UNIT-I:— Syllabus

The Internet of things: An overview of Internet of things, Internet of things Technology, behind Io Ts Sources of the Io Ts, M2M Communication, Examples of IoTs, Design principles for Connected Devices Internet connectivity principles, Internet connectivity, Application layer protocols: HTTP, HTTPS, FTP, Telnet.

1) An overview of Internet of Things(IOT):—

Defination:— The internet of things describes the network of physical objects — "things" — that are embedded with sensors, software and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

2nd def:—
→ IOT is a technology transition in which the devices will allow us to sense and control the physical world by making objects smarter and connecting them through an intelligent network.

Evolutionary phases:-

First phase: Connectivity (Digitize Access)

- * Began in the mid 1990's
- * This phase connected people to email, web Services and Search, so this information is easily accessed.

Second phase: Network Economy (Digitize Business)

- * caused one of the major disruptions of the past 100 years.
- * This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business

Third phase: Immersive Experiences (Digitize Interactions)

- * This phase extended the internet experience to encompass widespread video and social media while always being connected through mobility.
- * More and more applications are moved to cloud.
- * person to person interactions have become digitized

Fourth phase : Internet of things (Digitize the world)

* we are beginning of the IOT phase.

* 99 % of "things" are still unconnected.

* This phase is adding connectivity to objects and machines to the world around us to enable new services and experiences.

* It is connecting the unconnected.

Advantages:-

i, Efficient resource utilization:-

if we know the functionality and the way that how each device work, we definitely increase the efficient resource utilization as well as monitor natural resources.

ii, Minimize human effort:-

As devices interact & communicate with each other and do lot of task for us. It reduces the human effort.

iii, Save Time:-

As it reduces the human effort then it definitely saves out time.

iv, Improving Quality of life:-

As IOT (technology) increased

comfort, convenience & better management, hence it improves the quality of life.

Disadvantages:-

privacy:- Even without the active participation on the user, the IOT system provides substantial personal data in maximum detail.

Complexity:- The designing, developing, and maintaining and enabling the large technology to IOT system is quite complicated.

Security:- The system offers little control despite any security measures, and it can be lead the various kinds of network attacks.

Characterstics:-(or) Features:-

i) connectivity:- In IOT, anything, anywhere, anytime should be connected to the infrastructure, without connection nothing makes sense.

ii) Intelligence:- Extraction of knowledge from the generated data is important, sensor generate data and this data should be interpreted properly.

iii, **Dynamic & self-Adapting:-**

IOT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, users context, or sensed environment.

iv, **self-configuring:-**

IOT devices may have self-configuring capability, allowing a large number of devices to work together to provide certain functionality like setup networking, fetch latest software upgrades.

v) **unique Identity:-**

Each IOT device has a unique identity and a unique identifier.

vi, **Heterogenity:-**

IoT architecture should support direct network connectivity between heterogeneous networks

vii, **Interoperable Communication protocols:-**

~~Able~~ Ability to communicate with other devices and also with the infrastructure.

Applications:—

(1) wearables:—

This technology is the hallmark of IoT applications and one of the earliest industries to deploy IoT. we have fit bits, heart rate monitors and smart watches these days.

(2) Smart home applications:—

→ Smart homes control home appliances including lights, alarms and water flow from taps, while promoting home security and safety through elaborate, smart security systems.

→ Smart homes allows you to manage all your home devices from one place.

(3) health care:—

→ IoT applications can transform reactive medical-based systems into active wellness-based systems.

→ Resources that are used in current medical research lack important real world information.

(4) Smart city:—

→ Smart city uses technology to provide services.

→ The Smart city includes improving, transportation, social services, promoting stability and giving voice to their citizens.

⑤ Agriculture :—

→ one way to feed everyone is better agricultural practices which can be enhanced using IoT.

→ Machine learning and IoT to create custom recommendations for each farm that will optimize the planning procedure, irrigation, fertilizer amount etc...

⑥ Industrial Automation:—

→ It is one of the areas where the Quality of products is an essential factor for a more significant investment return.

→ Anyone can reengineer products and their packaging to provide superior performance in cost and customer experience with IoT applications.

