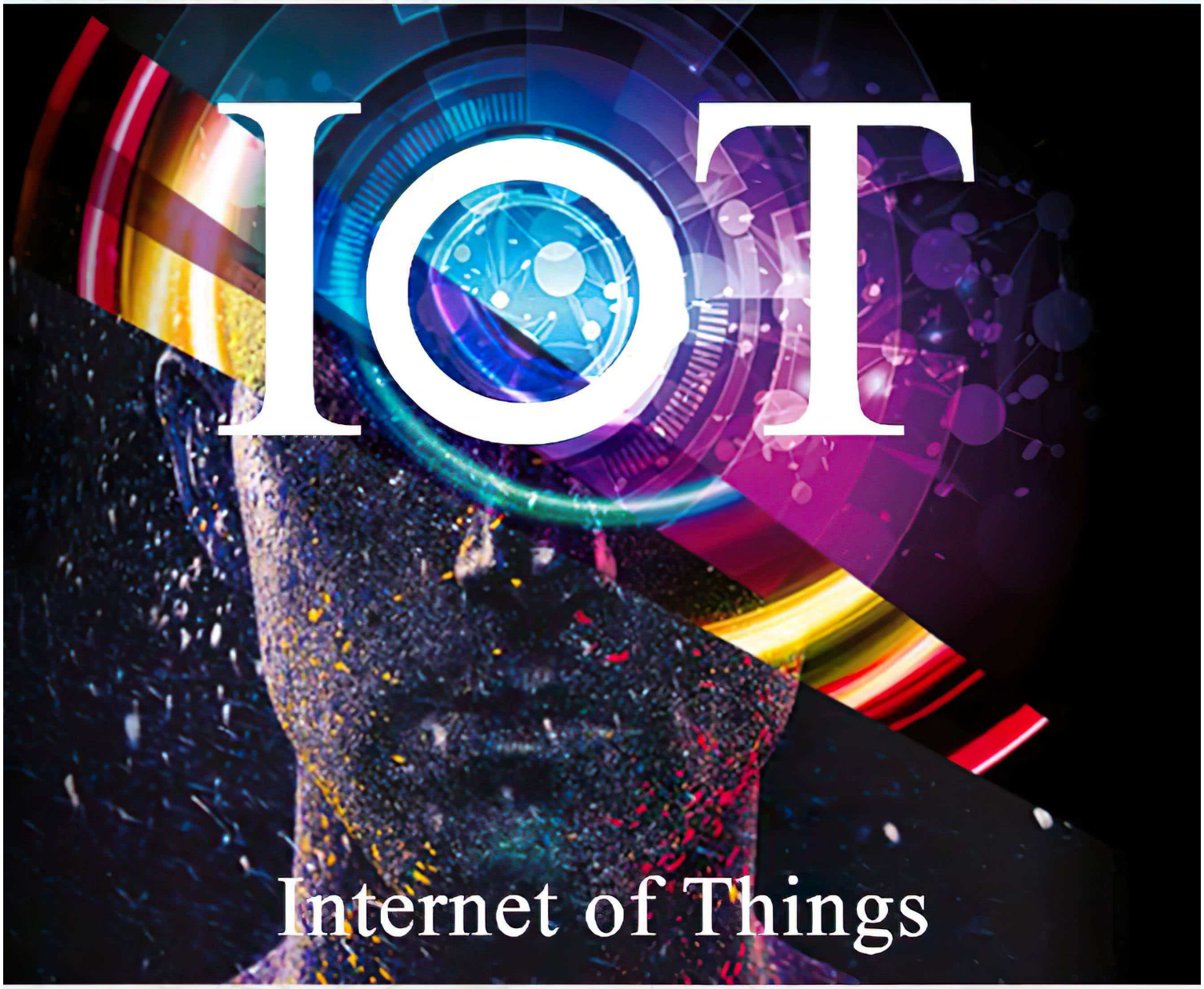
Jump2Learn
PUBLICATION

www.jump2learn.com



Internet of Things

Jump2Learn - The Online Learning Place

Mr. Vijesh Shukla | Ms. Khushbu A. Patel | Mr. Ankit R. Patel

UNIT-1

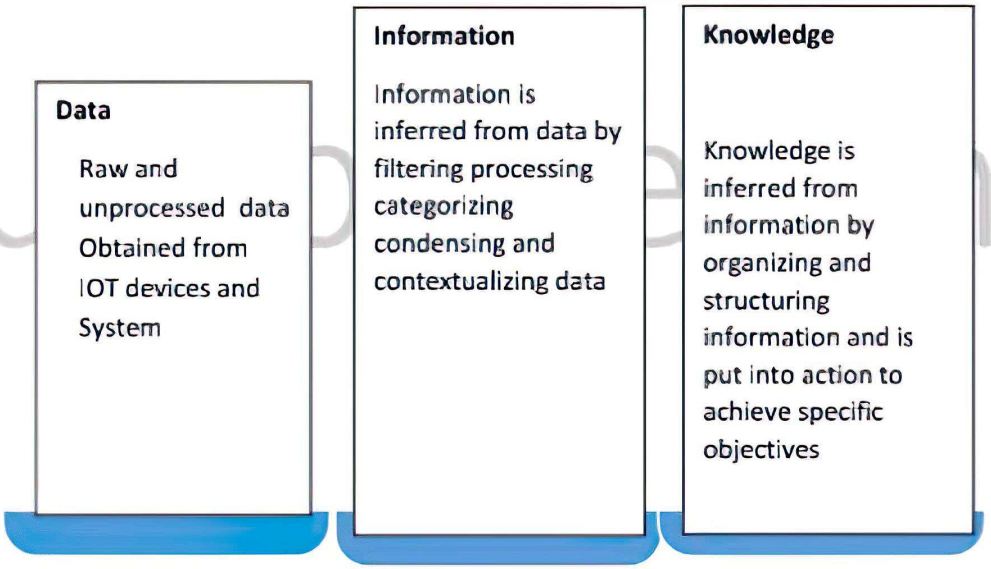
INTRODUCTION TO INTERNET OF THINGS

1.1 Definition and Characteristics.

Internet of things(IOT) comprises things that have unique identities and connected to the Internet. While many existing devices such as network of computers or 4G-enabled mobile phones, which have unique identity are also connected to the internet. The focus of IOT is in the configuration, control and networking via internet of devices that is not traditionally not associated with the Internet . Devices which are included in this are thermostats, utility meter, blue-tooth connected headset, sensor, irrigation pump, control circuit of electric car engine.

Internet of Things is new revolution in the capabilities to connect the endpoints which are connected through internet and this is being driven by advancement in sensor network, mobile devices, wireless communications, networking and cloud technologies due to