GOVT. POLYTECHNIC BALASORE

LECTURE NOTE
ON
IOT (TH.4)
SIXTH SEMESTER
DIPLOMA
IN
ELECTRONICS & TELECOMMUNICATION
ENGINEERING
BY

PRAKASH CHANDRA DAS

DEPT. OF E&TC ENGG.

* What is IOT

IOT stands for internet of things.
It is a highly distributed networks of smart objects embedded with electronic sensors, actuators and softwares each capable of dynamically generating, analysing and communicating intelligence that can be used to increase operational efficiency and power new buisiness models & make life more easier and comfortable.

* Application of IOT

Home
→ Smart lighting
→ Smart appliences
→ Smoke and Gas detector

Cities
→ Smart parking
→ Smart Roads
→ Structural health monitoring
→ Emergency response

Environment

- → Weather monitoring
- → Air pollution monitoring
- → Noise pollution monitoring
- → Fire Detection

Retail

- → Inventory management
- → Smart payment
- → Smart vending machine

Energy

- → Smart grid
- → Renewable energy Stem
- →

Logistic

- → Route generation & scheduling
- → Fleet tracking
- → Shipment monitory
- → Remote vehicle diagnosis.

Agriculture

- → Smart irigation
- → Green house control

Industry

→ Machine diagnosis and prognosis
→ Indoor air quality monitoring

Health

→ Health and fitness monitoring
→ Wearable electronics.

* Characteristics of IOT

Dynamic and self adapting → It can adapt to the environment.
Ex:- A surveillence system can adapt no. of Cameras dynamically.

Self Configuring

Devices can configure themselves in appli association with IOT infrastructure.
Ex:- Set of networking, fetch latest software update with minimal user

Inter operable Communication protocols

It support different protocols for different devices and which is interoperable.

Unique identity

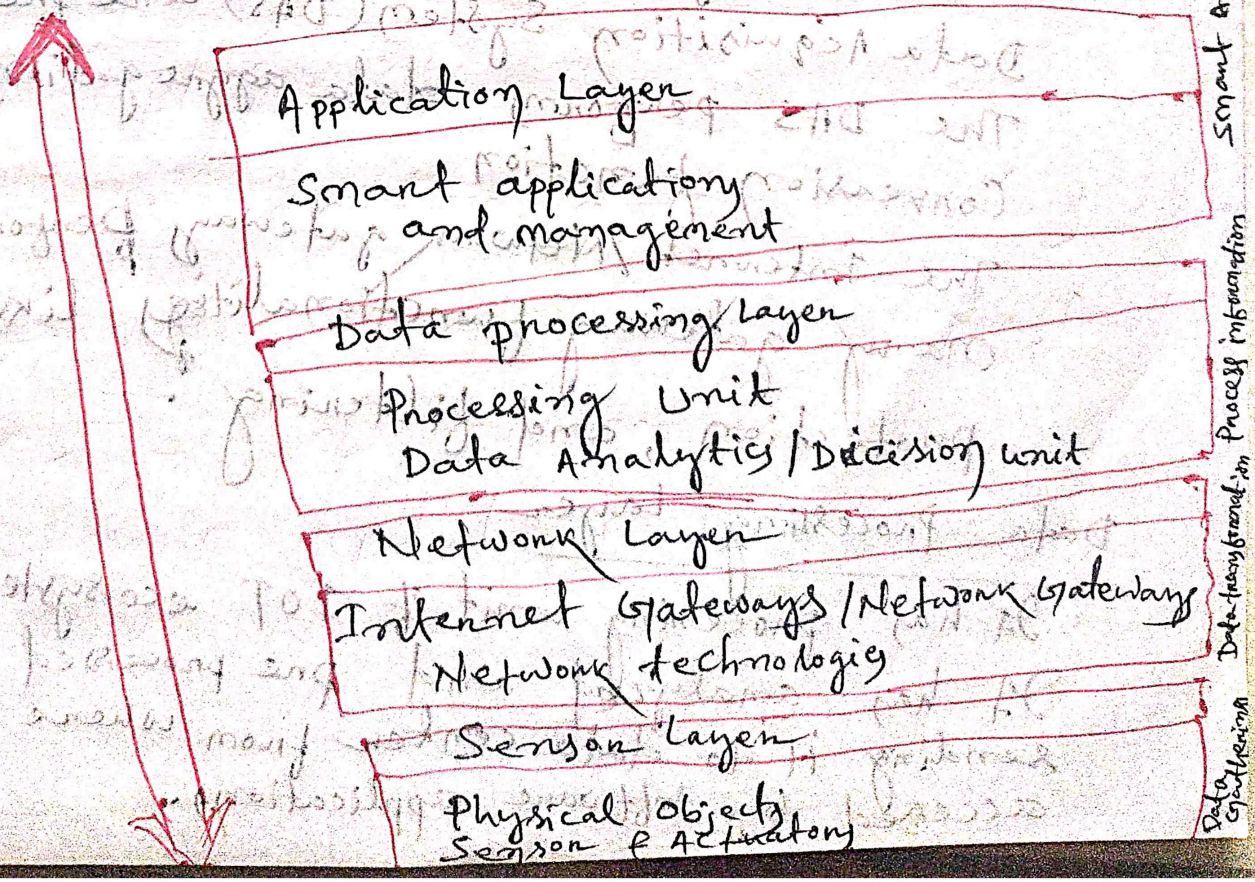
IP address and URL are used for identity.

Integrated in to information network

IOT devices can be dynamically discovered in the network by other devices and have the capability to describe themselves to other devices or user application.

* Architechtural overview

→ In an internet of things (IOT) technology has a wide variety of applications.
→ It has use of internet of things is growing so fasten.
→ It's depend upon different applications areas of internet of things.
→ It's work accordingly as per it has been designed / developed.
→ It has strictly followed by universally.
→ It depends upon its functionality and implementation in different sectors.
There is basic process flow based on IOT.



The above architectural overview is 4 layers. It can divided as follows.

→ Sensing layer
→ Network layer
→ Data Processing Layer
→ Application Layer

Sensing Layer

In this layer sensors, actuators, devices are present.
This devices accept data (physical / environmental parameters), processes data and emits data over network.

Network Layer

In this layer Internet / Network gateways, Data Acquisition System (DAS) are present.
The DAS performs data aggregation & Conversion function.
The Internet / Network gateway performs many gateway functionalities like, malware protection, and filtering.

Data Processing Layer

It has processing unit of IOT ecosystem.
It has analyzed and pre processed before sending it to data center from where data accessed by software applications.

The data can be monitored & managed, due to Edge IT on edge analytics comes in to picture.

Application Layer

The data ~~centers~~ centers where data is managed & it's used by end user applications. like, agriculture, health care, aerospace, farming, defense etc.

Design Principles and Needed Capabilities

Every day life will be more filled with intelligent, connected objects.
IOT Solutions consist of multiple elements. physical devices like sensors, actuators & interactive devices.

Design Principles

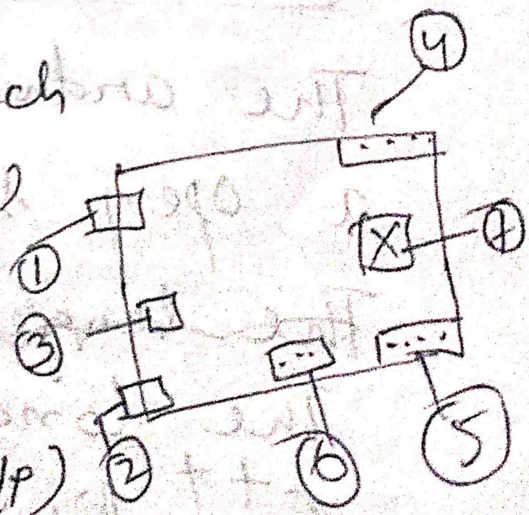
Arduino

Arduino is a open source electronic platform based on easy to use hardware & software. Arduino boards are able to read inputs such as light on a sensor, a finger on a button or a message and turns it into an o/p activating a motor, turning on a LED, publishing on line etc.

We can tell the board what to do by sending a set of instruction to the microcontroller on the board. Arduino programming language, Arduino software (IDE) can be used to write program for giving instructions.

Important parts of Arduino board

① → USB Connecton
② → power Connecton
③ → Automatic power Switch
④ → Digital pins (i/p or o/p)
⑤ → Power pins
⑥ → Reset Switch
⑦ → Analog pins (i/p or o/p)



Advantages of Arduino

Inexpensive

→ Arduino boards are relatively inexpensive. Compare to other microcontroller platforms.

→ The rest is less than 50 US$.

Cross Platform

Arduino software ID Seen on windows, Machintosh and linux OS.

Simple Clean programming environment

It is easy to use for beginners & flexible enough for advance user

open source and extensible software

The arduino software is published as a open source tool.

The language can be expanded through C++ libraries.

It is based on AVR C. Programme Language

Open source and extensible hardware

The ckt design can make their own version of the module extending the arduino board and improving it.

RASPBERRY PI

→ It is the name of a series of single-board computers made by the Raspberry Pi foundation;
→ The Raspberry Pi launched in 2012.
→ The original Pi had a single-core 700MHz CPU and 256 MB RAM and latest model is quand-core 1.4GHz CPU with 1GB RAM.
→ It has many more applications like; to learn programming skills, build hardware projects, do home automation, and industrial applications.
→ It is a very cheap, computer that runs Linux, but it also provides a set of GPIO (general purpose input/output) pins that allow to the control electronic components for physical computing and explore the Internet of Things (IOT).
→ It's a fully credit-card sized computer which can be plugged in to a computer/monitor.

→ It can perform tasks, such as browsing the internet, word processing, playing games and developing IOT based applications.

→ It have been three generations, such as Pi 1, Pi 2 and Pi 3 and there has been a Model A and a Model B of most generation.

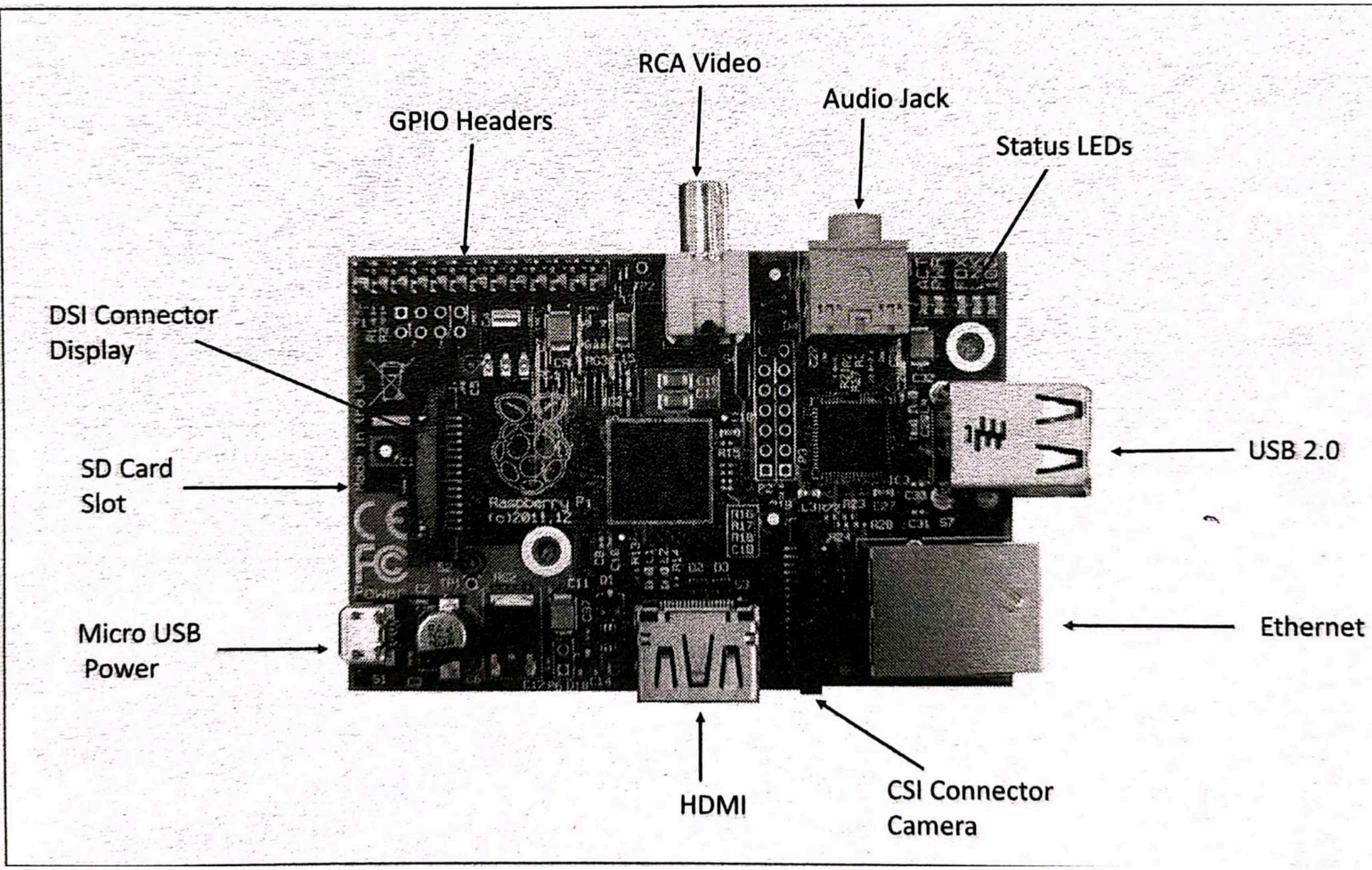
→ The Raspberry Pi is also called as single-board mini computer.

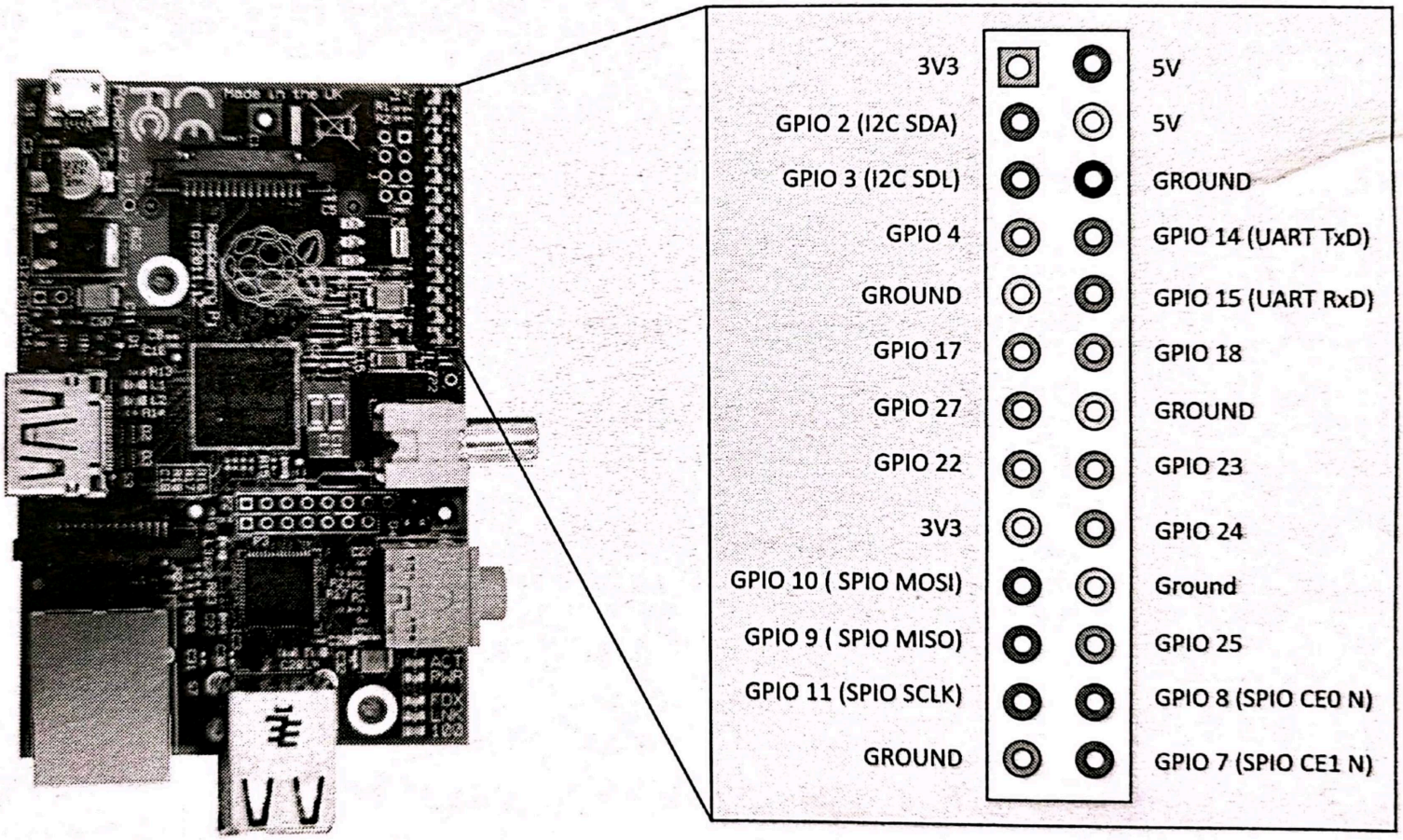
→ Raspberry Pi is a low-cost mini computer with the physical size of a credit card.

