item, logistic unit, fixed asset, documents
Digital object — music download, ~~etc~~ e-book, digital document.

EPCIS has two major standard

- Capture - It contains interface which allow other application to send event into EPCIS system.
- Interface - capture interface
  - Application
  - IOT interface

System component
- Filtering collection
- Data capture

Query interface - consist of interface and component.
Interface - EPCIS Query interface
interface exposed to other parties.

system component - EPCIS repository
Accessing applications.

Wireless Sensor Network. can be defined as a self configured and infrastructure less / wireless network to observe physical or environmental condition. to pass data to sink (where information is observed)
Sink - seems like interface b/w user and network.
WSN contain 1000 of sensor.
WS node are equipped with radio transreciver computing power.

Types - 5
Terrestrial WSN - used for communicating base station efficiently and comprise thousand of wireless sensor node deployed in structed or unstructed order.

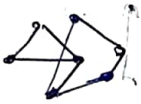
Underground WSN - contain several sensory nodes hidden in ground to observe underground cond". more expensive, limited battery.

Underwater WSN - Sensory node deployed in water. propagation delay, bandwidth, sensor fail

Multimedia WSN - Proposed to enable tracking/ monitoring of event in sort of multimedia contain, camera microphone

Mobile ~~wireless~~ WSN - comprise, sensor node that can be moved on their own and can interact with physical env.

Structure

1) Star 
2) Mesh 
3) Hybrid - 

Application
- military
- health
- Transport
- Threat detection.

Characteristic
- Easy to use
- can deal with node failure
- Homogeneity of node
- Heterogeneity of
- Mobility of node.

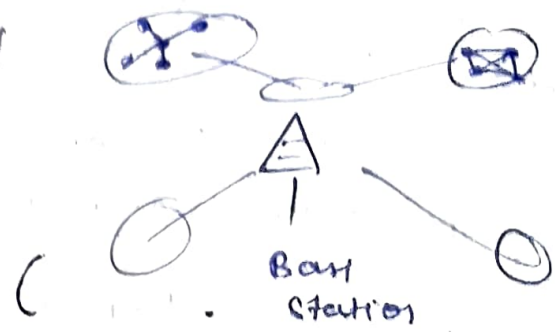
Issues
- low latency
- Transmission media
- fault
- Scalability.
- ~~Coverage~~ problem coverage.

WSN architecture (3)

Layered Network

- application layer
- transport "
- Network "
- data
- Physical

a) Clustered Network

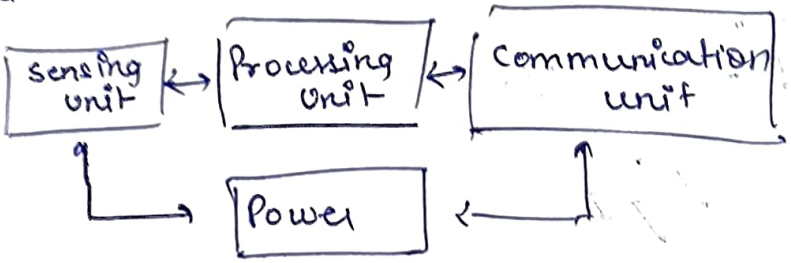


Two tier hierarchy architecture used leach protocol

LEACH - low energy Adaptive clustering Hierarchy.

In every cluster head node create TDMA (Time division multipl Acess) plan

WSN Node



Sensing unit - contain sensors (thermal magnetic, chemical etc)

- measured parameter are sent to processing unit.

Processing Unit - execute task and control functionality

It is pre-programmed. computation is also performed result is sent to base station via communication unit

Communication unit - used to transmit and receive information among node and base station. four states - transmit, receive, idle, sleep.

characteristic of wsn/ node / sensor

Fault tolerance - Each node is prone to unanticipated failure

Mobility - Node can move anywhere, ↑ communication

Dynamic topology -

communication failure - failure should be informed to base station.

Heterogenity - various sensor work in co-operation

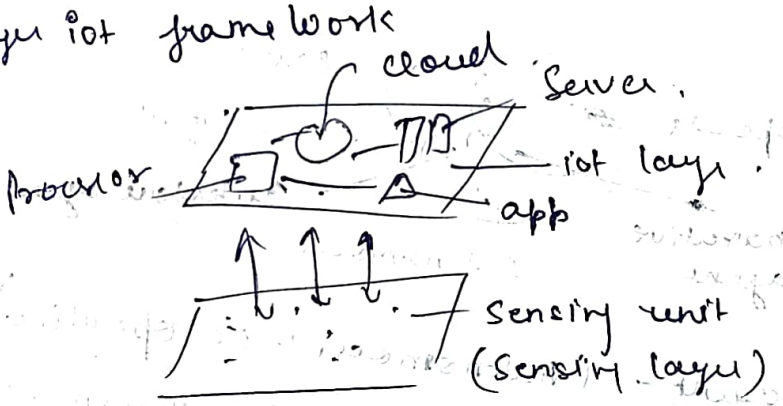
Scalability - (can be extended)

