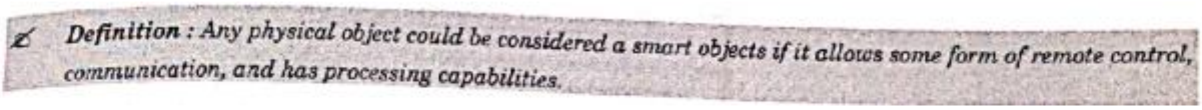
Smart Objects IoT

Smarts Objects:

- A smart object is an object that enhances the interaction with other smart objects as well as with people also.
- The world of IoT is the network of interconnected heterogeneous objects (such as smart devices, smart objects, sensors, actuators, RFID, embedded computers, etc.) uniquely addressable and based on standard communication protocols.
- Smart objects are utilized widely to transform the physical environment around us to a digital world using the Internet of things (IoT) technologies.

In a day to day life, people have a lot of object with internet or wireless or wired connection. Such as:

- Smartphone
- Tablets
- TV computer



***Definition :** Any physical object could be considered a smart objects if it allows some form of remote control, communication, and has processing capabilities.*

A smart object typically has the following components.

A smart object typically has the following components. There could be more, but these are the foundational ones. Controlling System: The controlling system controls, manages, and operates the smart object. It typically runs a Real-Time Operating System (RTOS). RTOS provides a time-guarantee of completion for the given real-time tasks. The scheduler, in a RTOS, is designed to provide a predictable (deterministic) execution pattern.

Sensors: Sensors get various inputs from the operating, depending upon the requirements. Sensors provide inputs to the control system may decide further processing steps.

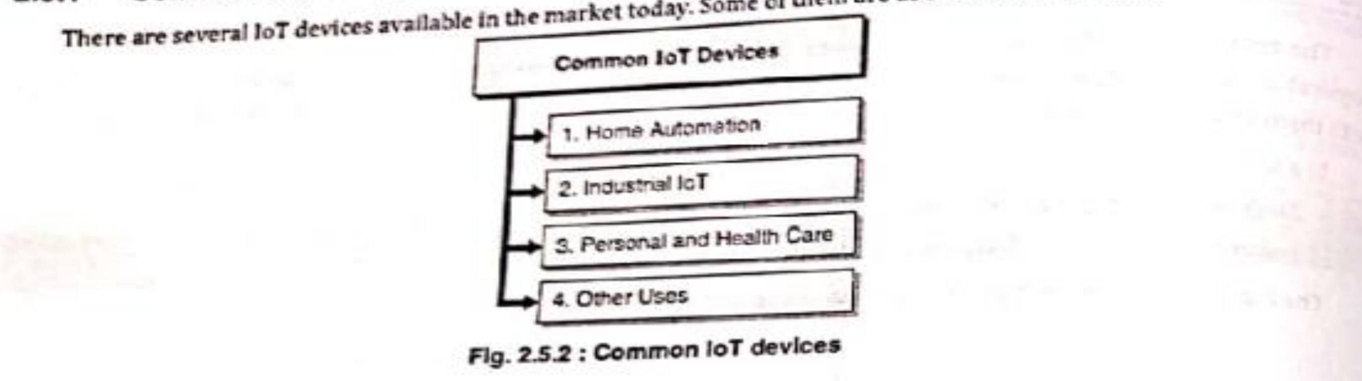
Actuators: Actuators control the operating environment as reg A smart object may have one or more actuators perform operations in the operating environment as directed. depending upon the requirements.

Communication Interface :

Power Source:

2.5.1 Common Smart Objects (IoT Devices)

There are several IoT devices available in the market today. Some of them are as shown in Fig. 2.5.2.