→ Raspberry Pi runs of Linux and it can perform all tasks that a normal desktop computer can do.

→ In addition to this, Raspberry Pi also allows interfacing sensors and actuators through the GPIO (General purpose Input/output pins.

→ Since Raspberry Pi runs Linux operating system, it supports Python "out of the box".





Raspberry Pi GPIO headers

Processor & RAM :- Raspberry Pi is based on an ARM.
Processor. The latest version (model B, 2) comes with 700MHz low power ARM 1176 JZ-F processor and 512 SDRAM.
USB ports

USB ports :- Raspberry Pi comes with two USB 2.0 ports. It can provide a current upto 100mA.

Ethernet Ports :- Raspberry Pi comes with a standard RJ45 Ethernet port. You can connect an Ethernet cable to provide internet connectivity.

HDMI output :- It can provides both video and audio output. You can connect to a monitor/computer using an HDMI cable.

Composite video output :- The composite video o/p with an RCA jack that supports both PAL and NTSC video output.

Audio output :- Raspberry Pi has a 3.5mm audio o/p jack.

GPIO pins :- It is a general purpose i/p/o/p pins. There are four types of pins on Raspberry Pi; true GPIO pins, I2C interface pins, SPI interface pins and Serial Rx and Tx pins.

Display Serial Interface (DSI) :- It can be used to connect an LCD panel to Raspberry Pi.

Camera Serial Interface (CSI) :- It can be used to connect a camera module to Raspberry Pi.

Status LEDs :- It has five status LEDs.

SD Card Slot :- Raspberry Pi does not have a built in operating System and Storage. You can plug-in an SD Card loaded with a Linux image to the SD Card Slot.

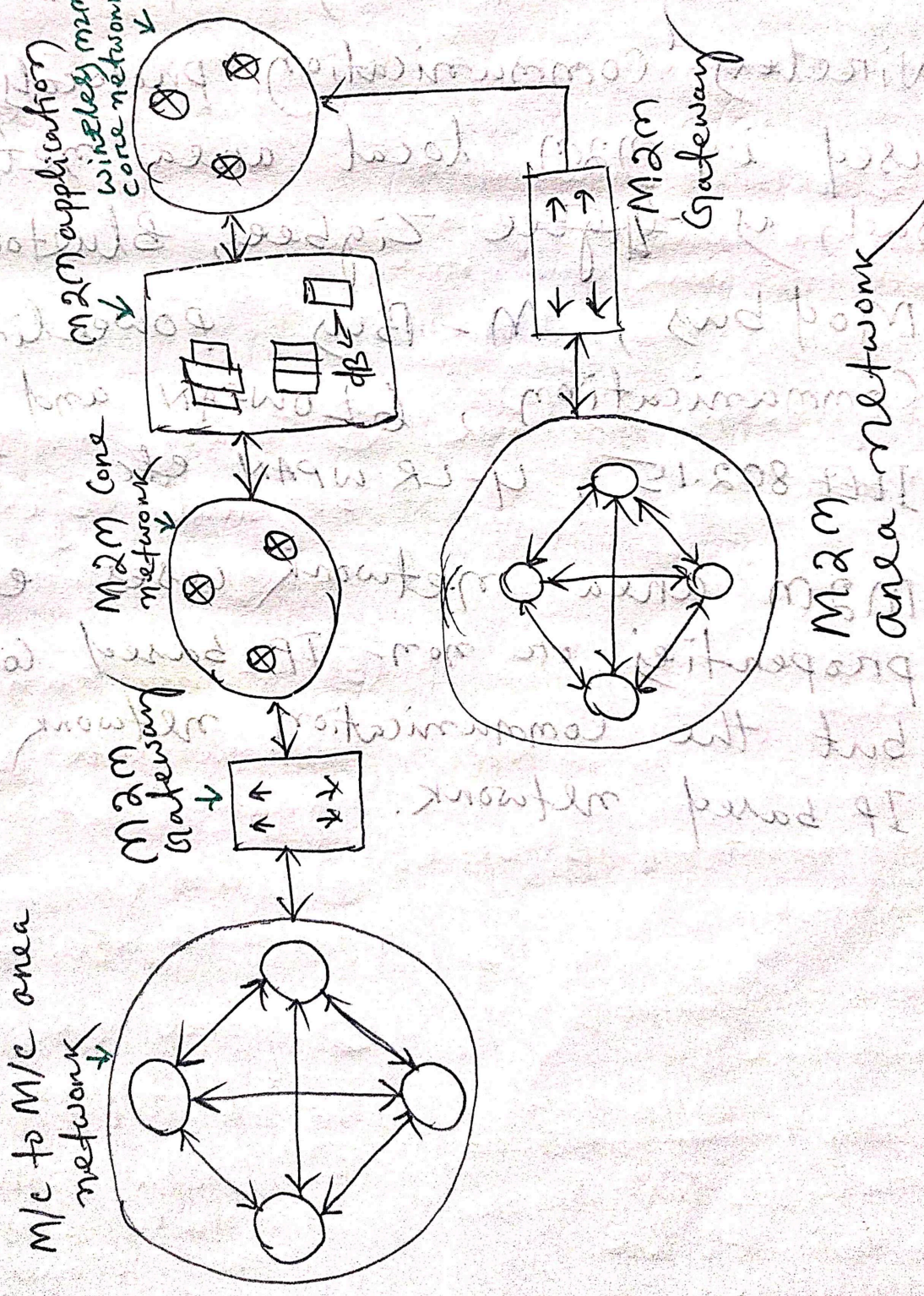
Power input :- It has a micro-USB connector for power input.

Raspberry Pi Status LEDs

Status LED	Function
ACT	SD Card Access
PWR	3.3V Power is present
FDX	Full duplex LAN Connected
LNK	Link/Network activity
100	100 Mbit LAN connected

Machine to Machine (M2M) or M/c to M/c

→ M/c to M/c (machine to machine) refers to direct communication bet machines or devices using any communication channel including wired and wireless.

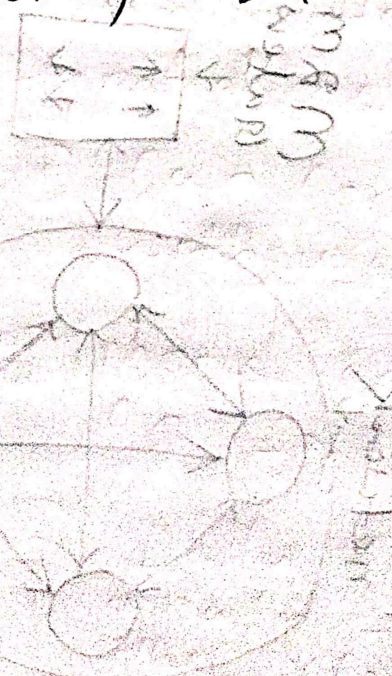


→ It is a networking of machine for the purpose of remote monitoring, control and data exchange.

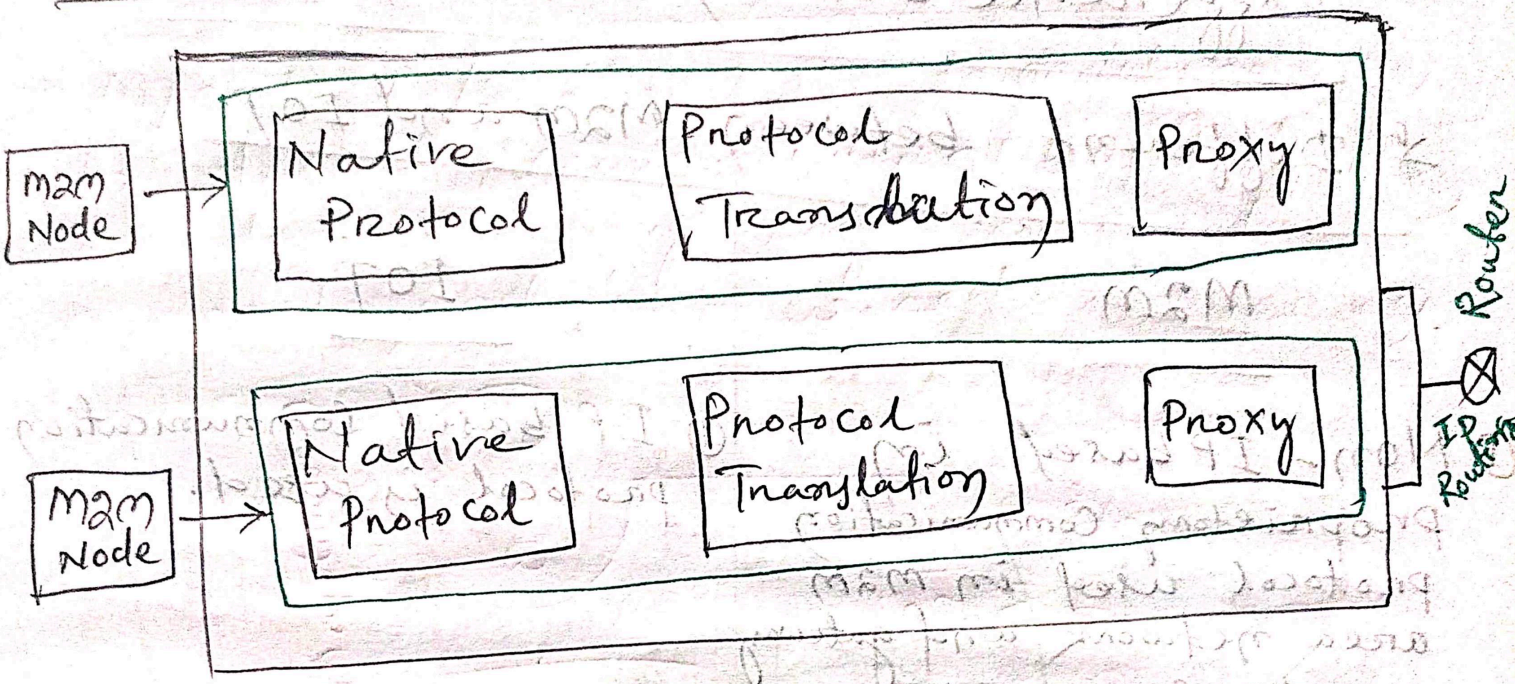
→ M2M area comprises of machine (M2M nodes) which has embedded hardware module for sensing, actuation and communication.

→ Wireless communication protocols can be used in M2M local area networks such as ~~Zigbee~~ Zigbee, Bluetooth, Modbus, M-Bus, Powerline Communication, 6LOWPAN and ~~IEEE~~ IEEE 802.15, 4-LR WPAN etc.

→ M2M area network uses either proprietary or non-IP based communication but the communication network uses IP based network.



M2M Gateway



→ Since Non-IP based protocols are used within M2M area network.

→ The M2M nodes within one network cannot communicate with nodes in an external network.

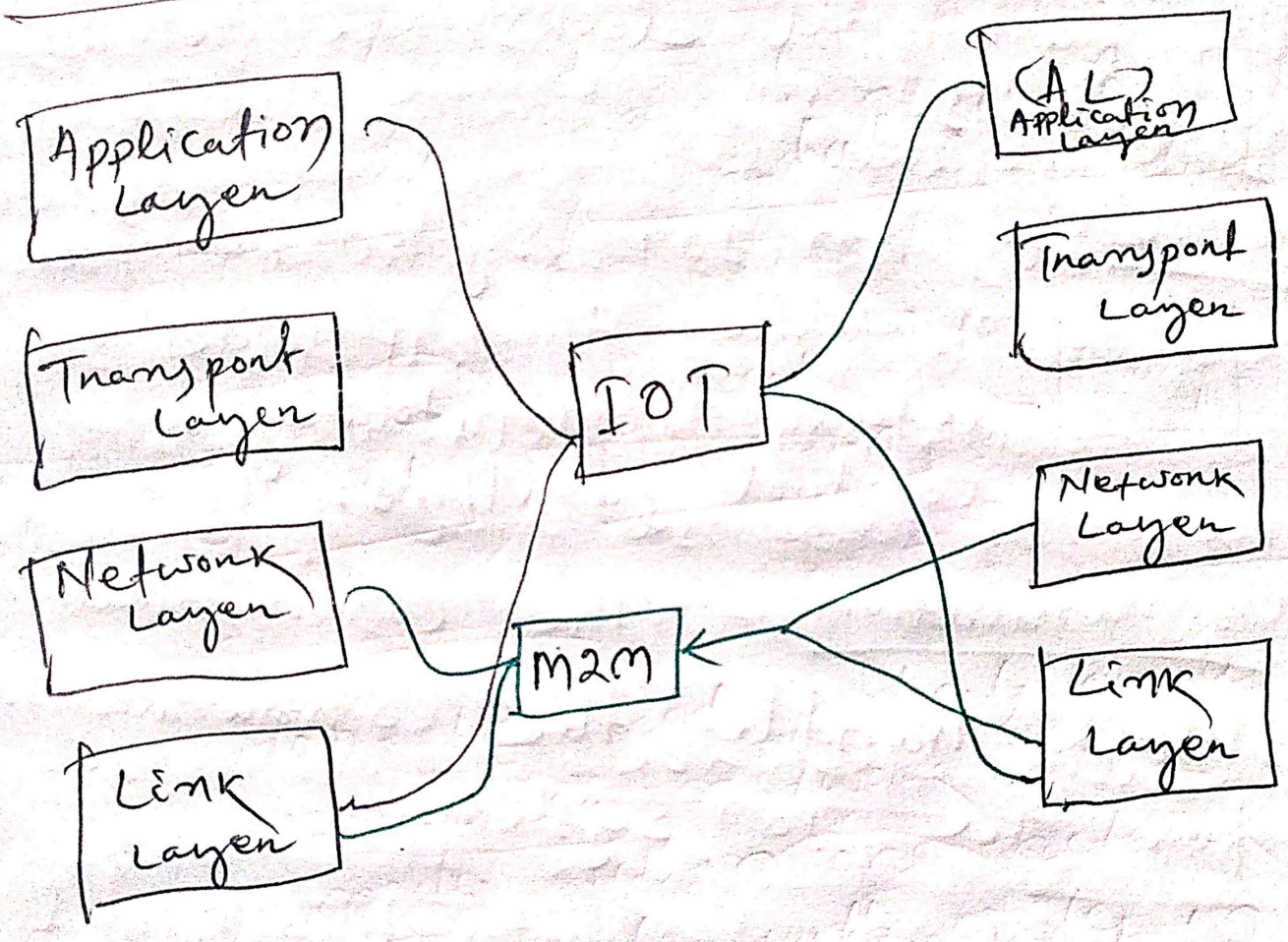
→ To enable communication between remote M2M networks, M2M gateways are used.

Difference between IOT and M2M

* Different between M2M and IOT

M2M	IOT
① Non-IP based in proprietory communication protocol used in m2m area network and gateway enables communication with external network	① IP based communication protocol is used.
② Homogeneous machine types.	② Things in IOT are physical object having unique identification.
③ Communicate via gateway.	③ Things can directly communicate with integrated network.
④ Communication is between machine	④ Can communicate with user application
⑤ More emphasises on Hardware	⑤ More emphasis is on software.
⑥ Data ~~communication~~ collection analysis is done at the machine	⑥ Data collections analysis is done at the cloud.

Communication Protocols in IOT VS M2M



IOT Functional Blocks

→ The functional blocks are described as follows.

Device :- An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.

Communication :- The communication block handles the communication for the IoT system.