Indundency - should work without central control

Programmability - programing and reconfiguring

Clustering Principles

Two layer iot framework



Software agent for object representation

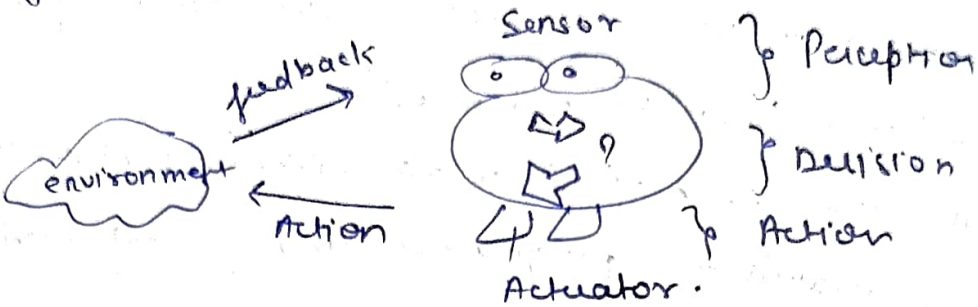
Software agent is a computer system that is able to interact with environment and capable of making autonomous decision on behalf of its owner. It work autonomously & continously.

Properties

1) Reactivity: Ability to sense surrounding and interact with it.

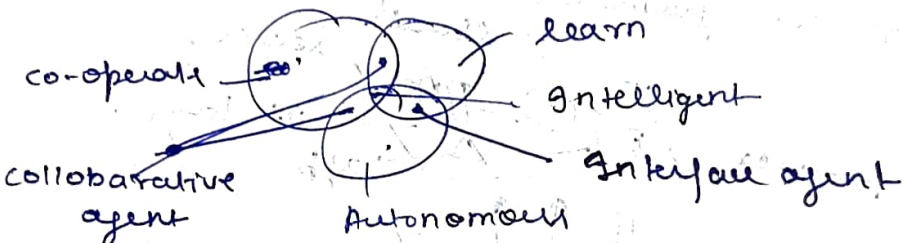
2) Pro-activeness - ability to change their behaviour to achieve its goal.

3) Social ability - ability to social and can interact with other to achieve its goal.



Software agent and representation

Software agent architecture.



Collaborative agent - (Autonomous + co-operative)

Property - autonomy, social ability, Responsive, pro active

Interface agent - (Autonomous + learning) work with user in same environment.

It is a personal agent that help owner by observing monitoring and learning. can suggest new method and better ways..

Mobile agent - Agent capable of transporting itself from one location to other.

(autonomous + co-operative + mobility)

Information agent - it helps owner to manage, collect and manipulate information from many distributed resources. (autonomous + mobility)

Reactive agent - Interact with other agent, perform particular task, low level nature close to raw sensor data.

Hybrid and heterogenous -
| (two or more agent)
└ similar to hybrid formed to ↑ strong point, ↓ weak point.

Data Synchronization - process of establishing consistency and consolidation of data b/w devices. very import for iot entails harmonization of data over time, in a complex process.

Challenges - ~~asyncro~~ asynchrony, conflicts, low bandwidth, file system.

Data replication - storing same data in several location. to prevent data loss. (Backup)

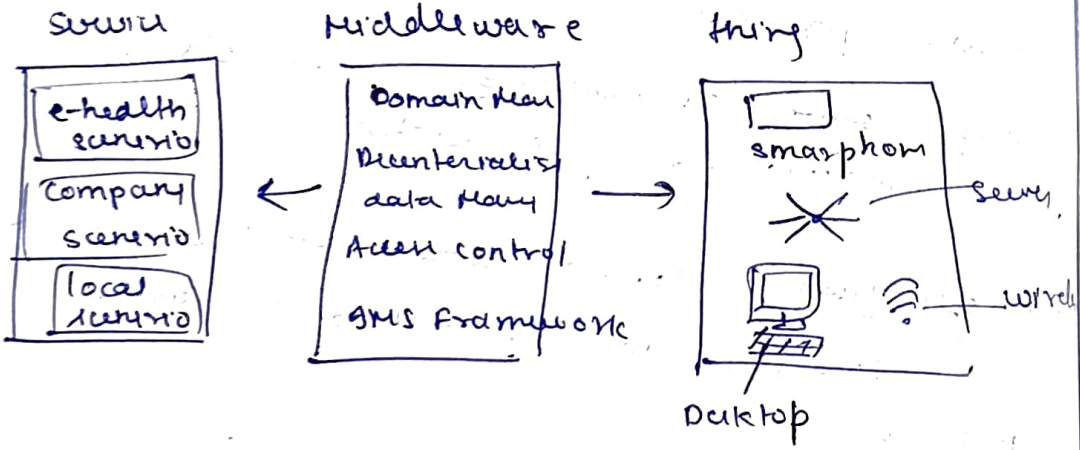
Need of synchronization
- for efficient communication
- to remove conflict.
- data management in cloud.
- data security
- Data privacy
- Synchronizing data effectively reduces data volume.