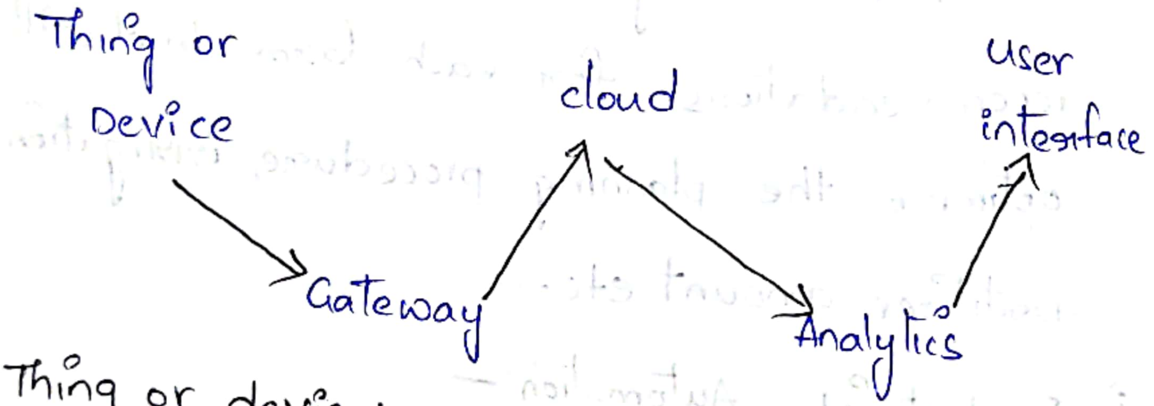
⑦ hacked car:-

The technology offers the user some benefits such as in-car infotainment, fuel-efficiency advanced navigation.

⑧ Smart Supply chain:-

customers automate the delivery and shipping with a smart supply chain.

Components of IOT:-



① Thing or device:-

These are fitted ~~technology~~ sensors and actuators. sensors collect data from the environment and give to gateway where as actuators performs the action.

② gateway:-

The sensors give data to gateway and

here some kind of pre-processing of data is even done. It also acts as a level of security for the network and for the transmitted data.

③ cloud:-

The data after being collected is uploaded to cloud.

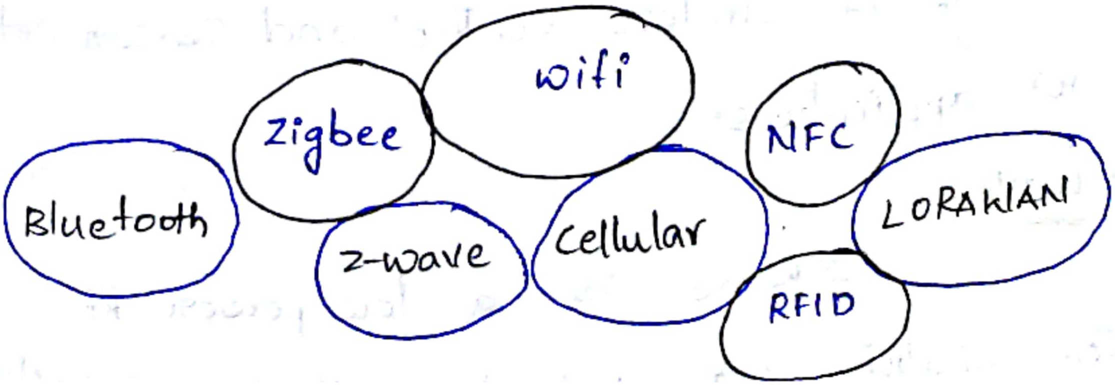
④ Analytics:-

The data after being received in the cloud processing is done. Various algorithms are applied here for proper analysis of data.

⑤ user interface:-

user end application where user can monitor/control the data.

2) Internet of things Technology:-



NFC:-

It consists of communication protocols for electronic devices, typically a mobile device and a standard device.

RFID:-

RFID technology employs 2-way radio transmitter-receivers to identify and track tags associated with objects.

Bluetooth:-

Bluetooth, which has become very important in computing and many consumer product markets. The new bluetooth Low-Energy (or) Bluetooth smart, as it is now branded-is a significant protocol for IoT applications.

Zigbee:-

It has some significant advantages in complex systems offering low-power operation, high security and is well positioned to take advantage of wireless control and sensor networks in IoT applications.

z-wave:-

z-wave is a low power RF Communication IOT technology that primarily design for home automation for products such as lamp controllers and sensors among many other devices.

wifi:-

wifi connectivity is one of the most popular IOT communication protocol. There is a wide existing infrastructure as well as offering fast data transfer and the ability to handle high Quantaties of data.

cellular:-

Any IOT application that requires operation over longer distances can take advantage of GSM/3G/4G Cellular Communication capabilities.