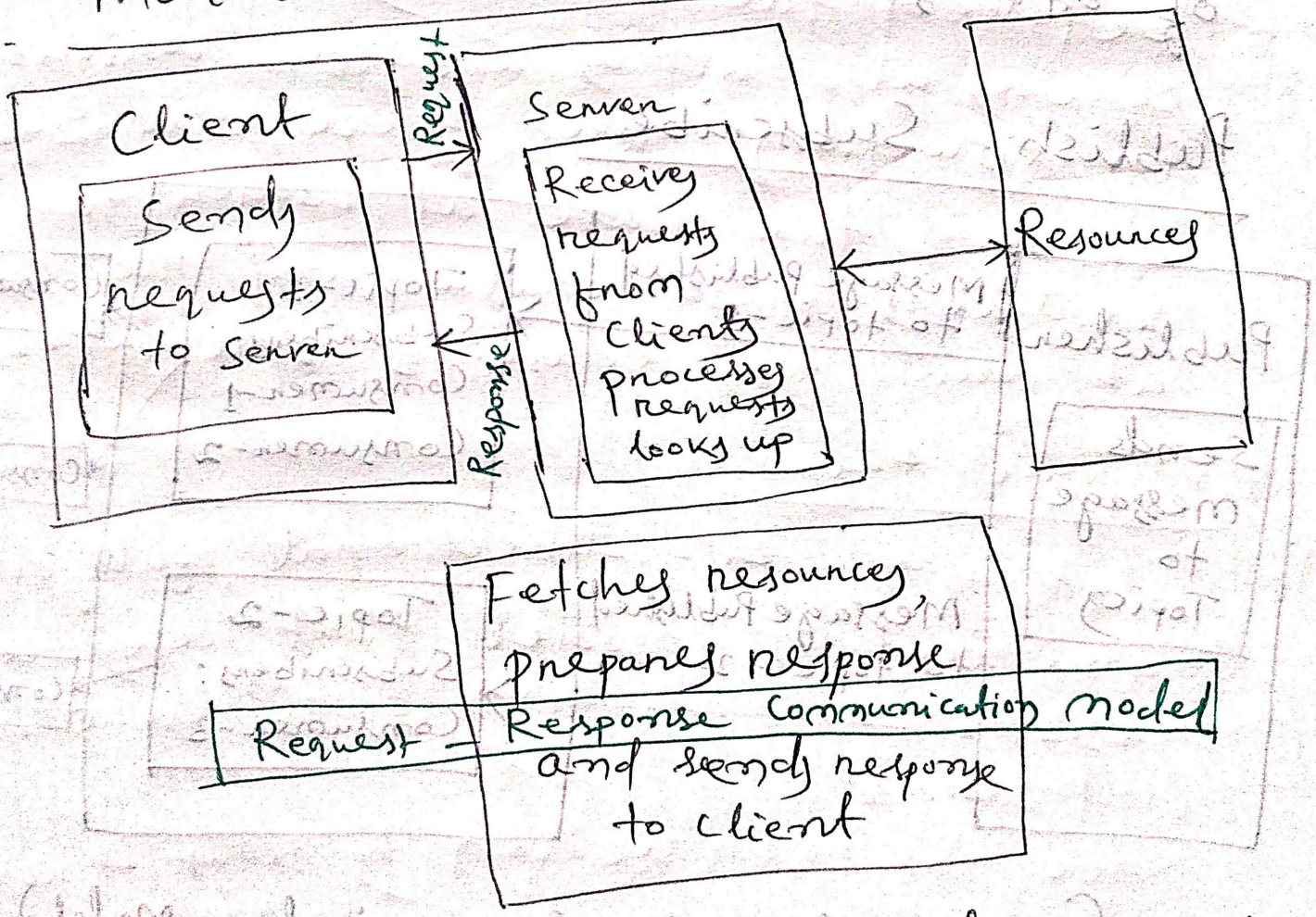
Security :- Security functional block secures the IoT sylten and by providing functions as authentication, autonization message and content integrity and data security.

Application :- IOT applications provide an interface that the users can use to control and monitor various aspects of the IOT system.

Services :- An IoT system uses various types of IoT services such as services for device monitoring, device control services, data publishing services and services for device discovery.

IoT Communication Models

① Request - Response Communication model

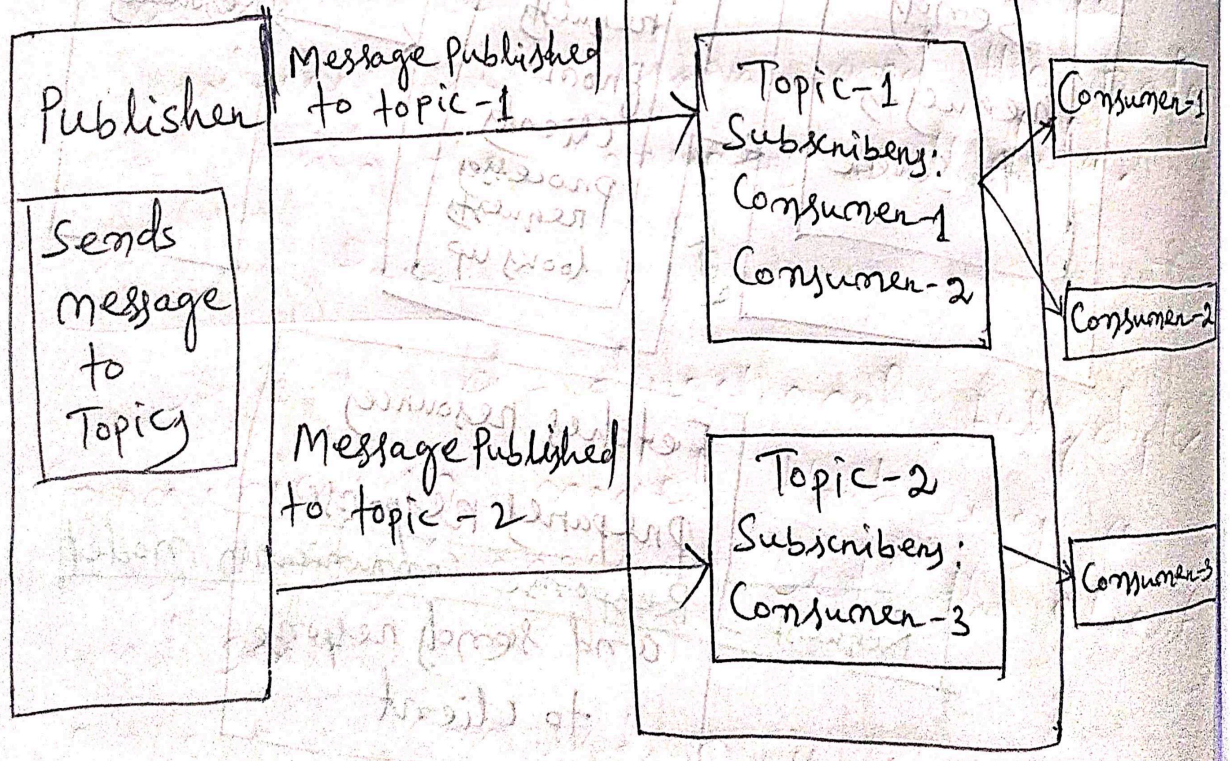


* Request-Response is a communication model in which the client sends request to the server and the server responds to the requests.

* When the server receiving a request, it decides how to respond, fetches the data, retrives resources representation, prepares the response and then sends the response to the client.

* Request - Response model is a stateless communication model and each request - response pair is independent of others.

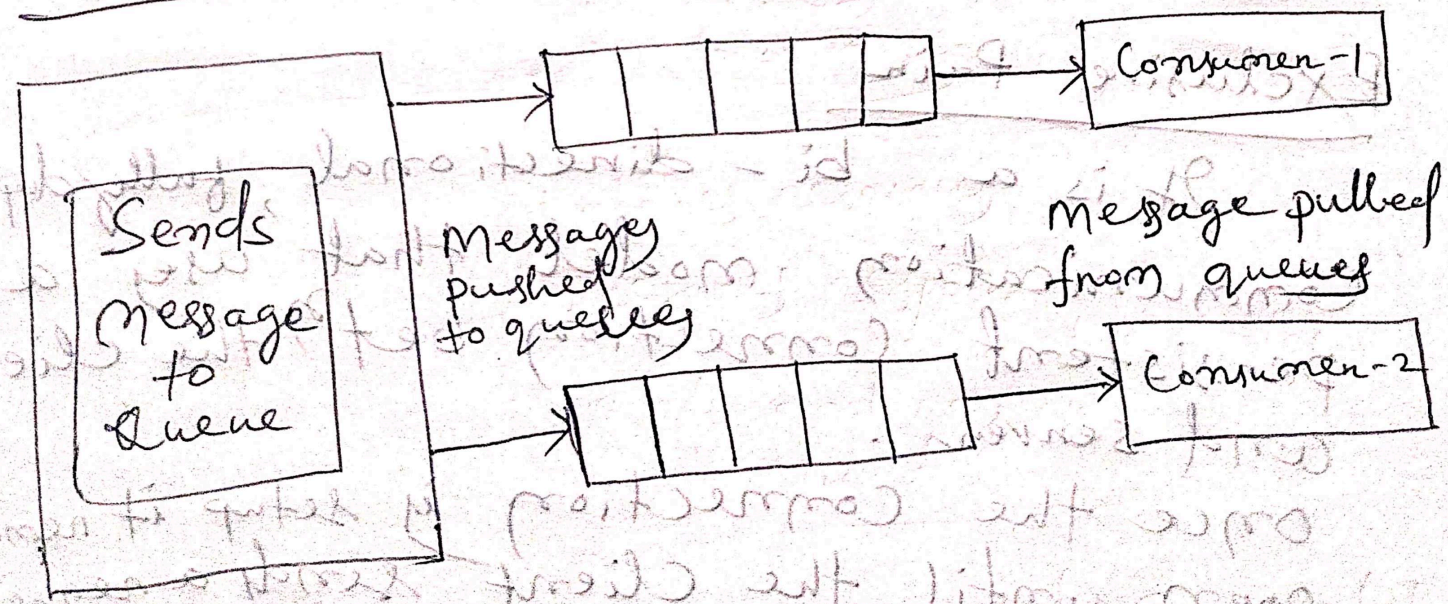
Publish - Subscribe



(Publish - Subscribe Communication Model)

→ It is a communication model that involves publishers, brokers and consumers.
→ Publishers are the source of data.
→ Publishers send the data to the topics which are managed by the broker. Publishers are not aware of the consumers.
→ Consumers subscribe to the topics which are managed by the broker.
→ When the broker receives data for a topic from the publisher, it sends the data to all the subscribed consumers.

Push - Pull

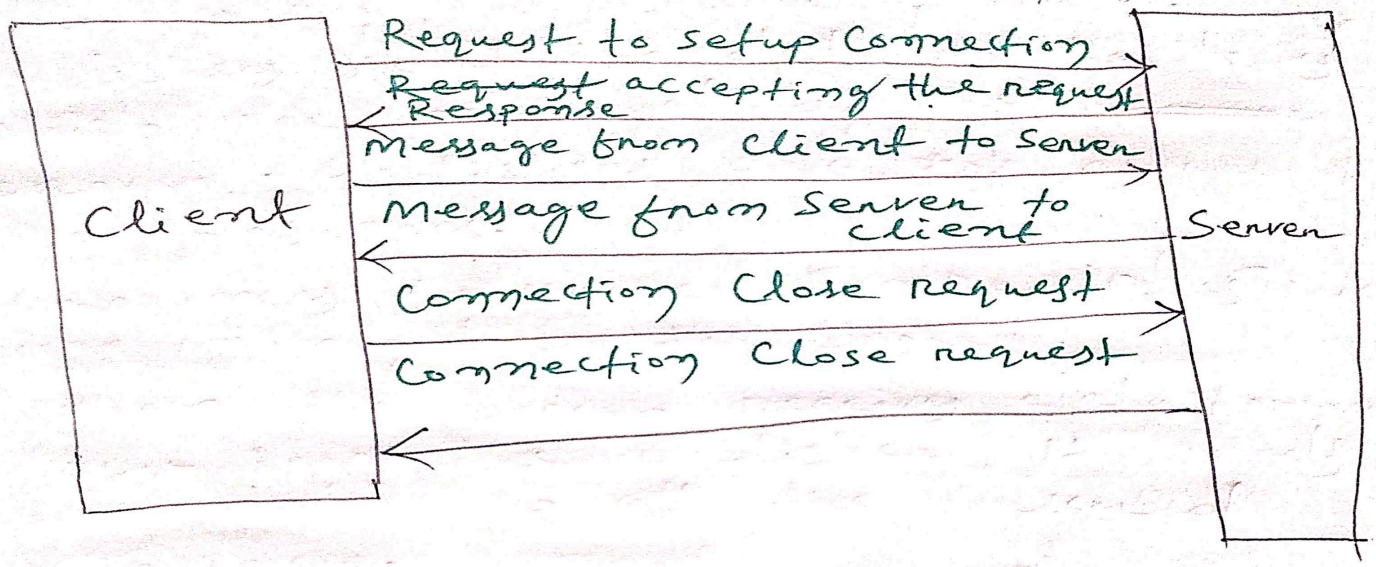


It is a Communication model in which the data producers push the data to queues and the consumers pull the data from the queue.
Producers do not need to be aware of the consumers.
Queue help in decoupling the messaging between the producers and consumers.
Queue also act as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate at which the consumers pull data.

Exclusive Pair

It is a bi-directional, fully duplex communication model that uses a persistent connection bet^n the client and server.
Once the connection is setup it remains open until the client sends a request to close the connection.
Client and server can send messages to each other after connection setup.

It is a stateful communication model and the server is aware of all the open connections.



IOT

✓ IOT stands for Internet of things.

✓→ It is a network of connected devices that can communicate with each other & with other system. actuators & softwares.

→ Each capable of dynamically generating, analysing & communicating intelligence that can be use to increase operational efficiently & Power new business models & make like more easier & comfortable.

* Application of IOT

① Home Automation:

a. Smart lighting — It helps in saving energy by adapting the lighting to the ambient conditions & switching on/off the light when need

b. Smart appliances:

To make the management easier & also Provid status information to the users remotely.

② Cities

a. Smart Lighting: For roads, Parks & buildings can help in saving energy.

b. Structural health monitoring: It use a network of sensors to monitor the vibration in the structures such as bridges & buildings.

③ Environment

a. Forest fire detection: Forest fire can cause damage to natural resources, Property & human life.

b. River flood detection: River flood can cause damage to natural & human resources & humanlife.

Early warnings of floods can be given by monitoring the watch level & flow rate.

(4) Energy

a. Renewable energy systems:

IoT based integrated systems with the transformers at the point of interconnection measure the electrical variables.

b. prognostics:-

On systems such as power grids, the real-time information is collected using specialized electrical sensors called Phasor measurment units (PMU's) at the substations.

(5) Retail:

a. Inventory Management:

IoT Systems enable remote monitoring of inventory using data collected by RFID readers.

b. Smart payments: Solution such as contact, less Payments powered by technologies such as near field communication (NFC) & bluetooth

6. Logistics:

a. Fleet Tracking: Use GPS to track locations of vehicles in real-time.

b. Route generation & scheduling:

IoT based system backed by cloud can provide first response to the route generation queries can be scaled upto serve a large transportation network.

7) Agriculture:

a- Smart irrigation: To determine moisture amount in soil.

b- Green house control: To improve productivity.

8) Industry:

a- Machine diagnosis & prognosis

b- Indoor air quality Monitoring

9) Health & Lifestyle:

a- Health & fitness Monitoring

b- Wearable Electronics

* Characteristics of IOT

Dynamic & Self adapting → It can adapt to the environment.

Ex: A survillence system can adapt no. of Cameras dynamically.

Self configuring

Device can configure themselves in associati with IOT infrastructures.

EX: Set of networking, fetch latest software update with minimal user.

Interoperable communication protocols

It support different protocols for different devices & which is interoperable.

unique identity

IP address & URL are used for identity.

Integrated into information network:

IOT devices can be dynamically discovered in the network by other devices & have the capability to describe themselves to other devices or user application.

* Architecture Overview:

→ On an internet of things (IOT) technology has a wide variety of applications.

→ It has use of internet of things is growing so faster.