decrease in cost and advancement of technology. IOT Products includes hardware and software components for IOT endpoints, sensors, hubs , control center which contains control server in IOT world.

Scope of IOT is not limited to just connecting different things like devices, appliances, machines to the internet. But IOT allows above different things to communicate and exchange data, information along with data of users when a particular application is made.



Data itself does not have any meaning until it is contextualized and processed into information. Various Application of IOT network extract and create information from lower level data by filtering and processing, categorizing, condensing the data. This information is then organized, structured into knowledge about the systems and its users.

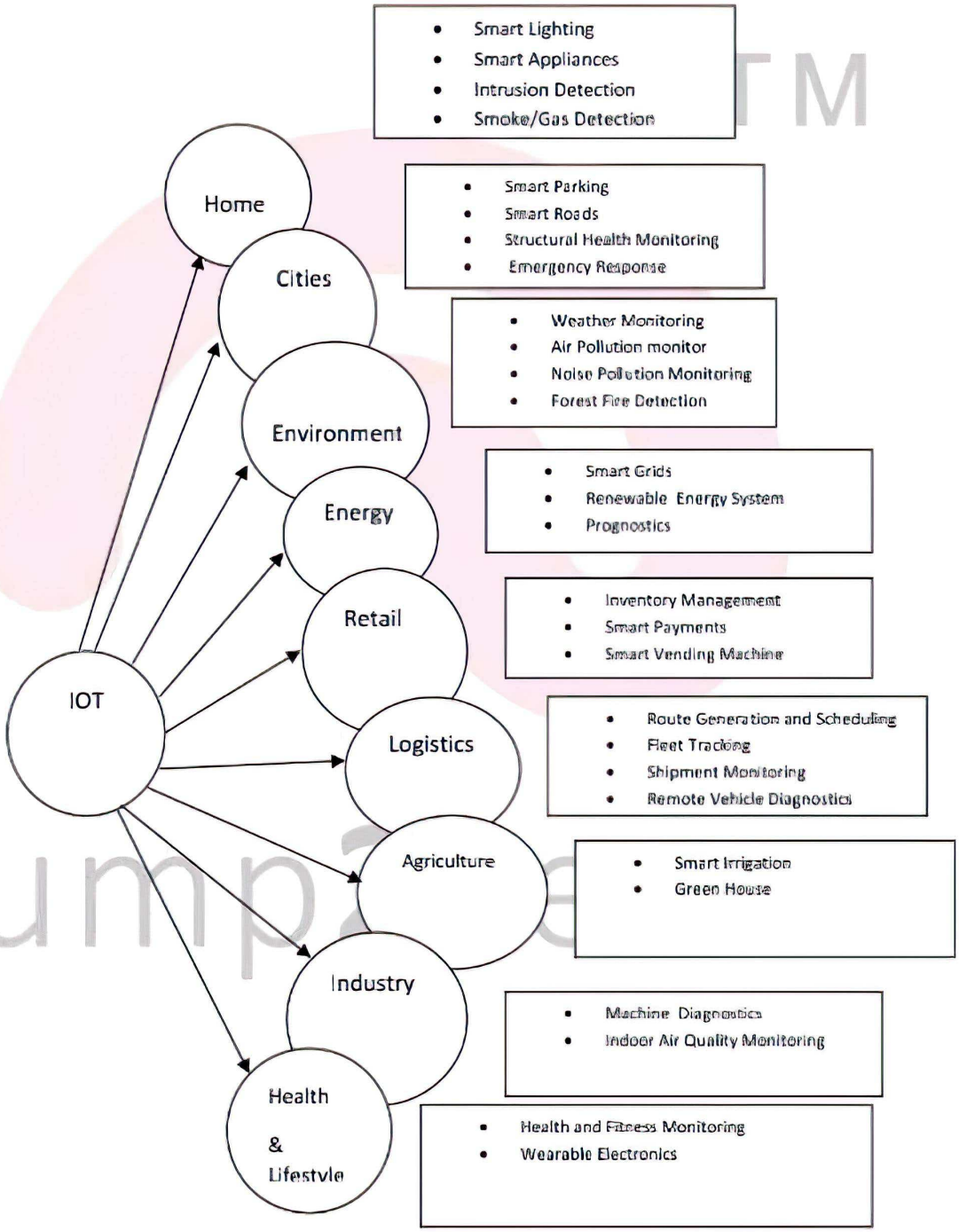


Fig :- Applications of IOT

Definition

A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities , physical attributes, virtual personalities and intelligent interfaces, and they are seamlessly integrated into information network where often communication data associated with users and environment.