Common IoT Devices

1. Home Automation

2. Industrial IoT

3. Personal and Health Care

4. Other Uses

Fig. 2.5.2 : Common IoT devices

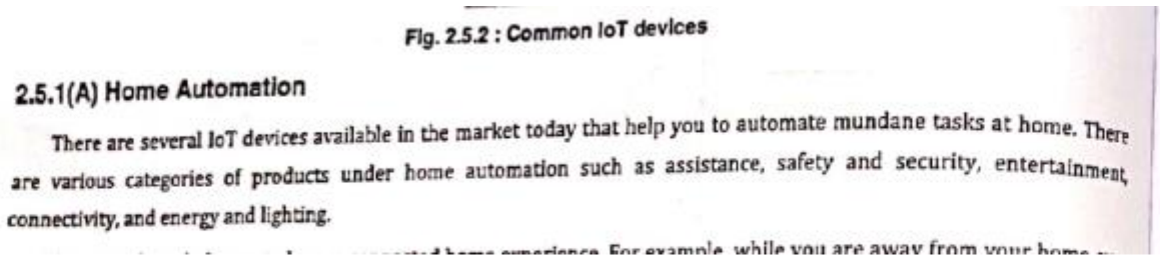
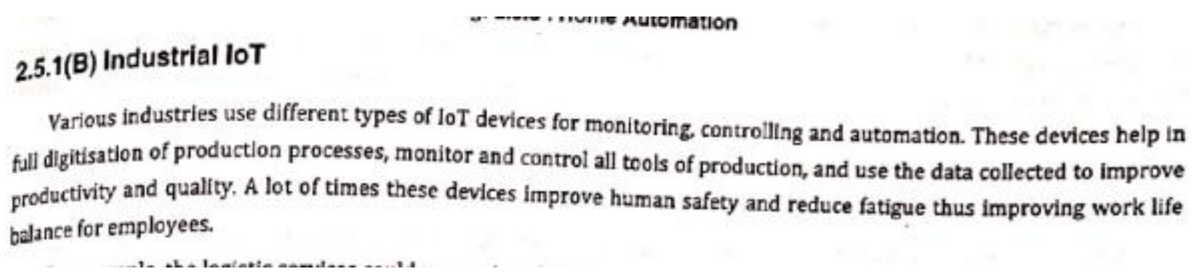


Fig. 2.5.2 : Common IoT devices

2.5.1(A) Home Automation

There are several IoT devices available in the market today that help you to automate mundane tasks at home. There are various categories of products under home automation such as assistance, safety and security, entertainment, connectivity, and energy and lighting.

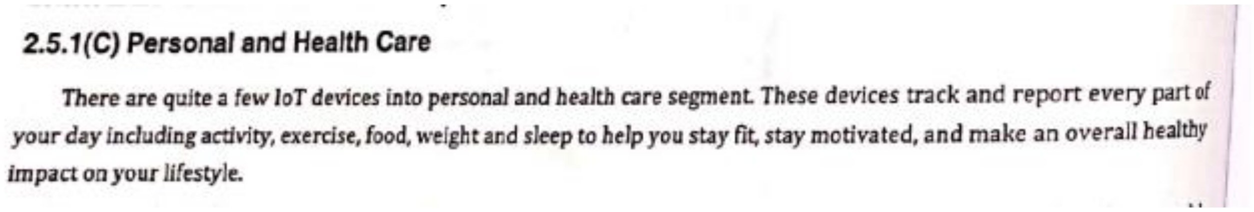
... connected home experience. For example while you are away from your home ...