LORaWAN:-

The LORaWAN design to provide low-cost mobile secure communication in IOT, smart city and industrial applications.

3) Behind to Ts Sources of the IO Ts:-

① **Role of RFID and IOT applications:-**

→ RFID enables tracking and inventory control, identification in supply chainsystem, access to buildings and road tolls.

→ RFID networks have new applications in factory design, 3pl-management, brand protection, and anti-counterferting in new business processes for payment, leasing, insurance and Quality management.

② Wireless Sensor Networks:—

→ Sensors can be networked using wireless technology and can co-operatively monitor physical or environmental conditions.

→ Sensors acquire data from remote locations, which may not be easily accessible. Each wireless sensor also has communication abilities for which it uses a radio-frequency transceiver.

→ WSN node is autonomous.

③ Actuators:—

Devices which is a contrast to sensors. It transforms electric signals into physical movements. Both sensors and actuators are transducers that convert one form of energy to another.

4) M2M Communication:—

→ Machine-to-Machine refers to the Communication (or) exchange of data between two or more machines without human interfacing or interaction.

→ Communication in M2M may be wired (or) wireless system.

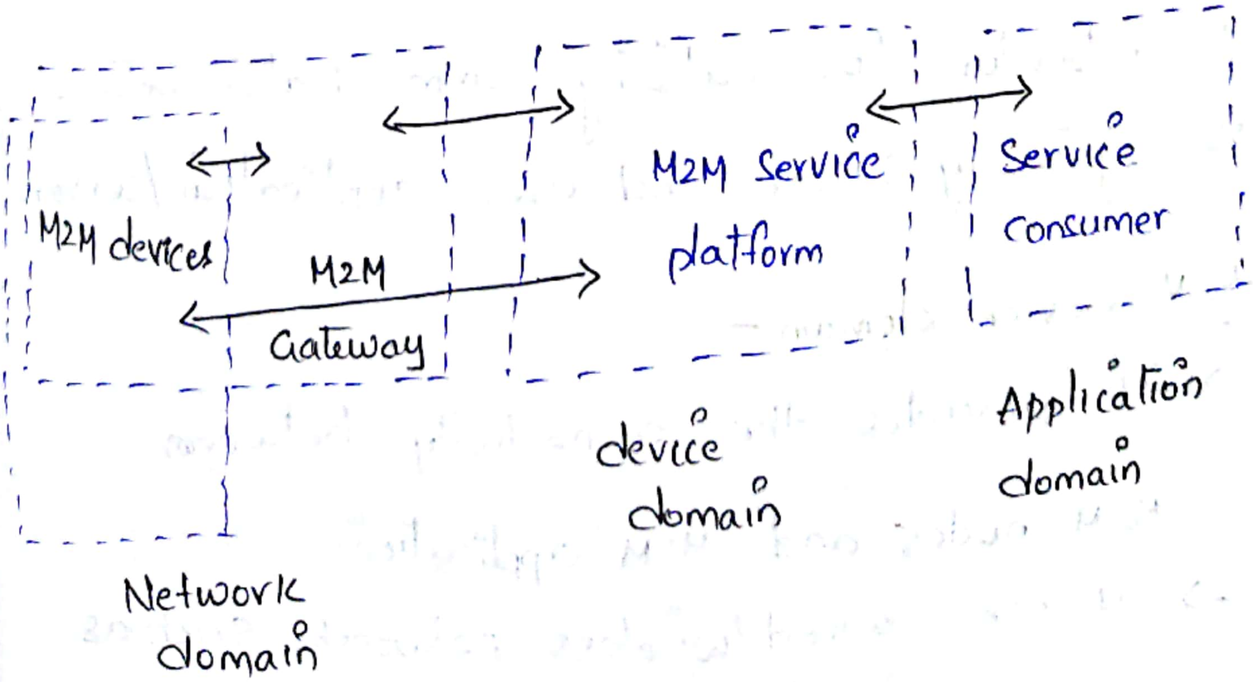
→ M2M uses a device such as Sensor, RIFD, meter etc., to capture an events like temp, inventory level etc.. that translates the captured event into meaningful information.