Characteristics

- **Dynamic & Self Adapting:-**

  IOT Devices and systems may have the capabilities to dynamically adapt with the changing contents and take actions based on their operating condition, Users context, sensed based environment. Take a example If a Surveillance system comprising of a number of surveillances camera then this cameras can adapt their modes from normal to infrared night modes and vice versa based on whether it is night or day. Camera can switch from lower resolution to higher resolution modes when any motion is detected and alert surrounding cameras to do the same. Here Surveillance system is adapting itself on the based of dynamic condition.

- **Self Configuring**

  IOT devices may have self configuring capabilities which will allow a large number of devices to work together to provide certain functionalities like weather monitoring. This devices have self configuring themselves in accordance to IOT infrastructure, networking setup and latest software upgrades with minimal user interface.

- **Interoperable and Communication Protocols**

  IOT devices may support a number of interoperable communications protocol and it can communicate with other devices and also with infrastructure.

- **Unique Identity**

  Each IoT devices have unique identity and unique identifier like IP address OR URI. IoT Systems may have intelligent interfaces which can adapt based on context and it can allow

to communicate with users and the environmental contexts. IoT device interface can allow users to query the devices and monitor their status. Also it can be control remotely in association with control , configured and managed infrastructure

- **Integrated into Information Network**

IoT devices are usually integrated into information network that allows them to communicate and exchange data with other devices and systems. IoT device can dynamically discovered in the network by other devices and network and it have the capability to describe their characteristics to other devices and user applications.

Take an example of weather monitoring node can describe the monitoring capabilities to another connected node so that they can communicated and exchange data. This integration into information in the system will help in making IoT systems smarter due collective intelligence of each individual node devices in collaboration with infrastructure. This data from large number of weather monitoring IoT nodes can aggregated analyzed to predict weather.

Component of IoT

The hardware utilized in IoT systems includes devices for remote dashboard, devices for control, servers, routing or bridge devices and sensors. These devices manage the tasks and function such as system activation, specific action, security , communication and detection to support specific goals and actions. Major components of IoT devices are as follows

(1) Control Unit :- A small computer on a single integrated circuit containing processor, memory, programmable I/O peripheral and it is control unit responsible for main operation

(2) Sensor :- Devices that can measure a physical quantity and convert it into a signal which will be read and interpreted by the microcontroller unit. These devices consists of energy modules, power management modules RF Modules and sensing modules. Most of the sensor falls into two categories i.e. Digital or analog. An analog data is converted to digital value that can be transmitted to the internet like Temperature sensor, Light sensor etc.

(3) Communication Modules :- These are the part of the devices and responsible for communication with rest of the IoT platform. They provide connectivity according to wireless or wired communication.

(4) Power sources : - It is a small devices the current is usually produced by sources like batteries, thermocouples and solar cells.

Working of IoT : IoT working is as follows

(1) Collect and transmit data :- The device can sense the environment and collect the information related to it and transmit it to a different devices or internet

(2) Actuate devices based on triggers :- It can be programmed to actuate other devices based on condition set by the user

(3) Receive Information:- Device can also receive information from the network

(4) Communication assistance :- It provides communication between two devices of same network or different network.

Advantages and Disadvantages of IoT

(1) Improved customer engagement and communication.

(2) Support for technology Optimization

(3) Support wide range of data collections

(4) Reduced waste

Disadvantage of IoT

(1) Loss of Privacy and Security

(2) Flexibility

(3) Complexity

(4) Compatibility

1.2 Introduction to IoT Architecture

IOT technology has a wide variety of applications and use of Internet of Things is growing so faster. Depending upon different application areas of Internet of Things, it works accordingly as per it has been designed/developed. But it has not a standard defined architecture of working which is strictly followed universally. The architecture of IoT depends upon its

functionality and implementation in different sectors. Still, there is a basic process flow based on which IoT is built. Let us discussed 4 Stage IoT architecture