Identity management system - It provides manage identities individually and their privileges, roles, authorization, authentication to increase security and decrease delay/cost, ~~repetitive~~ repetitive operation.

Generate certificate, manage role, control access authentication.

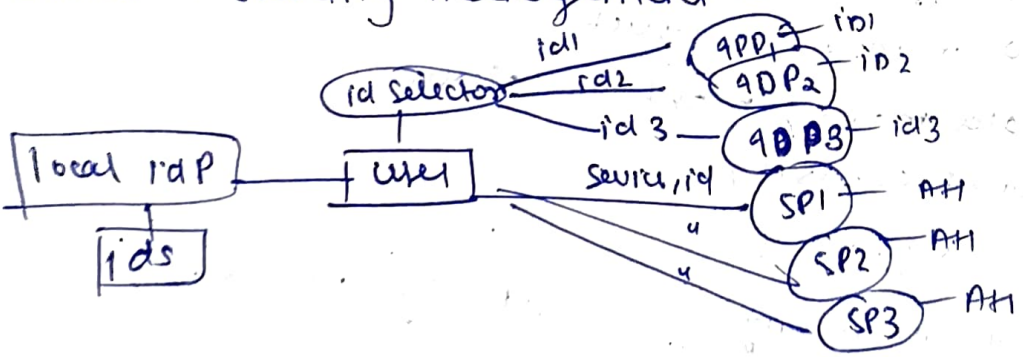
Identity management System include decentralized software resources and network protocol.

IMS architecture has thing such as simple device and complex device (smartphone). Each belong to user specific space and collaborate with other



IMS framework

User centric Identity management -



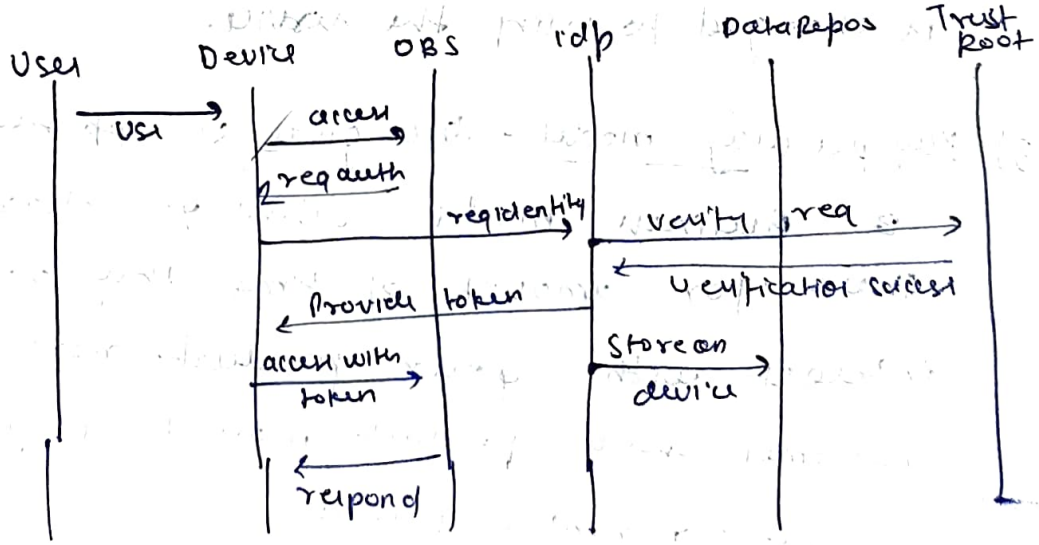
User centric identity management allows user to control their own digital identities.
User have portfolio of electronic identity and identity sector. At request of service SP they can select an identity and decide whether to release certain attribute. U-prove is a software solution responsible for signing token providing validity of user attribute.

Ex- Yahoo allows authentication from FB & Google.