Architecture:—

i, M2M application domain

ii, M2M network domain

iii, M2M device domain



M2M Network domain:-

→ M2M network area consists of machines (or) M2M nodes which communicate with each other. The M2M nodes embedded with hardware modules such as Sensors, actuators and Communication,

→ M2M uses communication protocol such as zigbee, Bluetooth, powerline communication etc...;

→ M2M nodes communicate with in one network it can't Communicate with external network node.

M2M Gateway:-

→ The gateway module provides control and localization services for data collection.

→ M2M communication network serves as infrastructure for realizing communication between M2M gateway & M2M end user application/server.

M2M device domain:-

→ It provides the connectivity betweem M2M nodes and M2M applications.

→ It uses wired/wireless network such as LAN, LTE, satellite....

M2M application domain:-

→ It contains the middleware layer where data goes through various app services and is used by the specific business processing engines

→ Applications may either target at end users, such as user of a specific M2M solution or at other application providers to offer more refined building blocks by which they can build more sophisticated M2M solutions & services.

*difference between M2M and IOT:-

M2M	IOT
① It is about direct machine to machine communication	① It is about sensor automation and internet platform.
② It support point-to-point communication	② It support cloud based communication.
③ It is mostly based on hardware.	③ It is mostly based on both hardware and software.
④ Its for only B2B business type	④ Its for B2B and B2C business type.

⑤ Device not necessary relay on internet	⑤ Device necessary relay on internet.
⑥ Machine normally communicate with single machine at a time.	⑥ Many user can access at a time over internet.
⑦ It is less scalable	⑦ It is more scalable
⑧ It doesnot support open API's	⑧ It supports open APIs
⑨ It uses either proprietary or non ip based protocols.	⑨ It uses ip based protocols.
⑩ extensive background of historical applications.	⑩ state-of-the-art approach with roots in M2M.

Example: Vending Machine: (M2M)

-> one can buy soft drinks, flowers, etc., from vending machine in self service manner.

-> once the vending machine detects the item in out of stock, it sends message to ~~order~~ order management server through 3G/4G communication link which further send information to vendor.

-> The vendor re-stocks the vending machine

-> vending machine stores daily sales data in internal database and sends information to vendor.

-> Vendor will know which product has been sold and the total daily revenue..

5) Examples of IOT's:-

-> Home automation :-

Home automation is automation of house, house work, household activities. we can control remotely using our mobile app/webapp. home automation is simple and affordable.

-> Intelligent Transportation System:-

It is a combination of advance information and telecommunications network for user road & vehicles.

-> Smart healthcare:-

It include smart hospital, patient Monitoring, pre-checkup, Real time health monitoring using smart wearable.

→ Smart city:-

To provide for the aspirations and needs of the citizens, urban planners, ideally aim at developing the entire urban eco-system, which is represented by the four pillars of comprehensive development, institutional, physical, social and economic infrastructure.

→ Smart home:-

i) Automatic control over fan, lights, AC, TV, etc---

ii) surveillance, Door lock, refrigerator, window curtain, Gardening.

→ Smart grid:-

with the smart grid, utilities can interconnect all their assets including meters and substations.

→ Activity trackers:-

These are sensor devices that can monitor and Transmit key health indicators in real-time.

Industrial Security and safety:-

IOT enabled detection systems, sensors and cameras can be placed in restricted areas to detect ~~trans~~ tres passers.

6) Design principles for connected devices:-

i, calm and Ambient technology:-

* The term calm technology- systems which don't compete for attention Yet are ready to provide utility /useful information when we decide to give them some attention.

* The term ambient technology- The most profound technologies are those that ~~appear~~ disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

* calm technology engages both the center and the periphery of our attention, and in fact moves back and forth between the two.

Eg:- live wire(Dangling string) is a Simple device: an electric motor connected to an eight-foot long piece of plastic string. The power for the motor is provided by the data transmission on the ethernet network to which is connected, so it twitches whenever a packet of information is sent across the network.

ii, Magic as Metaphor:-

→There are many examples when the main difference between a failed technology and a widly Successful one is that the successful one arrived a few years later, when people were more receptive to what was offered.

→ For a technology to be adopted, it has to make its way inside the manufactured norm~~day~~alcy field.

→ Arthur C. Clarke has claimed that "any sufficiently advanced technology is indistinguishble from magic," and given that the IOT commonly bestows semi-hidden capabilities onto everyday objects, maybe the enchanted objects of magic and fairy tale are a good metaphor to help people grasp the possibilites.