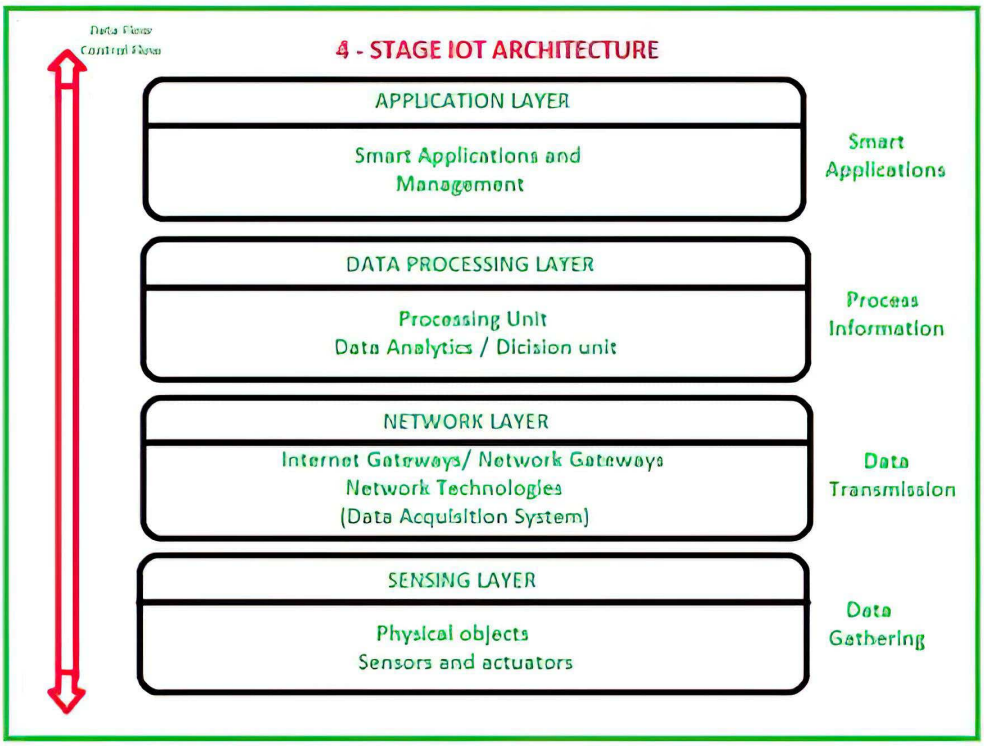


Fig :- 4 Stage Architecture of IOT

So, from the above figure it is clear that there is 4 layers are present that can be divided as follows: Sensing Layer, Network Layer, Data processing Layer, and Application Layer.

These are explained as following below.

- **Sensing Layer –**

Sensors, actuators, devices are present in this Sensing layer. These Sensors or Actuators accepts data(physical/environmental parameters), processes data and emits data over network.

- **Network Layer –**

Internet/Network gateways, Data Acquisition System (DAS) are present in this layer. DAS performs data aggregation and conversion function (Collecting data and aggregating data then converting analog data of sensors to digital data etc.). Advanced gateways which mainly opens up connection between Sensor networks and Internet also performs many basic gateway functionalities like malware protection, and filtering also sometimes decision making based on inputted data and data management services, etc.

- **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 often termed as business applications where data is monitored and managed and further actions are also prepared. So here Edge IT or edge analytics comes into picture.

- **Application Layer**

This is last layer of 4 stages of IoT architecture. Data centers or cloud is management stage of data where data is managed and is used by end-user applications like agriculture, health care, aerospace, farming, defense, etc.

1.3 Physical Design of IOT

1.3.1 Things in IOT

Things of IOT is usually refers to as IoT devices which have unique identities and can perform remote sensing, actuating and monitoring capacitates. IoT devices can exchange data with other connected devices and applications directly or indirectly. It can also collect data from other devices and process the data either locally or send the data to centralized servers applications back end for processing the data. It can also perform some task locally and other tasks within IoT infrastructure which is based on temporal and space constraints.

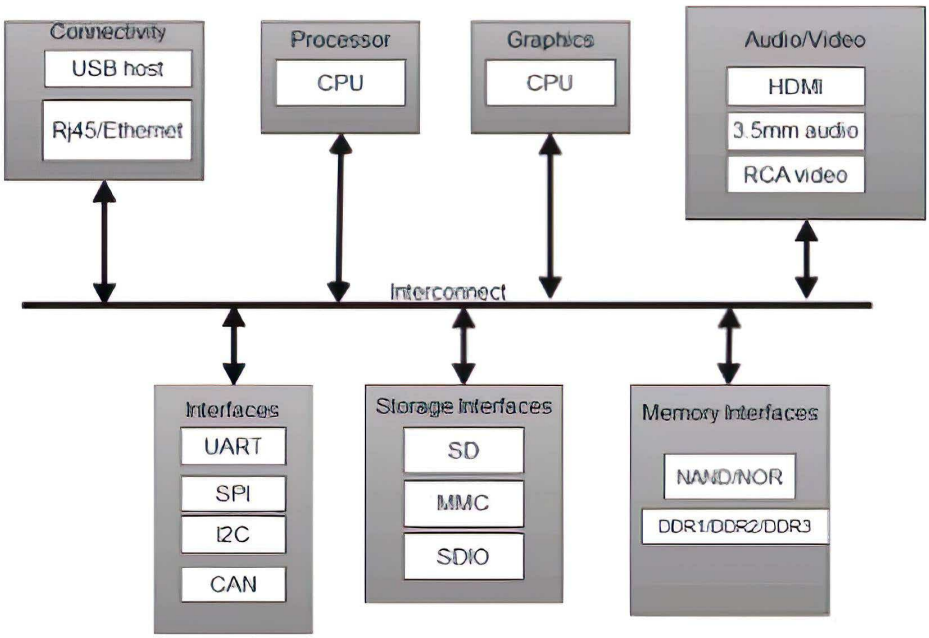


Fig:- Generic Block Diagram of IOT Device

The above Figure shows a block diagram of IoT device. An IoT device may consists of several interfaces for connections to other device which can wired or wireless. This can include

(i) I/O Interface for sensors

(ii) Interface for Internet connectivity

(iii) Memory and storage interface

(iv) Audio Video interface

An IoT device can also be connected to actuators that allow them to interact with other physical entities including non IoT devices in the neighbourhood of the device.