→ It depends upon different applications areas of internet of things (IOT)

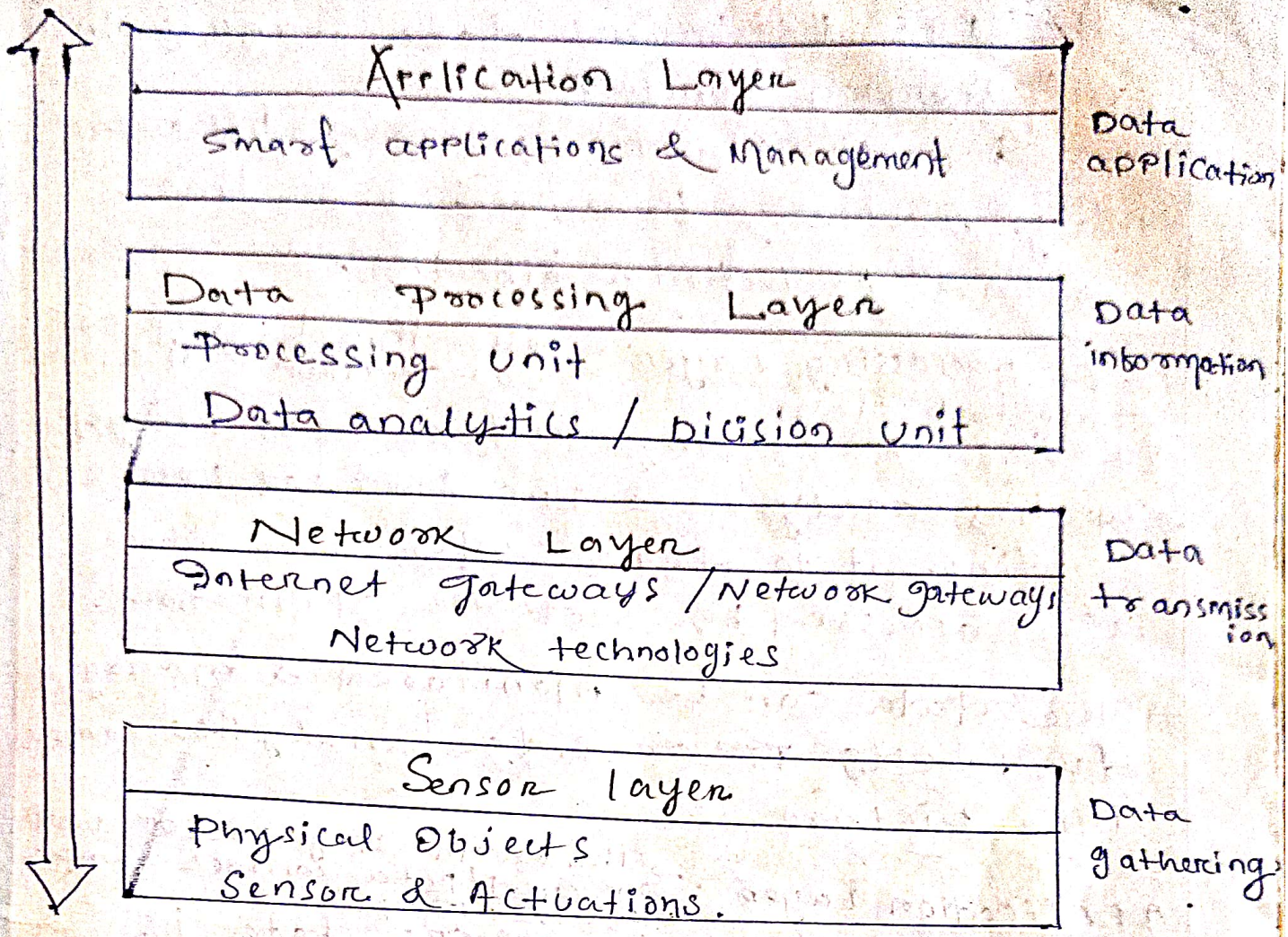
→ It work accordingly as per it has been designed / developed.

→ It is strictly followed by universally.

→ It depends upon its functionality & implimentation in different sectors.

→ There is basic process flow based on IOT.

Architecture overview



The above architectural overview is 4 layers

It can divided as follows

- → Sensing layer
- → Network layer
- → Data processing layer
- → Application Layer

Sensing layer → The first stage of IoT includes ~~sensors~~ ~~In this layer~~ sensors, actuators devices are present.

→ This devices accepts data (physical/environmental parameters), processed data & emits data over network.

Network layer → The second stage of the IoT consist ~~in this layer~~ internet / network gateways, data acquisition system (DAS) are present

- The DAS performs data aggregation & conversion function.
- The internet network gateway performs many gateway functionalities like, Malware protection & filtering.

Data processing Layer: →The third stage of IOT consist is the most important stage.
- It has processing unit of IOT ecosystem.
→ It has analyzed & pre processed before sending it to data center from where data accessed by software applications.
→ The data can be monitored & managed due to edge 'IT' or edge analytics comes into picture.

APPCication Layer: →The fourth stage of IOT consist of cloud/Data centres ~~where data is manage~~.
The data centers where data is managed & it's used by end user applications.
→ Like agriculture, healthcare, aerospace, farming, defense etc.

* **Sensor:**
It is a device used for the conversion of physical characteristics ito the electrical signal.
→ This is a hardware device that takes the input from environment & gives to the system by converting it.

Ex: Thermometer takes temperature as physical characteristic & then converts it into electrical signals for the system.

* **Actuator:**

2m

→ It is a device that converts the electrical signals into the physical characteristics.

→ It takes the i/p from the system & gives output to the environment.

→ EX: Motors & heaters are some of the common used actuator.

* **Difference between M2M & IOT**

M2M	IOT
(1) M2M Stands for Machin to machine.	(1) IOT Stands for Internet of things.
(2) Non IP based in ~~Property~~ Proprietory communication Protocol used in M2M area network & gateways enables communication with external networks.	(2) IOT based communication Protocal is used.
(3) Homogeneous machine types.	(3) Things in IOT are physical objects having unique identification.
(4) communication is in between machines.	(4) Things can directly communicate with integrated network.
(5) communication via gateways.	(5) Communication with user application
(6) More emphasis on hardware.	(6) More emphasis on Software
(7) Data collection analysis is done on at the machine	(7) Data connection analysis is done at the cloud.

Dt - 11/02/25

M2M (Machine to Machine)

Machine to machine refers to direct communication between a machine or devices using any communication channel including wired & wireless.

→ It is a networking of machine for the purpose of remote monitoring, control & data exchange.

→ M2M ~~are~~ comprises machine to machine nodes which has embedded hardware modules. For sensing, actuation & communication

→ Wireless communication protocols can be used in M2M local area networks (LAN) such as 'Zigbee' bluetooth, Modbus, M-bus.

→ Power line communication (Low Plan & IEE 802.15. 4LR-WPAN etc.

- M2M area networks uses either properties or non IP based communication but the communication on network uses IP based network.

M2M gateway

Since, non IoT based protocols are used with in M2M area network.

→ The M2M nodes with in one network can't communicate with nodes, in an external network.

→ To enable communication between remote M2M networks & M2M gateways are used.

Date - 15.02.25

Difference between M2M & IOT technology.

M2M	IOT
1. M2m is machine to machine	1. IOT is internet of things.
2. Uses fixed-IP-SIM card.	2. Uses fixed-IP sim card.
3. Mainly used for automation	3. Used for remote maintenance & control
4. Less scalable	4. very scalable
5. Doesn't necessarily use the cloud.	5. Uses cloud Platform.
6. Uses either an internet or non-internet connection	6. Uses the internet & cellular networks.
7. more emphasis on hardware.	7. More emphasis on software
8. Communication is in between machines	8. Communication with user application.

Data management, Business Processes in IOT:

In IOT environment, data management business ~~Proce~~ Process encompass, the practices of collecting, storing, processing, analyzing & securing vast amounts of data generated by connected devices.

→ Ensuring its accuracy, accessibility & integration into business operation to make informed decisions

→ Involving real-time analytics & advanced data governance strategies to maintain data quality & privacy across entire lifecycle.

Key components of data management:

Business Process in IoT:

Data collection: Gathering data from various IoT Sensors & devices, including real-time Streaming data, Considering factors like data volume, frequency, device capability.

Data Processing:
Cleaning, filtering, normalizing raw data to ensure consistency & quality before further analysis.

Data storage:

selecting suitable storage solutions based on data volume, access requirements & including cloud-based storage.

Data Security:
Implementing robust security measures to protect Sensitive IoT data from unauthorized ~~access~~ access cyber threats.

Data Integration: combining data from multiple sources (IoT devices, external APIs, internal systems) into a unified format for analysis.

IoT data Management

Smart Home Automation:
managing home appliances and lighting based on user preferences & environmental conditions.

Smart Manufacturing:
Monitoring Production processes on the factory floor to identify inefficiencies & improve quality control.

Challenges in IoT data management:
Data Privacy: Protecting Sensitive user data generated by IoT device.

Data quality: Maintaining data accuracy and consistency across different devices & system

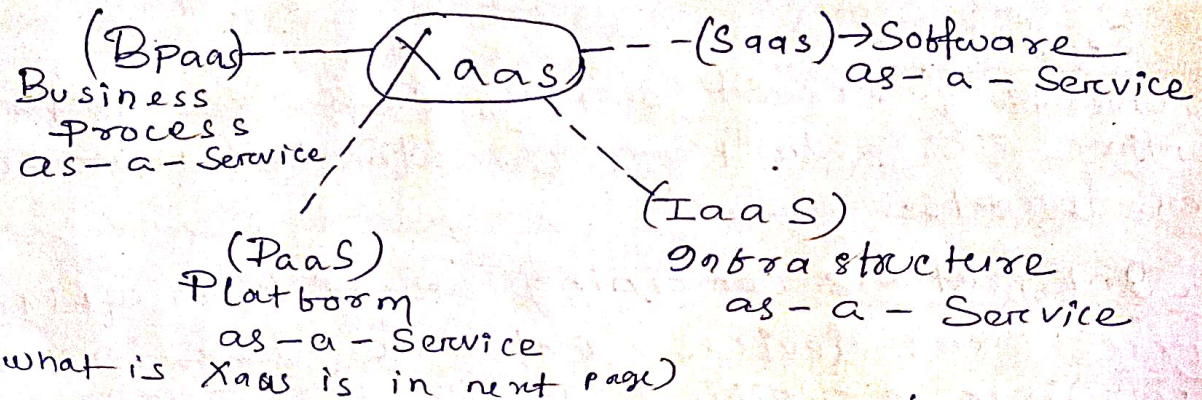
How it works:

- Uses sophisticated tools for real-time analytics.
- Ensures data quality.
- Maintains privacy & security standards.
- Includes policies, technologies & practices
- Requires a planned strategy to ~~not~~ handle large amounts of diverse data.

Benefits:

- Helps organizations make sense of large amount of data.
- Helps organization make informed decisions.

* Everything as a service (Xaas)



(what is Xaas is in next page)

Bpaas: In the context of IOT 'Bpaas' stands for "Business process as a service"

→ It means a cloud-based service that allows companies to outsource and automate various business processes related to their IOT devices, data ~~flow~~ analysis, management

Cloud based delivery

→ Bpaas services are hosted on the cloud.

→ Allowing companies to access & manage their IOT data & processes from anywhere with an internet connection.

Examples Bpaas applications in IOT

Smart building Automation:

Analyzing sensor data from industrial machines to predict potential failures & schedule preventative maintenance.

1. Smart building automation
2. Supply Chain management
3. Predictive Maintenance.

XaaS: (Anything-as-a-Service) is a cloud-computing model that delivers Products, services or resources over the internet.

→ XaaS is divided in various types
- (i) SaaS
- (ii) PaaS
- (iii) IaaS
- (iv) BaaS (Software as a Service)

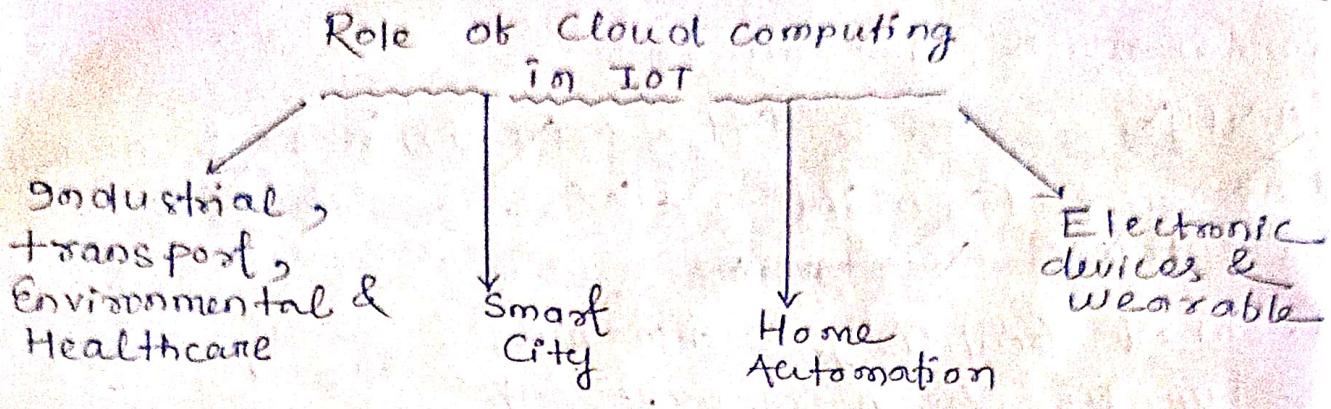
→ SaaS → Applications hosted in the cloud that users access through a web browser or mobile app.

→ PaaS → (Platform as a Service): A cloud environment that includes servers, operating systems, networking, storage & tools.

→ IaaS → (Infrastructure as a Service): On-demand access to IT infrastructure components, such as storage, processing power & computing.

→ XaaS has grown in popularity due to the convergence of technologies like 5G, AI & machine learning.

* Role of cloud in IOT ; Security aspects in IOT



Cloud computing :

Cloud computing provides the infrastructure for the (IOT) by storing, processing, & analyzing data from connected devices.

→ This allows for real-time in-sights, efficient data management & scalability.

How cloud computing Helps IOT :

Data Storage: Cloud computing provides space to store the large amounts of data generated by IOT devices.

Real-time insights : cloud computing provides real-time insights from data

Data exchange: Cloud computing ~~Provides tools for~~ allows devices to share data securely with other parties.

Data Analysis: Cloud computing provides tools for analyzing data to make devices work better.

Applications

IOT & cloud computing applications are used in many industries, including healthcare manufacturing, Smart cities, home automation electronic devices & wearable etc.

5 mark 2021

Security aspects in IOT.

Security aspects of the IOT include data encryption, authentication & network protection.

Security in IOT

- Privacy → Keeping the Personal information including healthcare data safe.
- Trust → Make a mutual trust among Providers & People for data interaction
- Data confidentiality → Guaranteed that only authorized entities can access & modify data

IOT Security threats

→ Surveillance: Unauthorized access to IOT data can lead to surveillance.

→ Identity theft: unauthorized access to IOT data can lead to identity theft.

IOT Security solutions

→ Software solutions that Protect IOT devices & hubs from unwanted access.

→ Automated tools for device discovery & maintaining an inventory.

2. Elements of IOT

Hardware components - computing (Arduino, Raspberry Pi)

Raspberry Pi: It is a small, inexpensive computer, that is used for learning programming & exploring computing.

→ It is the name of a series of single board computers.
→ It launched in 2012.
→ It is also called as single board mini computer
→ Raspberry Pi is a low-cost mini computer with the physical size of a credit card.
→ It is a very chip computer, that runs linux but it also provides a set of GPIO (general Power i/p o/p) pins that allow the control electronic components for physical computing.

~~Features~~

→ can be used to learn programming language like Python & Scratch.
→ It have been three generations, such as Pi 1, Pi 2, Pi 3 ~~& there has been a model~~

Applications

Music machine
Weather stations
Tweeting birdhouses with infrared cameras
programming skills
Build hardware project
Home Automation
Industrial application
Browsing the internet
Playing games
Developing IOT based application

History

- The raspberry pi foundation developed the first raspberry pi computer in UK.
- The raspberry pi foundation's goal was to promote basic computer science in schools.
- Raspberry pi Ltd has developed all Raspberry pi products since 2012.

What is Raspberry pi used for.

The Raspberry Pi is a small in expensive computer that can be used for many purpose including Robotics, Home automation, Teaching, Computer Science.

- Home automation → It create a smart home hub, smart speaker.
- Robotics: Use it to build robotic & robotics command centers.
- Teaching: Use it to teach programming & physical computing.
- Data analysis: Use it to develop systems for data organisation, device management & data analysis.

Features

- Low cost
- Open design,
- Can connect to monitor mice, & keyboard

Parts of Raspberry Pi:

Processor & RAM: Raspberry Pi is based on an ARM process. The latest version (Model B, 2) comes with 700MH low power ARM 1176JZ-F processor & 512 SDRAM.

USB ports:
Raspberry Pi comes with two USB 2.0 ports, It can provide a current upto 100MA.

Ethernet port: Raspberry Pi comes with a standard RJ45 Ethernet port. You can connect an ethernet cable to provide internet connecting.

HDMI Output:
It can provides both video & audio o/p. You can connect to a monitor computer using an HDMI cable.

Composit Video Output : The composit video o/p with an RCA jack that support both PAL & NTSC video output.

Audio Output : Raspberry Pi has a 3.5mm audio o/p jack.

GPIO Pins : It is a general purpose i/p o/p pins There are 4 types of pins on Raspberry Pi ; ~~there~~ GP IO pins I_2C interface pins, SPI interface pins & Serial RX & TX pins.