Eg:- Mobilephone.→ It was first introduced as a phone that wasn't tethered to a particular location.

iii, privacy:-

→with more Sensors and devices watching us and reporting data to the internet, the privacy of third parties who cross our Sensors paths is an important consideration.

→ Keeping Secrets:-

* security professionals Troy Hunt was able to watch the what information the app was requesting from the server and found that it was a simple unencrypted web request.

* The intial request URL had a number of parameters including the search string, but also including information such as number of results to return.

iv, web thinking for connected devices:-

→ when you are thinking of the networked aspect of IOT objects, it might help to draw an experiences and design guidelines from existing network deployments.

→ Create devices which are of the webrather than those which just exist on the web.

→ small pieces, loosely joined.

v) First-class citizens on the internet:-

→ where possible, you should use the Same protocols and conventions that the rest of the internet uses.

→ a good rule of thumb for the past 20 years or more ~~than~~ has been to expect the IP protocol to penterate everywhere.

c→ we see no reason for it not to continue into the IoT.

vi, Graceful Degradation:—

→ The endpoints have a massively disparate and diverse range of capabilities.

→ As a result, building services which can be used by all of them is a nearly impossible task.

vii, Affordances:—

* Affordances provide strong clues to the operations of things.
* Knobs are for turning.
* Balls are for throwing/bouncing.
* when affordances are taken advantage of, the user knows what to do just by looking: no picture, label, or, instructions.
* Complex things may require explanation, but simple things should not.

7) Internet connectivity and their principles.—

→ The internet connectivity of the computers, mobile devices, computer networks to the internet enables the users to access the various Internet services. There are many ways and technologies of the connection to the internet with different data signaling rates: wireless, ethernet cable, optical fiber.....

-> The term "internet connectivity refers to the way people are hooked up to the internet, and may include dial up telephone lines, always on broadband connections and wireless devices.

Types:-

① Dial-up:- uses phone lines to connect to the internet. You cannot talk on the phone and be on the internet at the same time

② DSL:- Also uses phone lines to connect to the internet but faster than dialup. Allows you to talk on the ~~read~~ phone and be on the internet at the same time.

③ Satellite:- uses satellite to provide an internet connection. used in remote areas.

④ Cellular:- uses the same channels as your phone to connect to the internet. handy

, when you are away from home and need a connection.

⑤ cable:-

one of the most common types of connections. uses the same co-axial cables that deliver your cable television.

⑥ Fiber-optic:-

The fastest type of connection. uses fiber-optic cables to transfer data which light waves as opposed to electricity.

Principles:-

① IP:-

* Data is sent from one mobile to another in a packet, with a destination address and a source address in a standardized format (protocol)

* The packets of data have to go through a no.of intermediary machines, called routers, to reach their destination.

② TCP:-

* It is built on top of the basic ip protocol. and adds sequence numbers, acknowledgements and retransmissions.

* This means that a message sent with TCP

can be aribitrarily long and give the Sender some assurance that it actually arrived at the destination port.

iii, IP protocol suite (Tcp/ip):-

* The combination of Tcp and Ip is often referred as "Tcp/Ip" to describe a whole suite/stack of protocols layered on top of each other, each layer building on the capabilities of one below.

* The low-level protocols at the link layer manage the transfer of bits of information across a network link by an ethernet cable, wifi.

iv, UDP:-

* It is also the transport for some Very important protocols which provide common, low-level functionality Such as DNS and DHCP, which relate to the discovery and resolution of devices on the network.

* In UDP, each message may or may not arrive.

v) Ip addresses:-

* Ip addresses are numbers.

* An IP addresses is a unique address for

every host computer in the world. It consists of 4 bytes or 32 bits. every machine on the internet has at least one Ip address.

* This is represented in Quad notation (or dot notation) as four 8-bit numbers, each in the range 0 to 255 eg: 131.123.2.220.

vi) DNS:-

* Although computers can easily handle 32-bit numbers, most humans to forget.

* It helps our feeble brain's navigate the internet.

* Domain names, such as following, are familiar to us from the web, or perhaps from email or other Services:

google.com, ~~bbb~~ bbc.co.uk, wiley.com.

vii) IPV6:-

* when IP* was standardllized, few Could have predicted how Quickly the 4.3 billion addresses that IPV4 allowed for would be allocated.