An IoT device can also be of various types for instance wearable sensors, smart watches, LED lights, automobiles and industrial machines. Almost all IoT devices generate data in some form which can processed by data analytic teams which then lead to information to guide further action.

1 .3.1 IOT Protocols

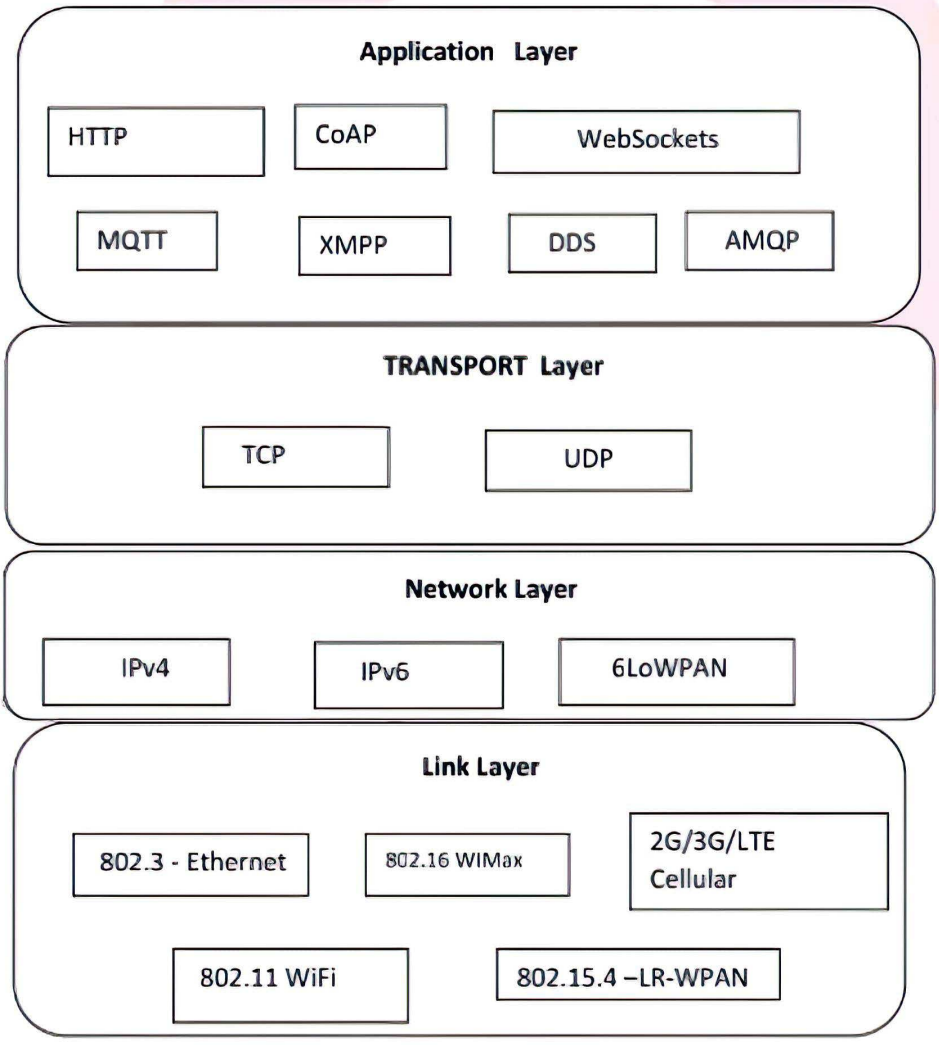


Fig :- IoT Protocol

We can divide IoT Protocols as Protocols of Link Layer, Protocols Network Layer, Protocols of Transport Layer and Protocols of Application Layers

(A) LINK LAYER :- Link Layers Protocols will determine how data is physically send over the network physical layer or medium. The scope of link layer is local network connection to which host is attached. Hosts on same link exchange the data packets over the link layer using link layer protocols. In Link layer it is determine how packets are coded and signalled by the hardware device over the medium to which host is attached. Some the Link layer protocols are

(1) 802.3-Ethernet : IEEE 802.3 is collection wired Ethernet standard for link layer. These standards provides data rates from 10Mbs to 40Gbs and higher. The shared medium in Ethernet can be coaxial cables, twisted-pair or optical fibre. This shared medium carries the communication for all the devices in the network. So the data sent by the one device can be received by all devices subject to propagation conditions and transceiver capabilities.

(2) 802.11 WiFi : IEEE 802.11 is collection of wireless local area network (WLAN) communications standards. 802.11a operates at 5GHZ band , 802.11b and 802.11g operate at 2.4GHZ band, 802.11coperates at 5 GHZ band, 802.11ad operates at 60 HZ band. These standards provide data rates from 1 MBS/s to 6.7 GHZ/s.

(3) 802.16 WiMax :- IEEE 802.16 is collection of wireless broadband standards. WiMax standards provides data rates from 1.5 Mb/s to 1 Gb/s.

(4) 802.15.4 LR-WPAN: IEEE 802.15.4 is a collection of standards for low rate wireless personal area networks (LR-WPAN). These standards form the basis of specifications for high level of communication protocols such ZIGBEE. LR-WPAN standards provide data rates from 40 Kb/s to 250 Kb/s. These standards provide low-cost and low-speed communication for power constrained devices.