Display Serial Interface (DSI) : It can be used to connect an LCD panel to Raspberry Pi.

Camera Serial Interface (CSI) : - It can be used to connect a camera module to raspberry Pi.

Status LEDs : It has five status LED.

SD card slot : Raspberry Pi doesn't have a built in operating system & storage you can plug-in an SD card loaded with a linux image to the SD card slot.

Power input : It has a micro-USB connector for power input.

Raspberry Pi Status LEDs

Status LED	Function
ACT	SD card access
PWR	3.3V Power is present
FDX	Full duplex LAN connected
LNK	Link/Network activity
100	100 mbit LAN connected

9mp
2022-2024

Arduino

Arduino is an open sources electronics platfor based on easy to use hardware & software.

Application

→ Arduino boards are able to read inputs such as light on a sensor, a finger on a button or a message & turns it into an o/p activating a motor turning on LED, publishing on line etc.

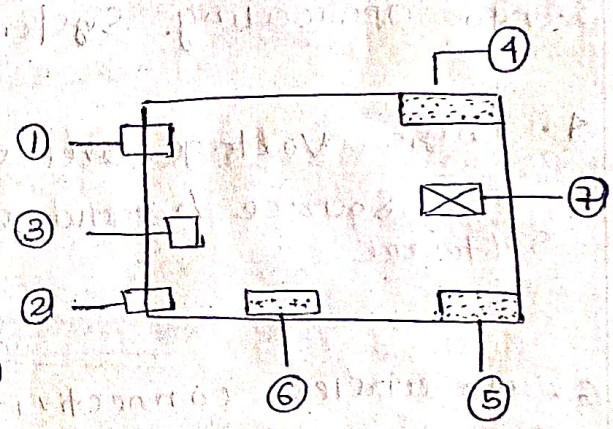
→ We can tell the boards what to do by sending a set of instruction to the microcontroller on the board.

Programming language:

Arduino software (IDE) can be used to write progragram for giving instructions.

Important Ports of Arduino board

1- USB connector
2- Power connector
3- Automatic power switch
4- Digital pins (i/p or o/p)
5- power pins
6- Reset switch
7- Analog pins (i/p or o/p)



Advantages of Arduino:

Inexpensive

→ Arduino boards are relatively inexpensive. compare to other microcontroller platform.

→ the rest is less than 50 US.

Cross Platform:

Arduino software ID seen on windows machines & linux os.

Simple clear programming environment:

It is easy to use for beginners & flexible enough for advance user

Open Source & extensible software:

The arduino software is published as a open source tool.

→ The long can be expanded through c++ libraries.

→ It is based on AVR C programming language.

open source & extensible hardware:

The CKt design can make their own version of the module extending the arduino boards & improving it.

Difference between Arduino & Raspberry Pi:

Arduino	Raspberry Pi
1. Development CKt board.	1. Single board computer
2. Based on microcontrollers.	2. Based on microprocessor
3. No operating system.	3. Raspberry Pi OS (Linux distribution based on debian)
4. Logic voltage level 5V	4. Logic voltage level 3.3V.
5. Open source hardware & software	5. close source hardware & software. can't be altered by the general public.
6. No wireless connectivity on the board.	6. Wifi - Blue tooth connectivity on the board.
7. can be programmable in C or C++	7. Run by programmed in Python, Scratch, Ruby C or C++.
8. Need arduino shields to connect to the internet	8. Can connect to the internet through wifi or ethernet.

* Communication

I/O Interface

An I/O interface or input/output interface is a connection point that allows data to be transferred betⁿ a device & external devices.

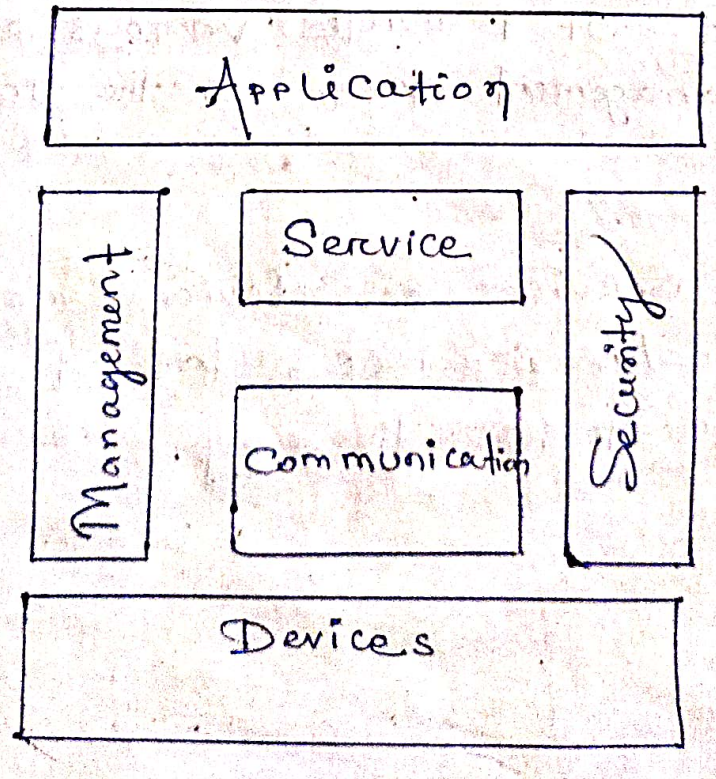
→ It is a vital part of computing, that enables communication between a computer & the outside world.

How does I/O Interface Work:

- The I/O interface manages data transfer between the computer's CPU or internal memory & external device.
- It support Serial & parallel communication, & converts signal to ensure compatibility between devices.
- It can synchronize the operating speed of the CPU to peripherals.
- It selects the peripherals appropriate for the interpretation of the i/p – o/p devices.

Examples of I/O devices: Keyboards, Mouse, Printer, Monitor.

* IOT Functional Block diagram ~~of~~ ~~IOT~~.



The functional blocks are devices are Device, communication, Security, Application, management & services.

Device:
An IOT system comprises of devices that provide Sensing, actuation, Monitoring & control functions

Communication:
The Communication block handles the comm for the IOT System.

Security:
This block secure the IOI system & by providing functions as authentication, authoriz tion, message & Contaiint, integrity & data security.

Application: IOT applications provide an interface that the users can use to control & monitor various aspects of the IOT system.

Management: It provides various functions & data management to govern the IOT System.

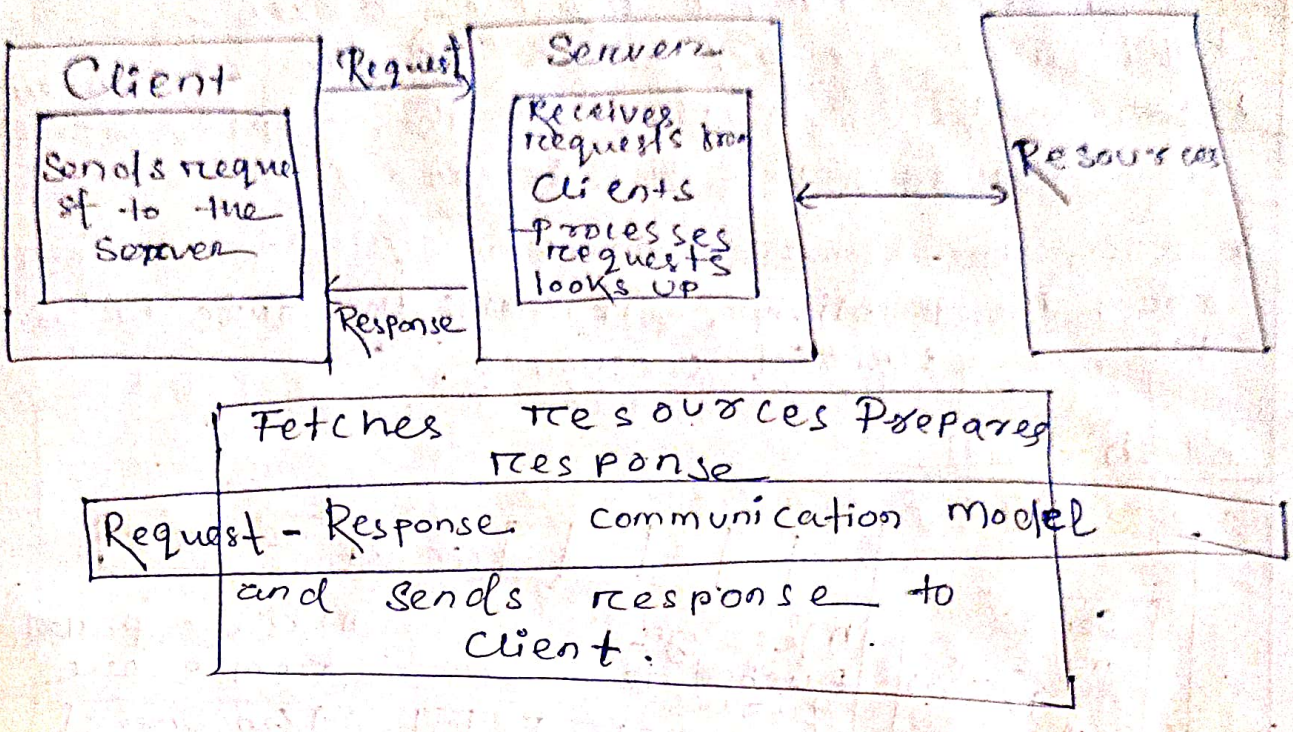
Services:
In this block Services for devices monitoring, device control services, data Publising Services & device discovery.

D-1 - 28.02.25

10 mark 2024

IOT communication Models:

① Request - Response communication model.

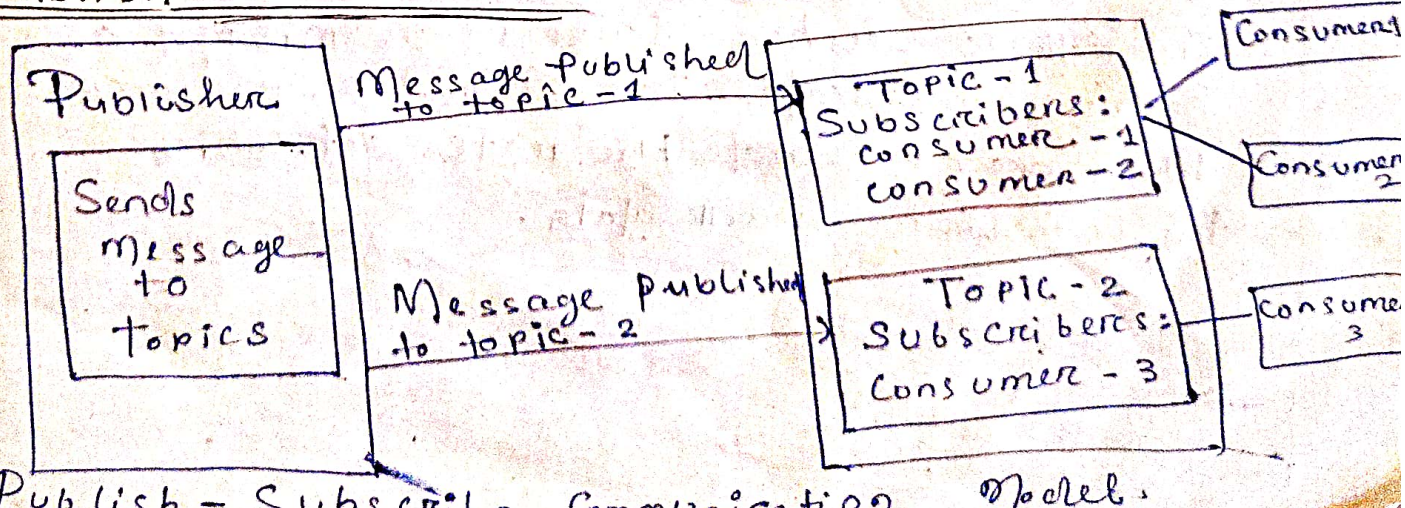


Request: Response is a communication model in which the client sends request to the server & the server responds to the requests.

→ When the server receives a request, it decides how to respond fetches the data, retrieves resources representation prepares the response to the client.

→ **Request:** Response the model is a stateless communication model & each request: Response pair is independent of others.

Publish Subscribe



Publish - Subscribe Communication Model.

→ It is a communication model that involves publishers, brokers & consumers.

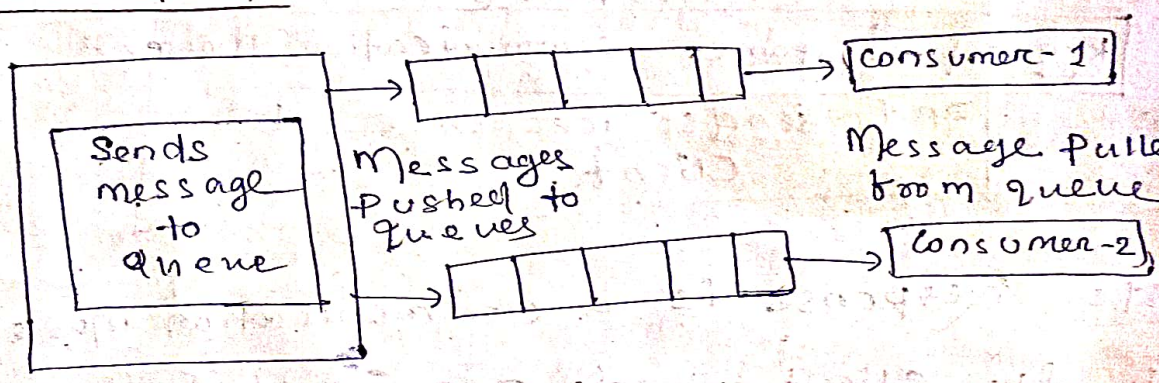
→ Publishers are the source of data

→ Publishers send the data to the topics which are managed by the broker. Publishers are not aware of the consumers

→ Consumers subscribe to the topics which are managed by the broker.

→ When the broker receives data for a topic from the publisher, it sends the data to all the subscribed consumers.

Push-Pull



It is a communication model, in which the data producers push the data to queues & the consumers pull the data from the queues.

→ Producers don't need to be aware of the consumers.

→ Queues help in decoupling the messaging betⁿ the producers & consumers queue also act as a buffer, which helps in situations when there is a mismatch between the rate at which the producers push data and the rate at which the consumers pull data.

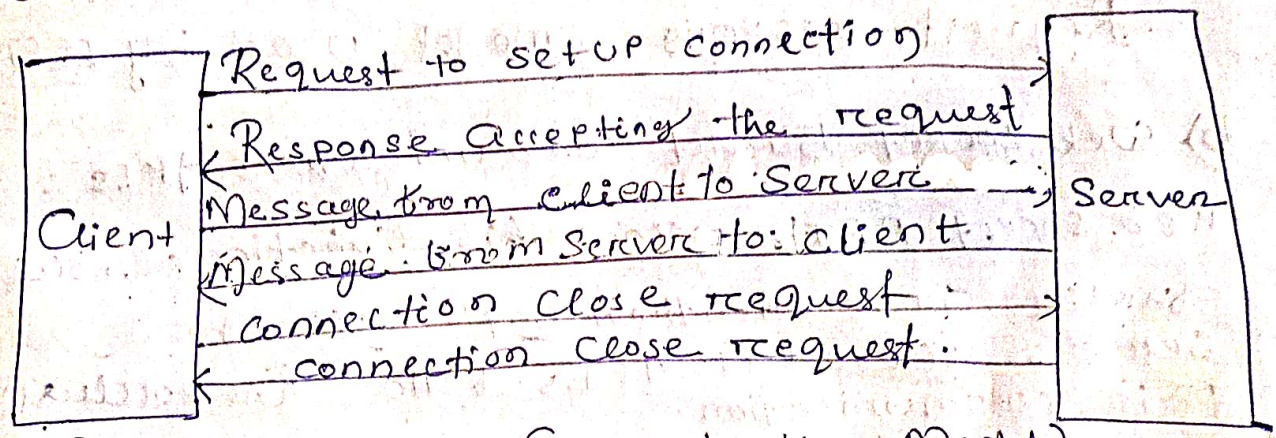
Exclusive Pair :

It is a bi-directional, fully duplex communication model that uses a persistent connection bet^n the client and server.

→ Once the connection is setup it remains open until the client sends a request to ~~help~~ close the connections.

→ Client & server can send message to each other after connection set up.

→ It is a stateful communication model & the server is aware of all the open connections.



(Exclusive Pair Communication Model)

Software components

IOT Communication APIs :

(10) 2021 4022

a. REST based communication APIs (Request - Response Based Model).