Home Automation

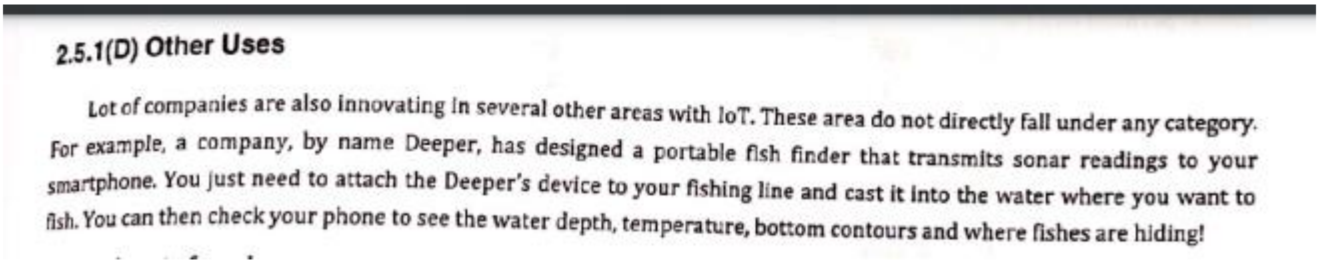
2.5.1(B) Industrial IoT

Various industries use different types of IoT devices for monitoring, controlling and automation. These devices help in full digitisation of production processes, monitor and control all tools of production, and use the data collected to improve productivity and quality. A lot of times these devices improve human safety and reduce fatigue thus improving work life balance for employees.

... example, the logistic services could ...


2.5.1(C) Personal and Health Care

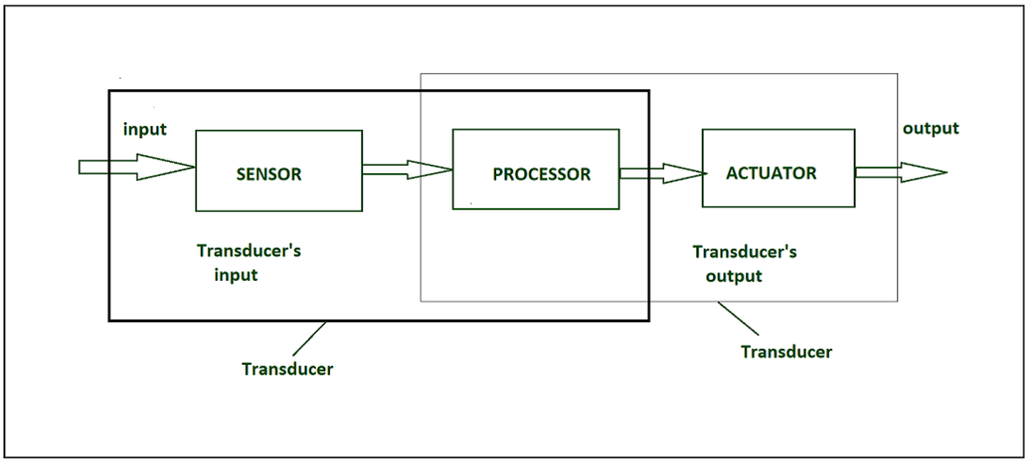
There are quite a few IoT devices into personal and health care segment. These devices track and report every part of your day including activity, exercise, food, weight and sleep to help you stay fit, stay motivated, and make an overall healthy impact on your lifestyle.


2.5.1(D) Other Uses

Lot of companies are also innovating in several other areas with IoT. These area do not directly fall under any category. For example, a company, by name Deeper, has designed a portable fish finder that transmits sonar readings to your smartphone. You just need to attach the Deeper's device to your fishing line and cast it into the water where you want to fish. You can then check your phone to see the water depth, temperature, bottom contours and where fishes are hiding!

✂Sensors:

- Sensors are used for sensing things and devices etc.
- A device that provides a usable output in response to a specified measurement.
- The sensor attains a physical parameter and converts it into a signal suitable for processing (e.g. electrical, mechanical, optical) the characteristics of any device or material to detect the presence of a particular physical quantity.
- The output of the sensor is a signal which is converted to a human-readable form like changes in characteristics, changes in resistance, capacitance, impedance, etc.



Transduce :

- A transducer converts a signal from one physical structure to another.
- It converts one type of energy into another type.
- It might be used as actuator in various systems.

Sensor Classification:

- Passive & Active
- Analog & digital
- Scalar & vector

Passive Sensor –Can not independently sense the input. Ex- Accelerometer, soil moisture, water level and temperature sensors.

Active Sensor – Independently sense the input. Example- Radar, sounder and laser altimeter sensors.

Analog Sensor – The response or output of the sensor is some continuous function of its input parameter. Ex-Temperature sensor, LDR, analog pressure sensor and analog hall effect.