(5) 2G/3G/4G- Mobile Communication:- There are different generations of mobile communications standards, including 2nd Generation i.e. 2G GSM and CDMA, 3rd Generation including UMTS and CDMA 2000, 4th Generation i.e. LTE. IoT devices based on these standards

can communicate over cellular networks. Data rates for these standards range from 9.6 Kb/S for 2G to 100 Mb/s for 4 G.

(B) NETWORK/INTERNET LAYER :- The network layer is responsible for sending of IP datagram from the source network to the destination network. This layer performs the host addressing and packet routing. The datagram contains the source and destination addresses which are used to route the data packet from the source network to destination network across multiple network. Some of the network /internet protocols are:

(1) IPv4 :- Internet Protocol version 4 is the most deployed Internet protocol that is used to identify the devices on a network using hierarchical addressing scheme. IPv4 uses a 32 bit addressing scheme that allows total of 2^{32} addresses. The IP protocol establish connection on packet network but do not guarantee delivery of packets

(2) IPv6 :- Internet Protocol version 6 is the newest version of Internet Protocols and it is successor of IPv6. Which uses 128 bit address scheme which allows total of 2^{128} addresses.

(3) 6LoWPAN: IPv6 over Low power wireless Personal Area Network bring IP Protocol to the low power devices which have limited processing capability. It operates in 2.4GHz frequency range and provides data transfer rates of 250Kb/s.

(C) TRANSPORT LAYER: - Transport Layer protocols provide end to end message transfer capability independence of network. The message transfer capability can set up on connection either using handshakes i.e. TCP or without handshake / acknowledgements i.e. UDP.

(1) TCP: - Transmission Control Protocol is most widely used transport layer protocol that is used by web browser along with HHTP, HTTPS, email protocol i.e. SMTP and File Transfer Protocol (FTP). TCP is connection oriented protocol. TCP ensures reliable transmission of packets in order. TCP also provides error detection capability so that duplicate packets can be discarded and lost packet can be retransmitted. Flow control of TCP make sure that rate at which sender sends the data is not too high for the receiver to process the packet. The congestion control capability helps in avoiding network congestion due to which congestion collapse occurs which will leads to degradation of network performance

(2) UDP: - UDP is connectionless protocol. It is useful for time sensitive application that have very small data units to exchange and do not want the overhead of connection setup. UDP is

transaction oriented and stateless protocol. UDP does not provide guaranteed delivery, Ordering of message and duplicate elimination.

(D) APPLICATION LAYER:- Application layer protocols define how the application interface with lower level protocols to send the data over the network. The application data are generally in files which is encoded by the application layer protocols and then encapsulated in transport layer protocol which then provides the connection over the network. Generally Port No are used for application addressing like port no 80 for HTTP. Various protocols in application layer for IoT are as follows

(1) Web Socket: - Web socket protocols allows full duplex communication over a single socket connection for sending messages between client and server. Web socket is based on TCP and allows Streams of message to be send back and forth between client server during which TCP connection remain open.

(2) MQTT: - Message Queue Telemetry Transport is light weight messaging protocol based on Published Subscribe Model. MQTT used client server architecture where any IOT device which works as client will get connected to server (which is also a MQTT Broker) and publish messages to topic on server. Now the broker will forward the message to the clients subscribed to topics. MQTT is suited for constraint environment where the IOT devices have limited processing and memory resources and bandwidth is low.

(3) AMQP: - Advance Message Queuing Protocol is open application layer protocol for business message. AMQP supports both point to point and Publisher/Subscriber Models, Routing and Queuing. AMQP brokers receives message from publisher i.e. IOT device or applications which generate data. Publisher publish the message to exchanges which then distribute message copies to queries. Messages are either delivered by the broker to the consumers which have subscribed to the queues or to the consumers which pull the messages from the queue.

1.4 Logical Design of IOT

Logical Design of IoT System means it is an abstract of the entities and processes without going into low level specification and implementation. Here we will discuss about functional blocks of an IoT system and Communications API that are used generally.