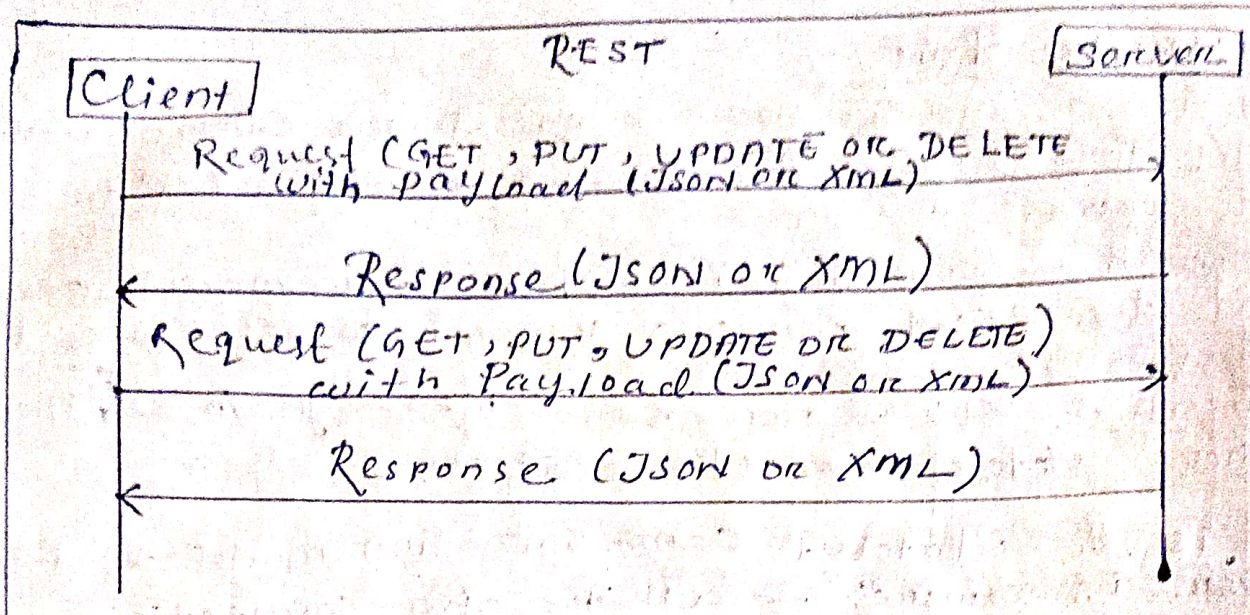
b. Web socket based communication APIs (Exclusive Pair Based Model)

Request-Response model used by REST:

→ RESTful webservice is collection of resources which are represented by URIs. RESTful web API has a base URI.

→ The Client & requests to there URIs using the methods defined by the HTTP protocol e.g. (GET, PUT, Post or DELETE)

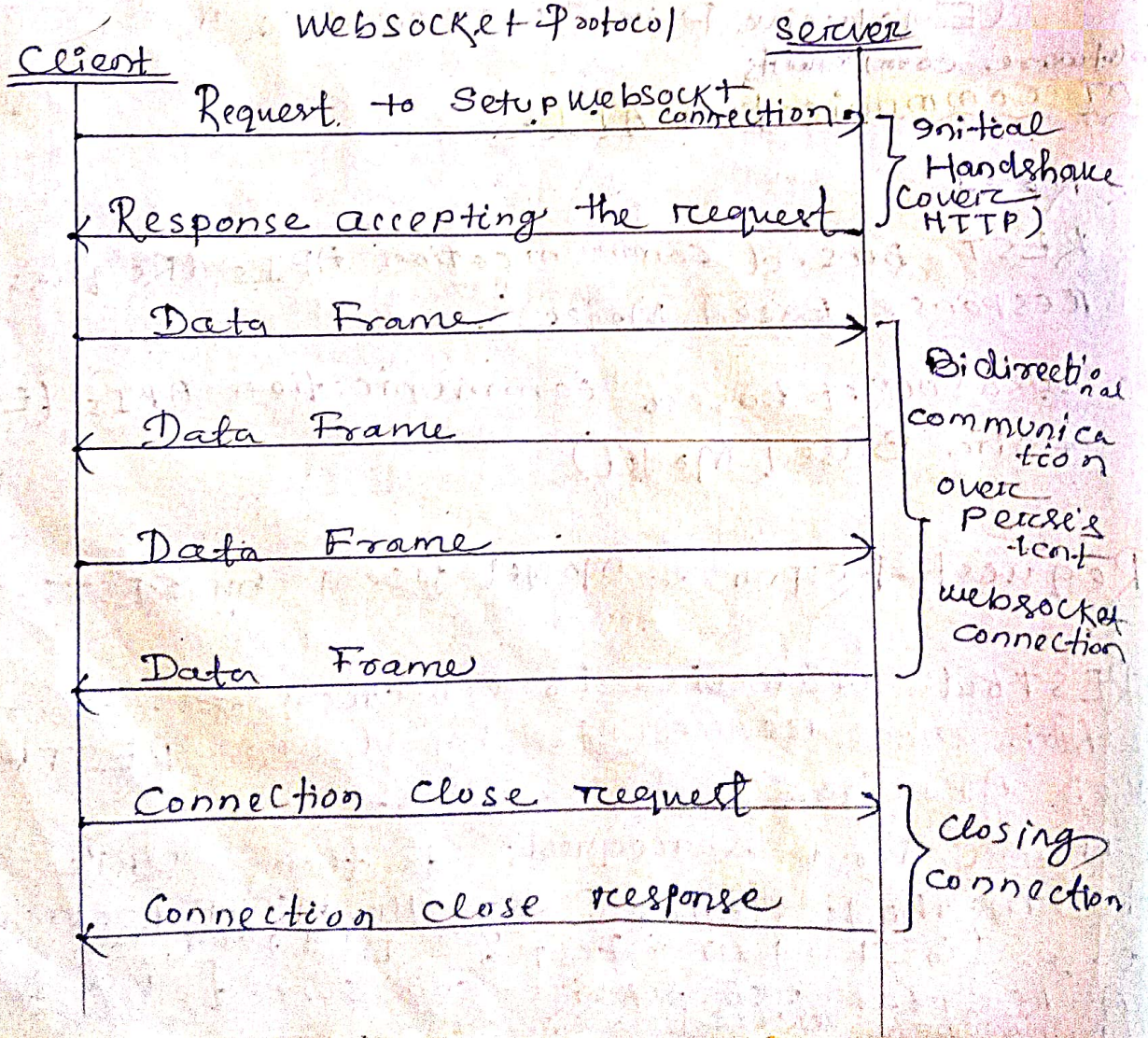
→ A RESTful web service can support various



Request-response model used by REST

b) Web socket Based communication APIs :

Web socket APIs allow bi-directional, full duplex communication betn clients & servers. Websocket APIs follow the exclusive pair communication.



* Design Principle of IOT:

We understand the design principles of IOT from two perspectives:

(a) Physical design of IOT

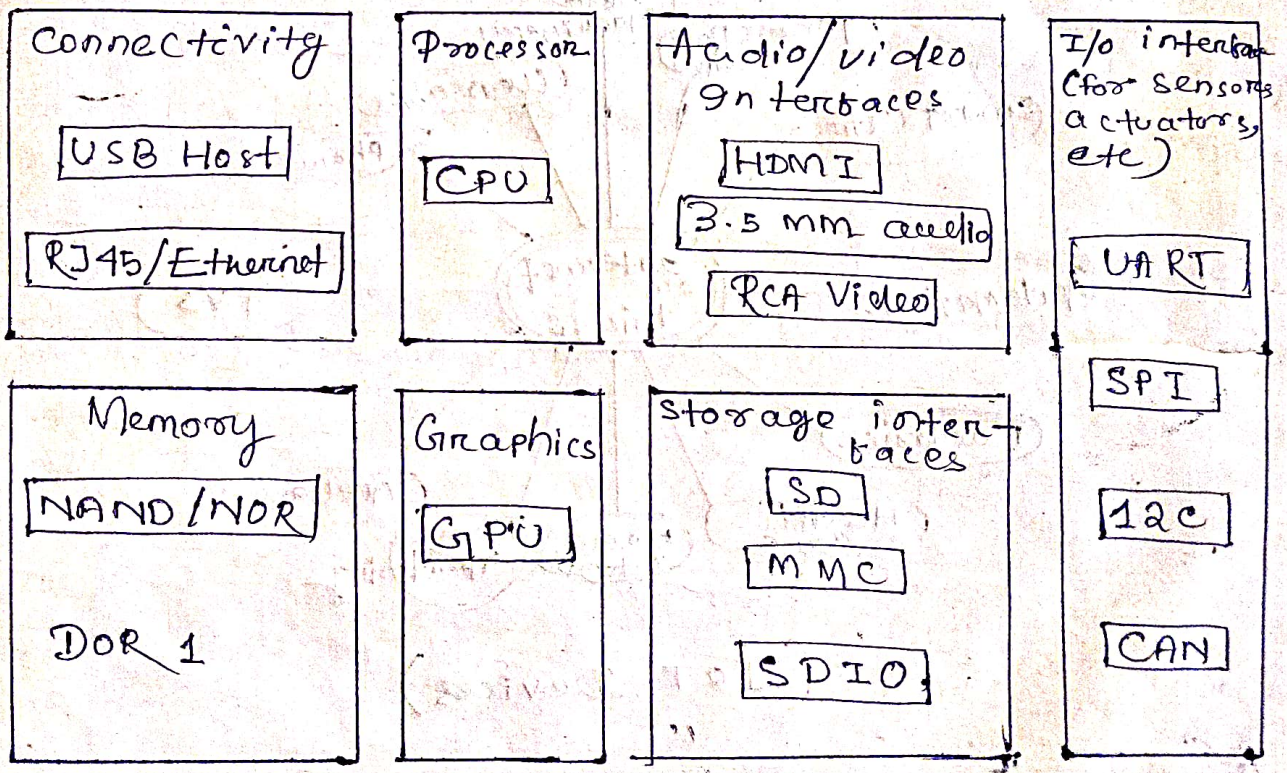
(b) Logical design of IOT

PHYSICAL DESIGN:

(1). IOT devices have a unique identity and they are referred as "Things" A device can perform remote sensing, actuating & monitoring

→ IOT devices can exchange data between them, process it and send it to centralized location for processing & storage.

(2). A generic block diagram or physical design block diagram of IOT devices is shown in the figure..

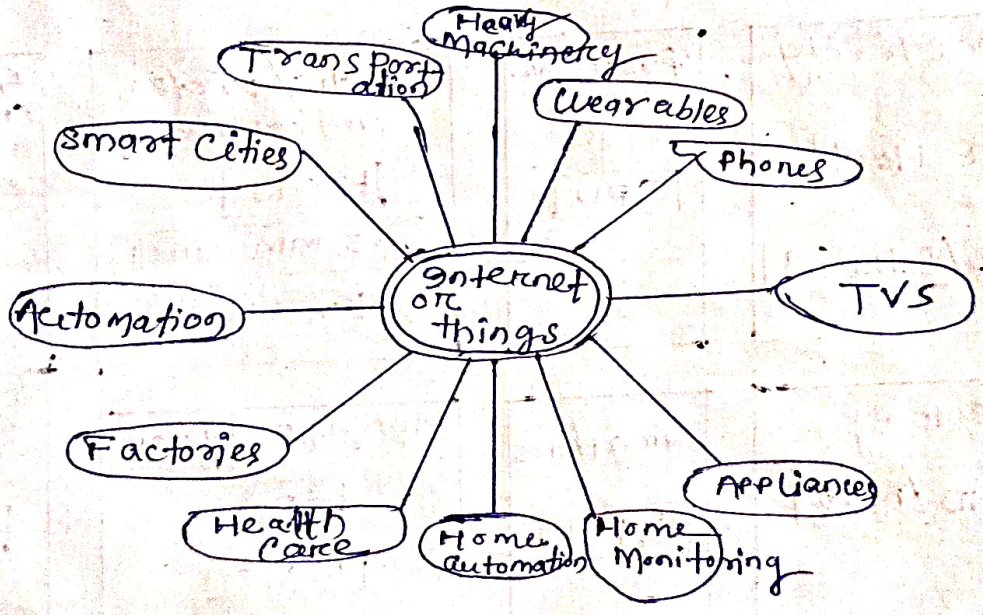


(Physical design block diagram of IOT devices)

3. IOT devices provide interface to various wired & wireless devices. Here, interface includes memory interface, I/O interface, Internet connectivity interface, storage, etc.

4. Using Sensors, IOT collects various types of information like temperature, Pressure, light intensity, humidity etc. Some applications use Cloud-based storage. Collected information is stored in cloud and transmitted to other device

5. Various types of IOT devices are smart clothing, smart watch, wearable sensors, LED lights, automobile industry etc.



(IOT Devices)

Logical Design of IoT : (IoT Functional block diagram)

1. Also called the Functional Model (FM) of IoT, it is derived from internal & external requirements. Functional view is derived from the functional model in conjunction with high-level requirements.

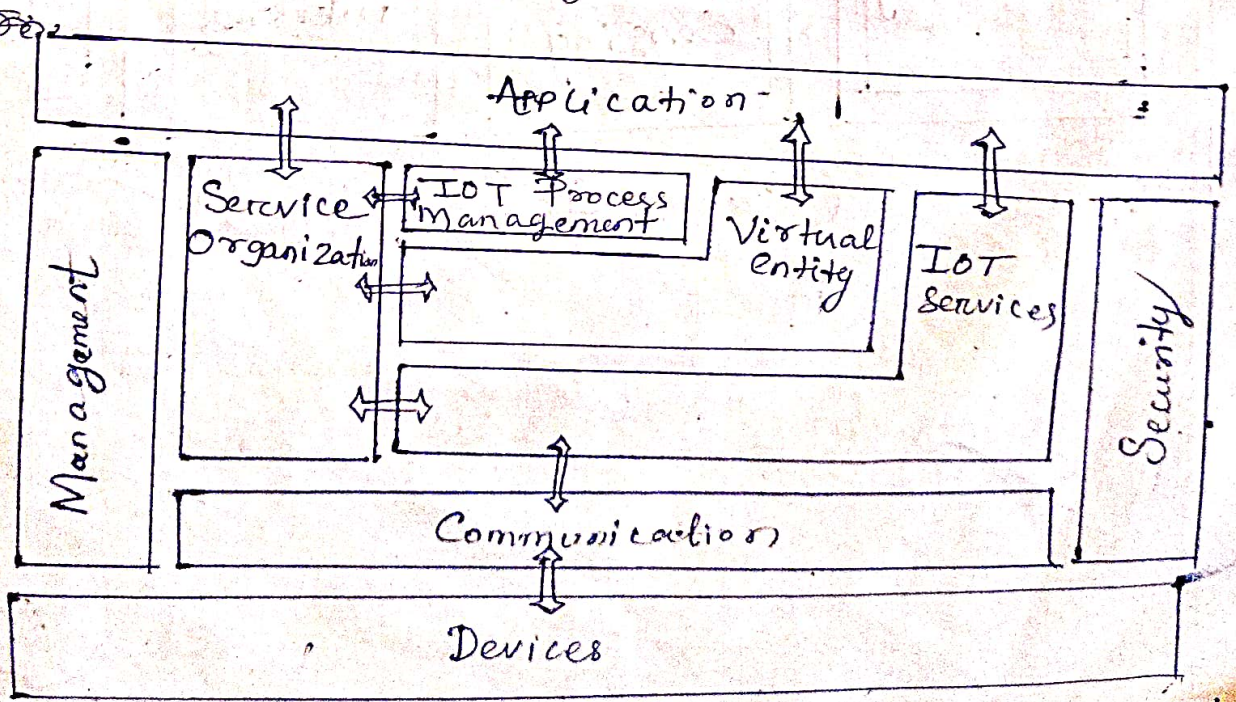
2. IoT functional model identifies "functional group" (FGs) i.e., the group of functionalities grounded in key components of the IoT domain model.