Digital sensor –Response in binary nature. Design to overcome the disadvantages of analog sensors. Along with the analog sensor, it also comprises extra electronics for bit conversion. Example – Passive infrared (PIR) sensor and digital temperature sensor(DS1620).

Scalar sensor – Detects the input parameter only based on its magnitude. The answer for the sensor is a function of magnitude of some input parameter. Not affected by the direction of input parameters.

Example – temperature, gas, strain, color and smoke sensor.

Vector sensor –The response of the sensor depends on the magnitude of the direction and orientation of input parameter. Example – Accelerometer, gyroscope, magnetic field and motion detector sensors.

☣Types of sensors:

Temperature Sensor:

- Devices which monitors and tracks the temperature and gives temperature’s measurement as an electrical signal are termed as temperature sensors.
- These electrical signals will be in the form of voltage and is directly proportional to the temperature measurement.

Speed Sensor:

Sensor used for detecting the speed of any object or vehicle which is in motion is known as speed sensor.

For example – Wind Speed Sensors, Speedometer ,UDAR ,Ground Speed Radar.

Light sensor:

- Light sensor is also known as photo sensors and one of the important sensor.
- Light dependent resistor or LDR is a simple light sensor available today.

Mechanical sensor:

Any suitable mechanical / electrical switch may be adopted but because a certain amount of force is required to operate a mechanical switch it is common to use micro-switches.

Touch sensor:

Detection of something like a touch of finger or a stylus is known as touch sensor

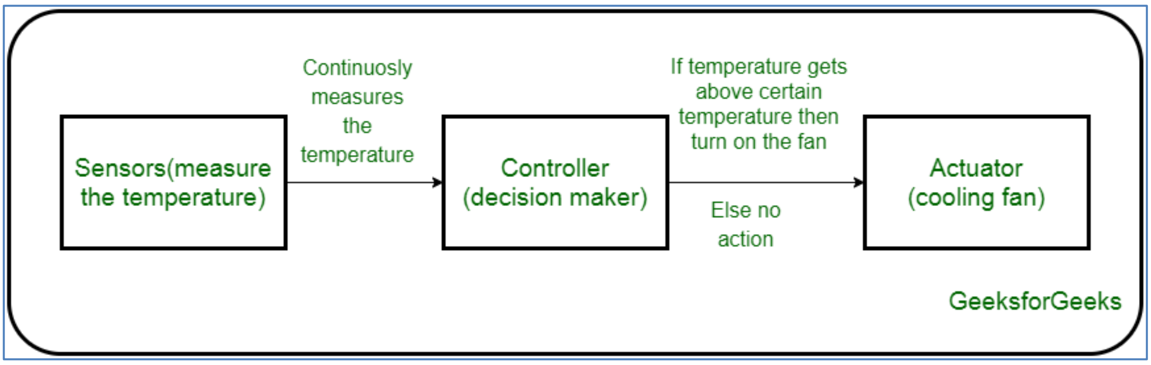
Pneumatic sensor:

These proximity sensors operate by breaking or disturbing an air flow.

The pneumatic proximity sensor is an example of a contact type sensor. These cannot be used where light components may be blown away.

ॐActuators:

- An actuator is a machine component or system that moves or controls the mechanism of the system.
- Sensors in the device sense the environment, then control signals are generated for the actuators according to the actions needed to perform.
- A servo motor is an example of an actuator.
- They are linear or rotatory actuators, can move to a given specified angular or linear position.
- We can use servo motors for IoT applications and make the motor rotate to 90 degrees, 180 degrees, etc., as per our need.


Sensors(measure the temperature)
Continuosly measures the temperature
Controller (decision maker)
If temperature gets above certain temperature then turn on the fan
Else no action
Actuator (cooling fan)
GeeksforGeeks

✡Types of Actuators:

1. hydraulic actuator

A hydraulic actuator uses hydraulic power to perform a mechanical operation. They are actuated by a cylinder or fluid motor. The mechanical motion is converted to rotary, linear, or oscillatory motion, according to the need of the IoT device. Ex- construction equipment uses hydraulic actuators because hydraulic actuators can generate a large amount of force.