1.4.1 IoT Functional Blocks

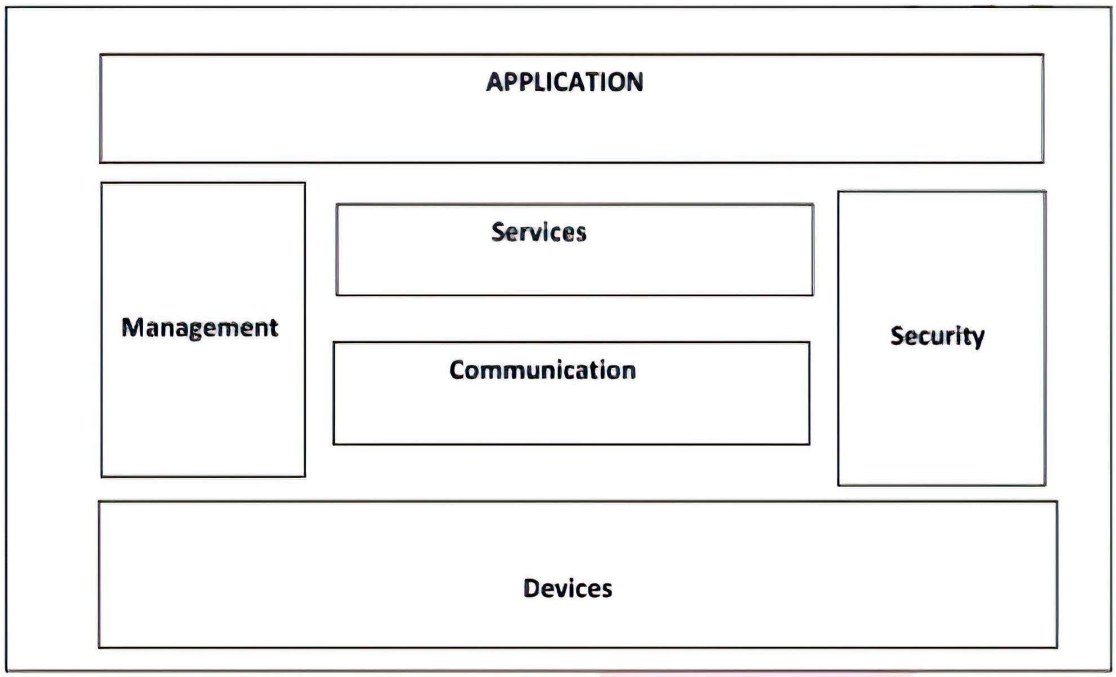


Fig : Functional Blocks of IoT

An IoT consists of number of functional blocks that provide the systems the capability for identification, sensing, actuation, communication and management as per above figure. The functional blocks are as follows:

(1) Devices : An IoT system consists of devices that provide sensing, actuation, monitoring and control function.

(2) Communication:- The Communication blocks handles the communication for the IoT system. Here various protocols which are used for communication and services to discover the devices are explained

(3) Services :- An IoT System uses various types of IoT services such services for device monitoring, devices for control services, device for publishing services and services for device discovery.

(4) Management :- Management Functional block provides various function to govern IoT system

(5) Security :- Security functional block secures the IoT system and provides the function through which one can have authentication, authorization, message and content integrity and data security.

(6) Application:- IoT Applications provide an interface that the users can use to control and monitor various functions of IOT system. It allows the users to view the system status and view or analyze the processed data.

1.4.1 IoT Communicational Models.

(1) Request- Response

(2) Publish – Subscribe

(3) Push- Pull

(4) Exclusive Pair

(1) Request Response

Request Response is a communication Model in which client sends the requests to the server and server responds to the requests. When the server receives a request then server decides how to respond, how to fetch the data, how to retrieve the resource representation, how to prepare the response and then it will sends the response to the client. In Request-Response is a stateless communication model and each request-response pair is independent of each other.

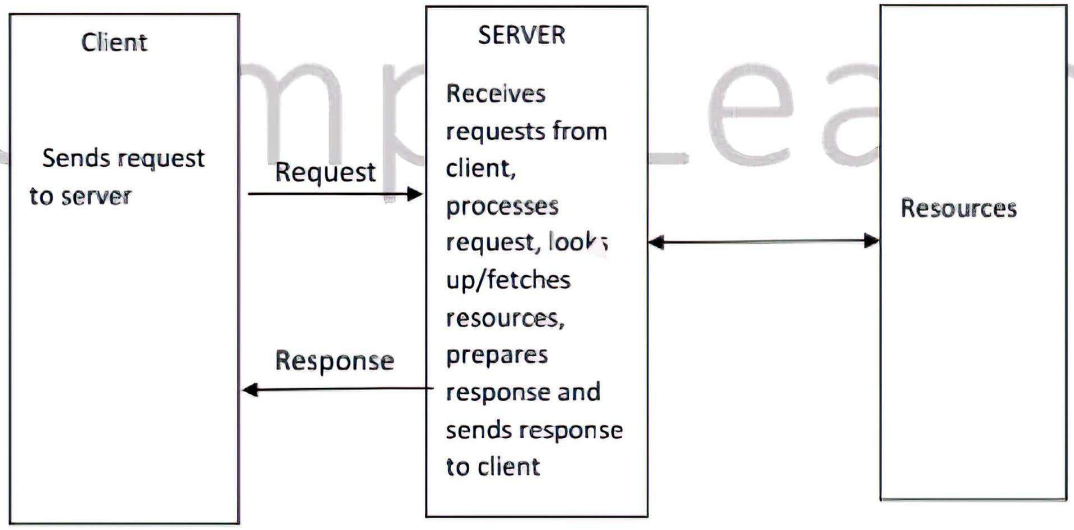


Fig : Request –Response Communication Model

(2)Publish-Subscribe :

Publish Subscribe is a communication model that involves publisher, brokers and consumers. Publisher the source of the data. Publisher sends the data to the topics which are managed by the broker. Publisher are not aware of the consumers. Consumers subscribe to the topics which are manage by the brokers. When brokers receives the data for a topic from the publisher it sends data to all subscribed consumer