3. Functional model is an abstract framework for understanding the main functionality groups (FG) & their interactions.

4. This framework defines the common semantics of the main functionalities & will be used for the development of IoT - A complaint functional views

5. The functionality model is not directly tied to a certain technology application domain or implimentation.

6. It does not explain what the different functional components are that make up a certain functionality group.



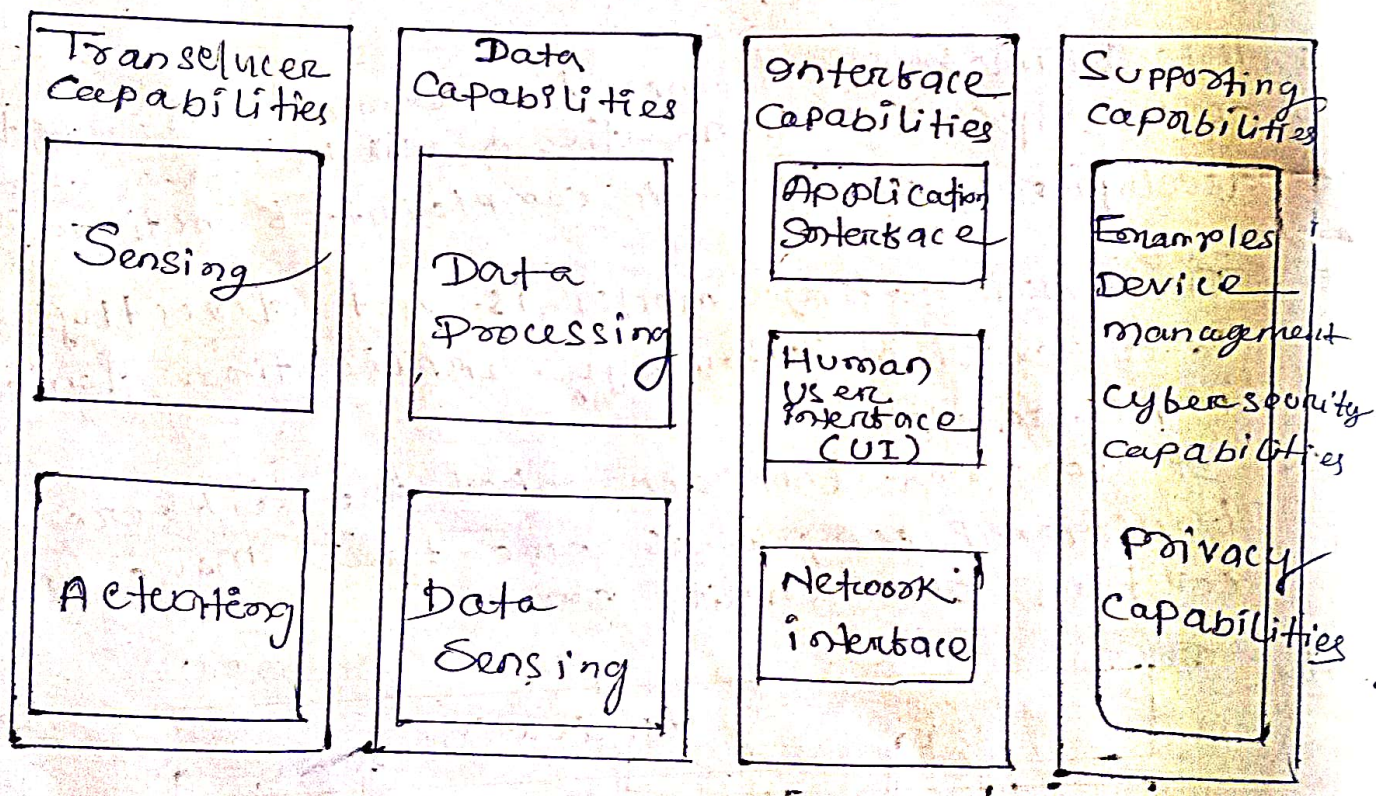
Needed Capabilities of IOT :

Some of the needed capabilities of IOT are shown

→ IOT is a highly dynamic & radically distributed network system. It is composed of a very large number of smart objects producing and consuming information.

→ The main challages associated with the IOT paradigm are as follows.

- Dealing with rapidly changing the environment
- Heterogeneity of devices forming the network
- Lack of human capacity in managing those devices.



(Capabilities of IOT)

These Challenges increase the uncertainty at design time about the operational content of devices in their run-time.

Working of IOT

The working of IOT can be explained as follows.

1. collecting and transmitting data: The device can sense the environment and collect the information related to it & transmit it to a different device or to the Internet.

2. Actuating the device based on triggers: It can be programmed to actuate other devices based on conditions set by the user.

3. Receiving information: Device can also receive information from the network.

4. Providing communication assistance: It provides communication between two devices of the same network or different network.

5. Sensors: For various applications like are used in different application like temperature, humidity, proximity, force etc.

6. Gateway: Takes care of various wireless standard interfaces and hence once gateways can handle multiple technologies and multiple Sensors.

7. The typical wireless technologies: used widely are LoWPAN, Zigbee, Zwave, RFID, NFC etc.

Gateway interfaces with cloud using back. wireless or wired technologies such as wifi, mobile, DSL or fiber.

8. The main goal of IoT is to enable things to be connected anytime, at any place, with anything & anyone ideally using any path/network and any service. It is the new revolution of the internet.

dt - 10.03.25

Protocols:

2022 (S) 2024 (W)

MQTT (Message Queue Telemetry Transport)

- The MQTT is light weight messaging protocol based on Publish subscribe model
- It uses client server architecture well suited for constrained environment.

→ It is a lightweight messaging protocol, designed for low bandwidth, high latency, or unreliable networks.

→ It follows a publish-subscribe model, making it ideal for IOT applications, real-time messaging & remote monitoring systems.

Key features of MQTT:

1. Light-weight & efficient: uses minimal bandwidth making it ideal for constrained devices.

Persistent sessions:
Stores messages for offline clients (depends on QoS)

Will Messages: ~~Notification when~~ Notifies when a client unexpectedly disconnects.

QoS (Quality of Service) levels: Provides different levels of message delivery assurance.

Publish-Subscribe Model: Devices publish messages to a broker & other devices subscribe to receive them.

Common uses
- IoT (smart home, industrial automation)
- Remote Monitoring (weather stations, sensors)
- Messaging applications (Real-time chat)
- vehicle telematic.

* ZigBee:
It is a wireless communication protocol designed for low-power, low-data-rate, and short-range applications.

→ It is based on the IEEE 802.15.4 standard and is primarily used for IoT devices, smart home automation, industrial control & sensor netw

Key features of ZigBee:

Low Power consumption: Devices can ~~communicate each other~~ operate for years on small batteries.

Mesh Networking: Devices can ~~create~~ communicate with each other & extend the network range.

Short range: Typically up to 100 meters indoor

Low data rate: Speed up to 250 Kbps making it suitable for simple sensor data and control signals.

Secure communication: uses AES-128 encryption for ~~security~~. Secure application.

Common applications:

- Home automation: Smart lights, thermostats, Security Systems.
- Industrial Automation: Sensor networks, smart meters.
- Health care: Medical monitoring devices.
- Smart cities: Street lighting, environmental sensors.

→ ZigBee is commonly used in products from companies like Philips Hue, Samsung Smart thing amazon echo devices.

→ It is an alternative to other wireless protocols like Wi-Fi, Bluetooth & Z-wave.

* Bluetooth

It is a short-range wireless communication technology used for exchanging data between device over short distance.

→ It operates in the 2.4 GHz ISM (industrial, scientific, and medical) band and follows the IEEE 802.15.1 standard.

→ Bluetooth is commonly used in consumer electronics, including smart phones, headphones, speakers & smart home devices.

* Key Features of Bluetooth:

- Short range: Typically 10 meters (33 feet) for most devices, but can extend up to 100 meters (328 feet) with bluetooth class 1 devices.
- Low power consumption: Bluetooth low energy (BLE) is optimized for battery powered IOT devices.
- Data transfer rates: Varies based on the bluetooth version:
  - Bluetooth 4.0 – 4.2: Up to 1 Mbps (BLE)
  - Bluetooth 5.0 – 5.3: Up to 2 Mbps (BLE) with extended range.
  - Bluetooth classic (BR/EDR): Up to 3 Mbps.
- Security: Uses AES-128 encryption and Pairing methods like Pin codes, Passkeys, secure connections.
- Multiple device connectivity: Supports one-to-one or one-to-many connections (e.g., Bluetooth speakers supporting multiple phone)

Application:

1. Wireless Audio: Headphones, speakers, earbuds
2. Wearables: Smartwatches, fitness trackers
3. IOT & Smart home: Smart locks, sensors, automation systems.
4. Automative: Hands-free calling, wireless infotainment.
5. Medical devices: Heart rate monitors glucose meters.

CoAP

CoAP is (Constrained application protocol)
→ It is a lightweight web transfer protocol designed for use in constrained environments, such as IoT devices.

Key features of CoAP

1. Light weight & Efficient: Uses UDP instead of TCP, reducing overload and improving performance in constrained networks.

2. Security support: can use DTLS (Datagram transport Layer security) for encryption and authentication.

3. Support for multicast - Unlike HTTP, CoAP supports multicast, making it useful for IoT application.

4. Low power & Low Bandwidth - Optimized for devices with limited processing power and energy resources.

5. Asynchronous communication: Uses message types (confirmable, non-confirmable, acknowledgment, reset) to handle communication efficiently

6. Built-in reliability mechanisms:
Uses retransmissions and acknowledgments for reliable communication.

Uses

CoAP is widely used in IOT applications including smart homes, industrial automations, & sensor networks.

* Smart homes:
→ Used in smart lightning.

* IOT & Smart Devices: Used in home automation, smart lighting & industrial IOT for device communication.

* Smart cities: Used for applications like smart parking, air quality Monitoring & streetlight control.

* Agriculture: Used in smart irrigation system and environmental monitoring.

* Healthcare & Wearables:
Used in remote health monitoring devices & smart medical equipment.

* Security & Surveillance: Enables communication bet^n security sensors, cameras & control systems.

* UDP: It stands for User Datagram Protocol, is a core protocol of the internet Protocol suite used for transmitting data across a network.
→ It is known for its simplicity & low overhead, which makes it suitable for applications where speed is more critical than reliability.

Key characteristics of UDP:

Connectionless: UDP doesn't establish a connection before sending data, meaning it sends packets (datagrams) independently without ensuring that they arrive at the destination.

- Low overhead: With minimal protocol mechanisms compared to TCP, UDP is faster and uses fewer resources, making it ideal for real-time applications.
- Unreliable: There is no guarantee of delivery, ordering, or error correction.
→ If a packet is lost or arrives out of sequence, UDP doesn't automatically retransmit it.

Uses

Commonly used in scenarios such as online gaming, video streaming, VoIP (Voice over internet protocol), DNS queries etc.

* **TCP**: (Transmission control protocol)

TCP stands for transmission control protocol. It is a core protocol in the internet protocol suite, primarily responsible for providing reliable, ordered, and error-checked data transmission bet^n application over a network.

Key characteristics of TCP:

connection-oriented:

TCP establishes a connection through a three-way handshake before any data is exchanged, ensuring that both sender & receiver are synchronized.

Reliable Data Transfer:

It guarantees that the data packets are delivered in sequence & without error.
→ If packets are lost or corrupted, TCP retransmits them.

- Error Detection: TCP includes checksums to verify the integrity of data, ensuring errors during transmission are caught & corrected.

- Ordered Delivery:
Data is received in the same order as sent; which is critical for applications, where the sequence matters such as web pages or files transfers.

Applications

TCP is widely used in applications where data reliability is paramount, including:

- Web browsing (HTTP/HTTPS)
- Email (SMTP, IMAP, POP3)
- File transfers (FTP)
- Secure communications (TLS/SSL)

PROTOCOLS: (set of rules)

802.3 – Ethernet: IEEE802.3 is collection of wired ethernet standards for the link layer.
Eg. 802.3 uses co-axial cable; 802 is uses copper twisted pair connection.
802.3j uses fiber optic connection; 802.3 ae uses ethernet over fiber.

→ 802.11 – Wifi: IEEE 802.11 is a collection of wireless LAN (WLAN) communication standards including extensive description of link layer. Eg: 802.11 a operates in 5GHz band, 802.11b & 802.11g operates in 2.4 GHZ band, 802.11 n operates in 2.4/5 GHZ band, 802.11 ac operates in 5GHz band, 802.11 ad operates in 60 GHZ band.

→ 802.16 – WiMax: IEEE802.16 is a collection of wireless broadband standards including exclusive description of link layer. Wi-max Provide data rates from 1.5 mb/s to 1 Gb/s

→ 802.154 – LR – WPAN: IEEE 802.15.4 is a collection

of standards for low rate wireless personal area network (LR-WPAN).

→ Basis for high level communication protocols such as ZigBee. Provides data rate from 40Kb/s to 250 Kb/s.

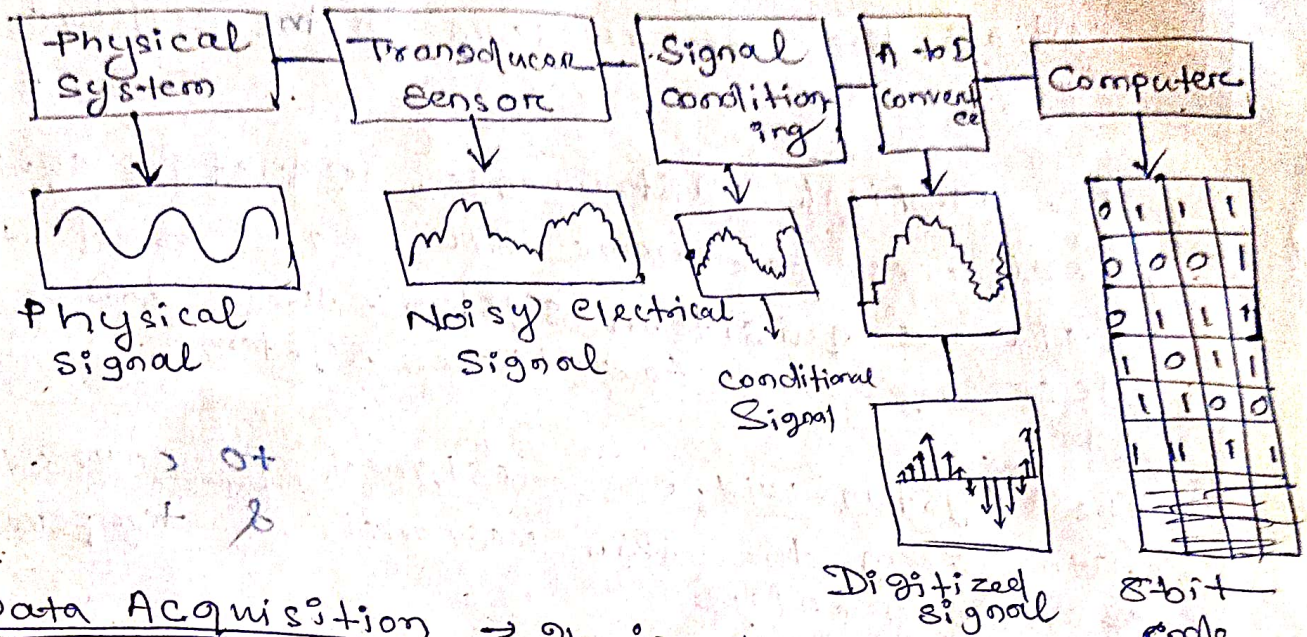
→ 2G/3G/4G - mobile communication: Data rates from 9.6 Kbps (2G) to UP. to 100 Mb/s

Unit - 3

IoT Application Development

DAS

Data Acquisition System & Integration



Data Acquisition → It is the process of sampling signals that measure real world physical condition and converting the resulting samples into digital numeric values that can be manipulated by a computer.

→ Data acquisition systems, abbreviated by the initialisms DAS, DAQ, or DAU, typically convert analog waveforms into digital values for processing

→ The components of data acquisition system include :

- Sensors, to convert physical parameters to electrical signal.
- Signal conditioning circuitry, to convert sensor signal into a form, that can be converted to digital values.
- Analog-to-digital converters, to convert conditioned sensor signals to digital values

→ Data acquisition applications are usually controlled by software programs developed using various general purpose programming languages such as assembly, BASIC, C, C++, C#, fortran, Java, LabVIEW etc.

tomorrow 2029 2022

DAS in IOT: (Device data storage)

1. The data acquisition system is simply defined as the system that either monitors or controls the parameters in the outside world.

2. For medical instruments, industrial equipments appliances for home etc. are used. Using data acquisition system, these has a necessary need for these systems.