Device centric identity management

device based identity utilizes security credentials on the device to authenticate with service and user identity provider to distribute public key for identity and maintain list of attributes

It introduce security token sent to device and get stored, used to identify service and authenticate the device requesting service.



Device - identity management for shopping system.

Business model

- Business model describe how an organization create, deliver and capture values.

IoT business model has two part

1) Focus on capturing and delivering value
2) leverage unique characteristic to produce innovative and differentiated value

1) Platform business model -

combine many actors and consumer in marketplace to benefit both. key to it is interoperability and interconnection of device and business to generate revenue.
to third party vendor.

Ex - Amazon sell alexa to generate revenue.

2) Subscription model - always on connectivity of IoT device to recurring revenue or subscription mode. timely fee is charged to use the service.

3) Pay per use model - ~~the give an opportunity to~~

Business model where you charge them for amount of time they actively interact with your product. more customer use a product more they pay.

Example - car rental service.

4) Asset-sharing model - Access instead of ownership.

In this model we do not own an equipment rather we rent it out.

Ex- Industrial firm in construction and mining partners with nearby business to share cost of heavy machinery.

Asset tracking model - Connected devices in supply chain business identify, monitor and track asset in real time. It help protect asset from loss or theft.

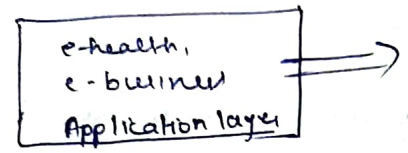
Ex - Sierra wireless help global company track cargo with high value IoT asset-tracking platform.

Outcome based model - idea for this model is for customer to pay for outcome of IoT product, not product itself. Many of model discussed are outcome based as they focus on what consumer gain from device rather than device itself.

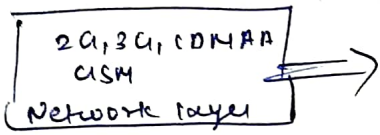
IoT issues

- IoT includes everything from fitness bands smart home appliances, medical device, auto... security has not been priority for them.

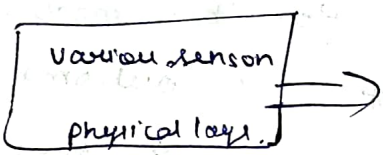
security architecture



End device/user authentication protocols, secure communication protocol



Crytographic protocol for data at cloud



softwared based crypto graphic protocol of data security

curity requirement

Key requirement —

- device and data security.
- authentication of device
- confidentiality of data
- integrity of data

Application layer – user confidentiality

Network layer – distributed denial of service of attack.

Physical layer – authentication.

rity goals

ngfidentiality – no one can read data except sender & receiver.

- limiting information access
- (Password, encryption)
- (Applied to transmission as well as to data)

been altered in any way has not
- No change in data
- source integrity (data come from sender)

Availability - Availability refers to availability of information resources to authorised user and do not show to unauthorised user.

challeges of iot Security -

- Device not reachable
- Device can be lost Stolen
- Device are not crypto engine
- finite life.
- device are transportable.

Vulnerabilities of iot
└ vulnerabilities are weakness them can cause harm or hacker/attacker can harm easily.

1) weak encoded password.
2) lack of an update process
2) unsecured network.
3) unsecured IOT app component
4) unsecured data storage

Threats -
Spoofing threat - Attacker intercept or partially override data stream of an iot device known as man-in middle attack.

Information disclosure threat - Attacker obtain information without authorization, from signal or replay information. They threaten to release or sell data

Tampering threat - Attacker can get access to firmware or OS of device running or the app and then partially replace it with the device

Dos - Denial of service tries to capacity overload in the target system by sending multiple request - It slow down service

Ransomware - It this attacker use malware to steal information

Information assurance - practice of protecting & managing risk related with storage and transmission of data.

Availability

Integrity

Confidentiality

Non-repudiation - It is assurance that someone cannot deny the validity of something

Sensor

Sensor converts a physical quantity into corresponding voltage. It respond to change in physical phenomenon (temperature, displacement force).

- Sensor type — Active — external power
  - Passive — power required is given by physical phenomenon.

Specification

- Accuracy
- Resolution
- sensitivity
- Repeatability - Precision
- Bandwidth.

Example - temperature sensor, proximity sensor, IR, pressure, touch, colour.

Type -

- Mechanical - (mechanical deformation) detects
- Pneumatic (measure gas pres)
- Optical (light to signal)
- Electrical (detects physical parameter)
- Range - (detect 3D view and calculate distance)

Actuator - device or mechanism capable of performing physical action. It is component of machine responsible for moving or controlling of system.