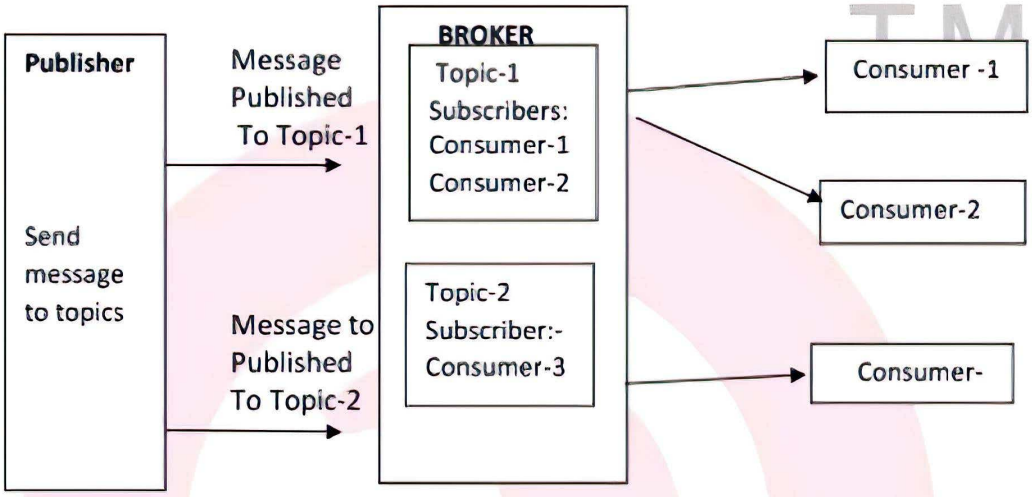


Fig:- Published Subscribe Communication Model

(3) Push-Pull.

Push-Pull is a communication model in which the data producer push the data to the queues and the consumers pull the data from the queues. Producer are not necessary need to be aware of the consumers. Queues help in decoupling the messaging between producers and consumers. Queues act as a buffer which helps in situation when there is mismatch between the rate at which producer is pushing the data and the rate at which consumer is pulling the data.

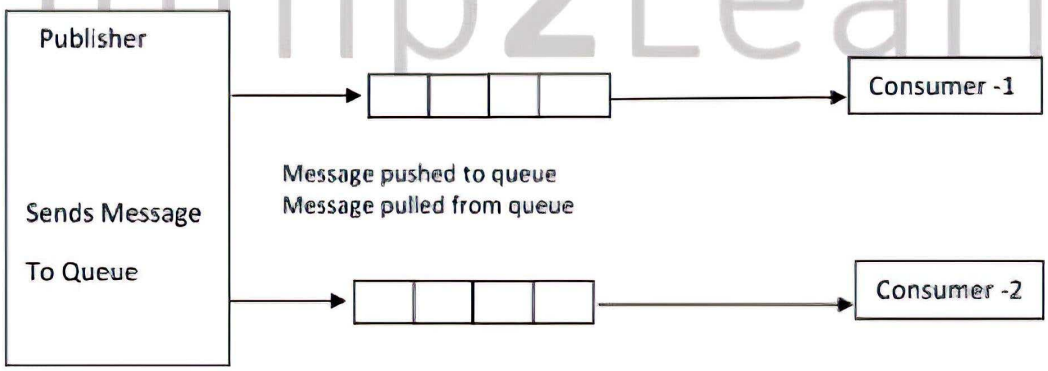


Fig : Push Pull Communication Model

(4) Exclusive Pair

Exclusive Pair is bi-directional fully duplex communication model that uses a persistent connection between the client and server. Once the connect is setup it remains open until client sends a request to close the connection to the server. Client and server can send message to each other after connection setup. Exclusive-Pair is a stateful communication model and server is aware of all the open connection.

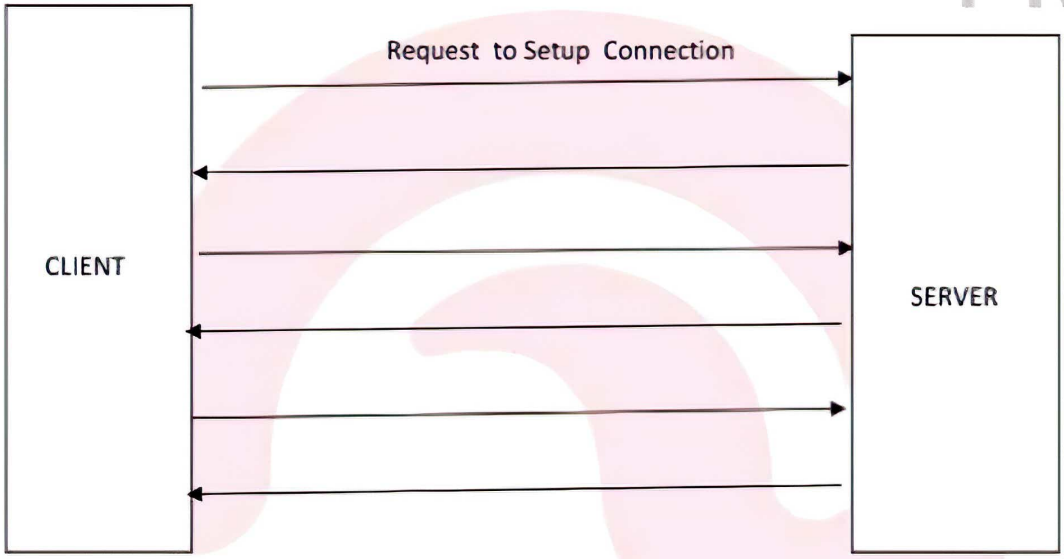


Fig :- Exclusive Pair Communication Model.

****