3. The system will be designed to collect data from the skin response & temperature of human body.

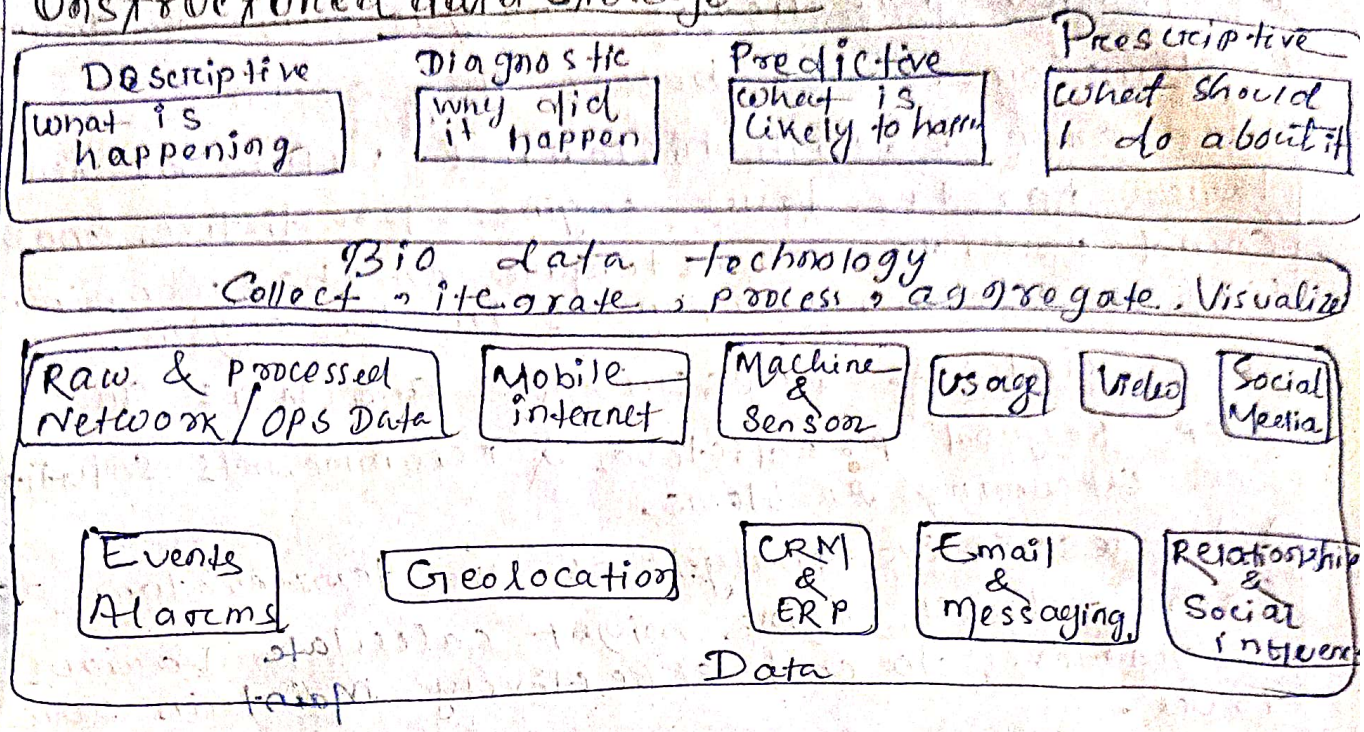
4. It will be useful for data acquisition & transfer from short distances to longer.

5. The system will be consisted of Raspberry Pi which is one of the advanced processor & has advantages like low price & small size.

(Dt - 28/3/25) The difference between authentication & authorization

Authentication	Authorization
(i) The process of confirming the truth of an attribute of a single piece of data plan true an entity	(i) Process of specifying excuss rights/previlages to resources related to information security.
(ii) Checks a person's details to identify him.	(ii) Checks a users right to excess resources.
(iii) Varify users credentials	(iii) Varify users a permiss
(iv) Occurs before authorization	(iv) Occurs after authori on pictures.
(v) Exp- A student can authenticate himself before excessing the learning management system of a University.	(v) Exp- It excess lecture write and other learning material of the courses based on the permissions given to him.

Unstructured data storage



Descriptive: Descriptive data analysis tells you what happening, either now or in past.

→ For example, a thermometer in a truck engine reports temperature values every second. From a descriptive analysis perspective, you can pull this data at any moment to gain insight into the current operating condition of the truck engine.

→ If the temperature value is too high, then there may be a cooling problem or the engine may be experiencing too much load.

Diagnostic: When you are interested in the "why" diagnostic data analysis can provide the answer.

→ Continuing with the example of the temperature sensor in the truck engine, you might wonder why the truck engine ~~has~~ failed.

→ Diagnostic analysis might show that the temperature of the engine was too high, and the engine overheated.

→ Applying diagnostic analysis across the data generated by a wide range of smart objects can provide a clear picture of why a problem or an event occurred.

Predictive: predictive analysis aims to b
problems or issues before they occur.
→ for example, with historical values of fe
tures for the truck engine, predictive an
could provide an estimate on the remain
life of certain components in the engine.

Prescriptive: prescriptive analysis goe
step beyond predictive & recommends solut
for upcoming problems.
→ A prescriptive analysis of the temperature d
from a truck engine might calculate Variou
alternatives to cost-effectively Maintain our
truck.
→ These calculations could range from the co
necessary for more frequent oil changes and
cooling maintenance to installing new cooli
equipment on the engine or upgrading t
a lease on a model with a more powe
engine.

~~Abstraction:~~

Chapter-4
Smart Technology

* **UNDERSTANDING NETWORK CONNECTIONS IN IOT**

IOT connectivity:

as a term defining connection betn all the points in the IOT ecosystem. such as sensors gateways, routers, applications, platforms & other systems.
→ It usually refers to different types of networ solutions based on their power consumption, rang and bandwidth consumption.

Cellular:

cellular networks use the same mobile netwo

a lease on a model with a more pow
engine.

~~Authentication:~~

Chapter-4
Smart Technology

UNDERSTANDING NETWORK CONNECTIONS IN IOT

IOT Connectivity:

as a term defining connection betⁿ all the points in the IOT ecosystem. such as sensors gateways, routers, applications, platforms & other systems.

→ It usually refers to different types of netwo solutions based on their power consumption, ra and bandwidth consumption.

Cellular:

Cellular networks use the same mobile netw as smartphones to allow IOT devices to commun te.

→ Because these networks were originally designed for power-hungry devices like smartphones, they weren't always considered the best bit for IoT devices.

2. **Local and personal area network (LAN/PAN)**

Networks that cover fairly short distances are called personal area network (PAN) & local area network (LAN).

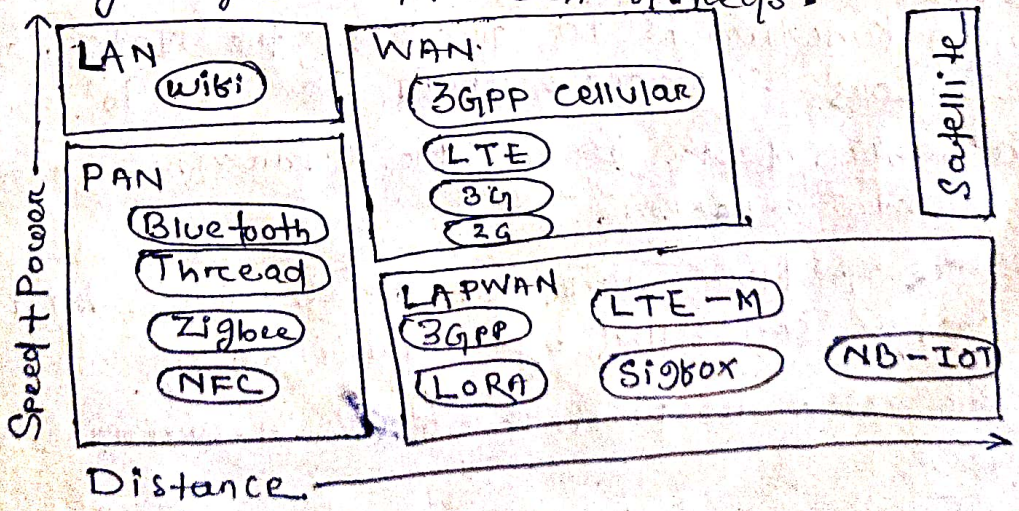
3. **Low Power Wide area networks (LPWAN)**

→ IoT devices are run on LPWANs send small packets of information infrequently and over long distances.
→ This type of wireless network was developed is response to the early challenges of cellular connectivity.

4. **Mesh Networks**

Mesh networks are best described by their connectivity configuration - how the components communicate with each other.
→ In mesh networks, all the sensor nodes cooperate to distribute data amongst each other to reach gate

Zigbee: It is one example of an IoT wireless network technology. Mesh networks are very short range and may require extra sensors throughout a building or the use of repeaters to get coverage your application needs.

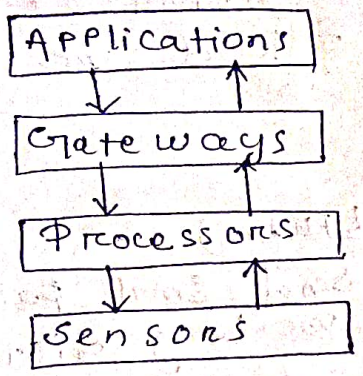


5 Mar 2023 2024

* Building Blocks OF IOT

Building blocks OF IOT four things basic building blocks of the IOT system - sensor, processors, gateways, applications.

→ Each of these nodes has to have its own characteristics in order to form an useful IOT system.



Sensors: These form the front end of the IOT devices. These are so-called things of the system.

→ Their main purpose is to collect data from its surrounding (sensors) or give out data to its surrounding (actuators)

→ Can be easily identifiable over a large network

→ These have to be active in nature, which means that they should be able collect the real time data.

Processors: processors are the brain of the IOT system.

→ Their main function is to process the data captured by the sensors & process them so as to extract the valuable data from the enormous amount of raw data collected.

→ Processors mostly work on real-time basis & can be easily controlled by applications.

→ These are also responsible for securing the data

Gateways:

They are responsible for routing the processed data & send it to proper locations for its (data) proper utilization)

→ In other words we can say that gateways help

in to and for communication of the data.
→ It provides network connectivity to the data.
→ LAN, WAN, PAN are examples of network gateways.

Application: Are essential for proper utilization of all the data collected.
→ Applications are controlled by users & are delivery point of particular services.
→ ~~Application~~ Examples of applications are home automation apps, security systems, industrial control hub etc.

* Understand IP address in IOT:

→ An IP address is a unique address that identifies a device on the internet or a local network.
→ IP stands for internet protocol, which is set of rules governing the format of data sent via the internet or local network.
→ In essence, IP address are the identifier that allows information to be sent between devices on a network.
→ The internet needs a way to differentiate between different computers, routers & websites.

How do IP address work:

IP address work's the same way as any other language, by communicating using set guidelines to pass information.
→ All devices find, send & exchange information with other connected devices using this protocol.
→ By speaking the same language any computer in any location can talk to one another.

Chapter - 5
Smart TV

What is smart TV & its use ?

A smart TV is also known as a connected TV (or
→ It is a traditional television set with integrated
internet & interactive web 2.0 features.
→ The TV sets on set-top boxes that offer
connectivity to the internet, via wibi wireless
technology.
→ That enable viewing of various streaming video
services, such as Netflix & hulu, also users
to stream music, browse the internet & view photo
→ The marketing term used to convey the ability
to view internet based program.
→ The concept of Smart TV isn't particularly new.
Smart TVs have been around since 2007 or so
under many different labels, including "connected" TV
"IPTV", and "internet" TV.

What's inside the Smart TV

2022 (5)

→ Wibi radio for home n/w.
→ CPU manages all the devices operations &
commands.
→ OS that serve as the interface bet^n the CPU
& software-based application.
→ GUI for displaying manuals & other options.
→ Software based apps that enable connections to
various web-based services.
Ex: It have built-in apps for netflix,
Hulu and pandora
→ Some Smart TVs include a built in camera &
microphone.
→ All smart TVs are controlled by some sort of
remote control.

Need to use a smart TV :

An internet connection : A home network that interfaces with your internet connection. This can be wireless (Wi-Fi) or wired (Ethernet) network.

→ Electricity Duh.

If you have a smart TV is a TV set-top box, you'll also need an HDMI cable to connet the device to your traditional television set.

→ A home network that interfaces with your internet connections.

→ It can be a wi-fi, or ethernet.

What Smart TV does

→ Connect to the internet via a local network. Most smart TVs are connect via wi-fi, although some can connect via ethernet.

→ Play video content from web-based streaming video services such as netflix, hotstar & amazon instant video.

→ Play music from web-based streaming audio services, such as pandora and spotify.

→ Play digital n/w media stored on other device connected to your home n/w.

→ Access selected websites and web-based services such as facebook, twitter & accu weather.

→ Play digital media stored on other devices connected to your home network.

→ Some smart TVs ~~your~~ other full-fledged web browsers, although it's more common to find disc etc apps for specific sites & services.

202
Smart

Smart TV operating systems :

There are a number of smart TV OS's in use to day, many properties to a specific company on devices.

→ Android TV
→ Fire OS
→ Firefox OS
→ iOS apple's mobile OS
→ Roku OS
→ Tizen, a linux-based OS.
→ web OS, a Linux derivative

All smart TVs & smart TV devices are like mini computers, in that they include a built-in OS and the appropriate software or middleware to run the necessary apps.

Smart TV set-top devices :

There are lots of these devices, with the most popular being the Roku models, apple TV WDTV live & amazon fire TV.

→ All of these devices are small enough to hold in your hand & sell for $100 or less
→ Consider the Roku 2 (between Roku 1 and Roku 3 naturally) & sells for $69.99.
→ It connects to you home n/w via wi-fi & to your TV via HDMI, and includes its own remote control.
→ Like all Roku models, the Roku 2 comes with a number of popular apps preinstalled including Netflix, HuluPlus, amazon instant video, youtube vevo, pandora, Spotify & tune in radio.
→ Another connection devices as a USB (universal Serial bus) dongle, such as google's chrome cast, the Roku streaming stick & amazon's fire TV stick.

These devices plug into any open HDMI connection on your TV & provide web based streaming.

Integrating smart TVs into IOT :

→ The current generation of smart TVs has very little to connect it to the internet of things.
→ It needs to do more. The TV manufacturers are likely to do is make it easier to control the smart TVs themselves.
→ Let's face it, picking through the choices on Hulu or searching for your favourite movie on netflix isn't easily accomplished with a traditional four-arrow remote control.
→ A better solution might be a touch screen tablet like controller a remote app, on ~~the~~ a smart phone or ipad, or even siri-like voice control.
→ The Smart TV might connect to your facebook or twitter account to discover what shows your friends are watching.
→ Future smart TV may also, use their internet connectivity to overly related information on the main viewing screen.
→ In addition the smart TVs include more interactive chat capabilities. When you're watching a movie or show, you'll be able to tweet or post on facebook about what you're watching, & participate in group chats about the show.
→ The video chat conducted in a pop-up window & enable by your set's built in camera.

IOT case studies

Smart 2022-2024

a. smart home

A smart home in IOT refers to a home equipped with devices that can be controlled remotely or automatically through an internet connection.

→ These devices often communicate with each other, collect data, adapt behaviour based on user preference or environmental condition.

Key components of a smart home:

1. Sensor: Detect changes in the environment @x: motion, temperature, humidity, light.
2. Actuator: perform actions like turning on lights or adjusting thermostat.
3. Cloud services: store & process data, enable remote access & automation.
4. Voice control: Integration with AI assistants li Alexa, google assistant or Siri.
5. Energy Efficiency: optimize usage (e.g. smart thermostats reduce energy consumption)
6. Remote control: control device from anywhere usi an app.
7. Automation: Devices perform actions automatic ny (e.g. lights turn on when someone enters a room)

Common Smart home IOT Devices:

- Smart Lights: Control brightness, color & schedu
- Smart Plugs: Turn devices on/off remotely.
- Smart appliances: fridges, ovens, Washers with connectivity features.
- smart locks: Keyless entry with access control.
- Smart cameras/doorbells: Monitor your home in real time.

10/1/2022

Industrial automation:

Industrial automation involves the use of control systems, such as computers, PLCs (Programmable logic controllers), and robots, to handle different industrial processes.

Goals

- Increase productivity & efficiency.
- Improve Safety
- Reduce operational costs
- Ensure quality & consistency.

Application

1. Predictive maintenance: Sensor monitor equipment health & predict failures before they occure - reducing downtime.

2. Remote monitoring & control

Factory systems can be monitored and adjuste remotely through dashboards.

3 - Smart manufacturing

Real time data from various stages of production helps optimize workflow & decision-making.

Benefits:

- Real time visibility
- Enhanced data analytics
- Faster decision-making
- cost savings.
- Improved safety & compliance

Smart Transportation:

Smart transportation refers to the integration of advanced technologies into transportation systems to improve safety, efficiency, sustainability & convenience.

→ It typically involves the use of IoT, AI, big data & communication technology.

Components of Smart transportation:

1. Intelligent traffic management systems: Use sensors, cameras & AI to monitor & manage traffic flow in real-time, reduce congestion & improve emergency response.

2. Data analytics & AI: Analyzes travel patterns to optimize infrastructure, route planning & emergency services.

3. Environmental monitoring: Track vehicle emissions air quality to support greener urban planning.

4. Smart Public Transit: Real time tracking of buses/trains, mobile apps for schedules and payments & demand based transit option.

5. Electronic toll collection & smart parking: Use sensors & mobile apps to automat toll payments & help users find available parking.