* The expected growth of the internet of things can only speed up this trend.

* It is hard to predict what order of

no. of Internet connected devices a household might have in the near future. Tens? Hundred?

Viii, MAC addresses:-

* every network connected device also has a MAC addresses, is the final address on a physical envelope in our analogy.

* It is used to differeniate ~~ma~~ different machines on the same physical network, so that they can exchange packets. This relates to the lowest-level "link layer" of the TCP/IP stack.

* MAC stands for medium access control. It is a 48 bit number, usually written as six groups of hexa decimal digits, separated by colons.

Eg: 01:23:45:67:89:ab.

IX) Tcp and udp ports:-

* when you send a TCP/IP message over the internet, you have to send it to the right port.

* Tcp ports are re-ferred to by numbers (0 to 65355) and eg: HTTP ports.

x) URL:-

- * It is a unique identifier for any resource on the internet.
- * can be typed into web browser.
- * can be used as hyperlink within a HTML document.
- * can be Quoted as a reference to a source.

8) Application layer protocols:

Application layer protocols define how application processes running on different end systems, pass messages to each other. An application layer is an abstract layer that handles the sharing protocol of the TCP/IP and OSI model. The purpose of application layer protocols is that users can send data, access data, and use networks.

i) HTTP:-

→ HTTP defines how you interact with www.

→ The interaction proceeds between a client and a server:

i, The client sends a request to the server

ii, The server process the request

iii, The server sends the answer back

iv, The client interprets the answer.

-> The request may be to fetch web page, to insert a record in a database

-> Depending on the request, a no. of answers are possible.

-> It transfers data in plain text, hypertext, audio, video etc...

-> It is a synchronmous protocol that works by making both percistent and non-percistent connections.

-> It includes such as GET, PUT, POST, HEAD, OPTIONS, TRACE....

ii, HTTPS:-

-> Hyperlext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and website.

-> It is encrypted in order to increase security of data transfer.

-> It is a protocol for Securing the communication between 2 systems.

-> This protocol uses the 443 port number for communicating the data.

-> It is alco called HTTP over SSL because the https communication protocols are encrypted using the SSL.

(iii) FTP:-

-> FTP stands for file Transfer protocol.

-> It is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

-> It is also used for downloading the files to computer from other Servers.

(iv) TELNET:-

-> TELNET stands for Terminal network. It is a type of protocol that enables ~~more~~ one computer to connect to local computer

-> It provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

HTTP	HTTPS
-> It works at the application layer	-> It works at the transport layer
-> port number is 80	-> portnumber: 443
-> url begins with http://	-> url begins with https://
-> less secure	-> More secure
-> It is not secure & unreliable	-> It is Secure & reliable.
-> It doesnot uses certificate.	-> It uses SSL certificate.
-> Doesnot support AMP	-> It is required for AMP
-> Data exchange on the internet.	-> confidental data exchange, including the exchange through unsafe networks.
-> They donot encrypt the text.	-> they encrypt the code so that no one access it.

HTTP	FTP
→ It is used to access websites.	→ It transfers file from one-one host to another.
→ It establishes data connection only	→ It establishes two connection one for data and one for control connection.
→ It uses port number: 80	→ It uses port number: 20 and 21
→ It doesnt require authenication	→ It requires a password
→ It is faster	→ It is slower
→ It uses one way communication system	→ It use two way communication system
→ It is a stateless protocol	→ It is not a stateless protocol and it maintain states.

IOT Types:-

① **Consumer IoT:-** primarily for everyday use.

Eg:- home appliance, light fixtures.

② **Commercial IoT:-** primarily used in the healthcare and transport industries: Eg

Eg: smart pacemakers and monitoring systems.

③ **Military things:-** primarily used for the application of IoT Technologies in the military field.

Eg:- surveillance robots and human-wearble biometrics for combat.

④ **Industrial Internet of Things:-** primarily used with industrial applications, such as in the manufacturing and energy sectors.

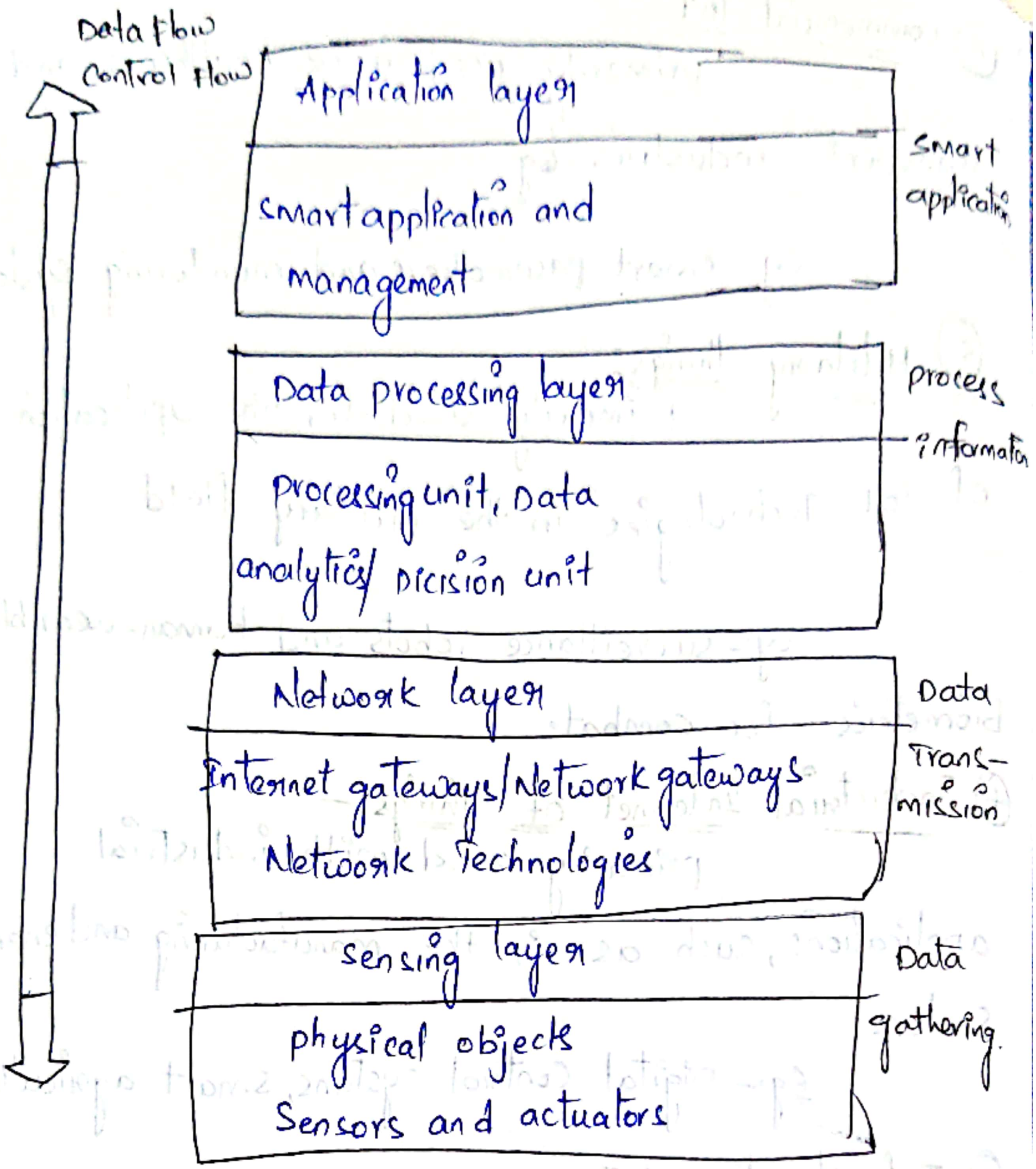
Eg:- Digital Control systems, smart agriculture.

⑤ **Infrastructure IoT:-** primarily used for Connectivity in Smart cities.

Eg:- Management Systems.

IoT Architecture:-

There are different phases in the architecture of IoT but they can vary according to the situations but generally, these are four phases:



① Sensing layer:-

Sensors, actuators, devices are present in this Sensing layer. These sensors or actuators accepts data, processes data and emits data over network.

② Network layer:-

→ Internet/Network gateways, Data acquistion system are present in this layer.

→ DAS performs data aggregation and

conversion function.

③ Data processing layer:-

This is processing unit of IOT ecosystem. Here, data is analyzed and pre-processed before sending it to data center from where data is accessed by software applications.

④ Application layer:-

Data centers or cloud management stage of data where data is managed and is used by end-user applications like agriculture, health//