Advantages:

- Hydraulic actuators can produce a large magnitude of force and high speed.
- Used in welding, clamping, etc.
- Used for lowering or raising the vehicles in car transport carriers.

Disadvantages:

- Hydraulic fluid leaks can cause efficiency loss and issues of cleaning.
- It is expensive.
- It requires noise reduction equipment, heat exchangers, and high maintenance systems.

2. Pneumatic Actuators –

A pneumatic actuator uses energy formed by vacuum or compressed air at high pressure to convert into either linear or rotary motion. Example- Used in robotics, use sensors that work like human fingers by using compressed air.

Advantages:

- They are a low-cost option and are used at extreme temperatures where using air is a safer option than chemicals.
- They need low maintenance, are durable, and have a long operational life.
- It is very quick in starting and stopping the motion.

Disadvantages:

- Loss of pressure can make it less efficient.
- The air compressor should be running continuously.
- Air can be polluted, and it needs maintenance.

3. Electrical Actuators –

An electric actuator uses electrical energy, is usually actuated by a motor that converts electrical energy into mechanical torque. An example of an electric actuator is a solenoid based electric bell.

Advantages:

- It has many applications in various industries as it can automate industrial valves.
- It produces less noise and is safe to use since there are no fluid leakages.
- It can be re-programmed and it provides the highest control precision positioning.

Disadvantages:

- It is expensive.
- It depends a lot on environmental conditions.

4.Thermal/Magnetic Actuators –

These are actuated by thermal or mechanical energy. Shape Memory Alloys (SMAs) or Magnetic Shape-Memory Alloys (MSMAs) are used by these actuators. An example of a thermal/magnetic actuator can be a piezo motor using SMA.

5.Mechanical Actuators –

- A mechanical actuator executes movement by converting rotary motion into linear motion. It involves pulleys, chains, gears, rails, and other devices to operate. Example – A crankshaft.
- Soft Actuators
- Shape Memory Polymers
- Light Activated Polymers
- With the expanding world of IoT, sensors and actuators will find more usage in commercial and domestic applications along with the pre-existing use in industry.

❅**Trends in Smart Objects**

1.Consumer IoT (CIoT) and Industrial IoT (IIoT)

CIoT is an IoT ecosystem that assists organizations with improving user experience by utilizing “insight” on users’ Internet-connected gadgets.

The customer IoT market is active for the last five years and is giving indications of slowing down. The Industrial Internet of Things on the other hand will start getting more attention as more and more companies start building modern industrial systems that want the adoption of IoT.

2. Smart homes will become a norm

Even people who discarded smart homes as devices for pretentious youngsters are now finding it difficult to ignore the capabilities the technology comes with. While it started with a steady growth, the demand for connected home devices will see a sharp rise in the years to come.

3. Cloud & edge computing

For a long time, the IoT devices have been relying on the cloud for storing their data. But the IoT application development industry has now started wondering about the implications of utilizing storing, calculation, and analyzing data to limit.

They are demanding that instead of sending the data from IoT devices to cloud, the data should first be transferred to local devices which are closer to the edge of the network. This local storage helps in sorting, filtering, and calculating the data and sending a part or the whole data to the cloud, thus reducing the traffic to network.

Edge computing offers a series of benefits to an iot application development company and developers, which makes it one of the key emerging trends in IoT technology –

- Better management of large amount of data which every device sends
- Lowered dependency on cloud helping apps perform faster with reduced latency
- IoT based mobile apps consumes less bandwidth.

4. A greater focus on IoT security

With the adoption being on a rise, more and more devices are getting connected to the Internet of Things. And as the network is expanding, the volume of data is also expanding and there is more information which is at risk. In fact, the security vulnerability has also become a prominent answer of what are the challenges in IoT domain.

5. Unified IoT framework

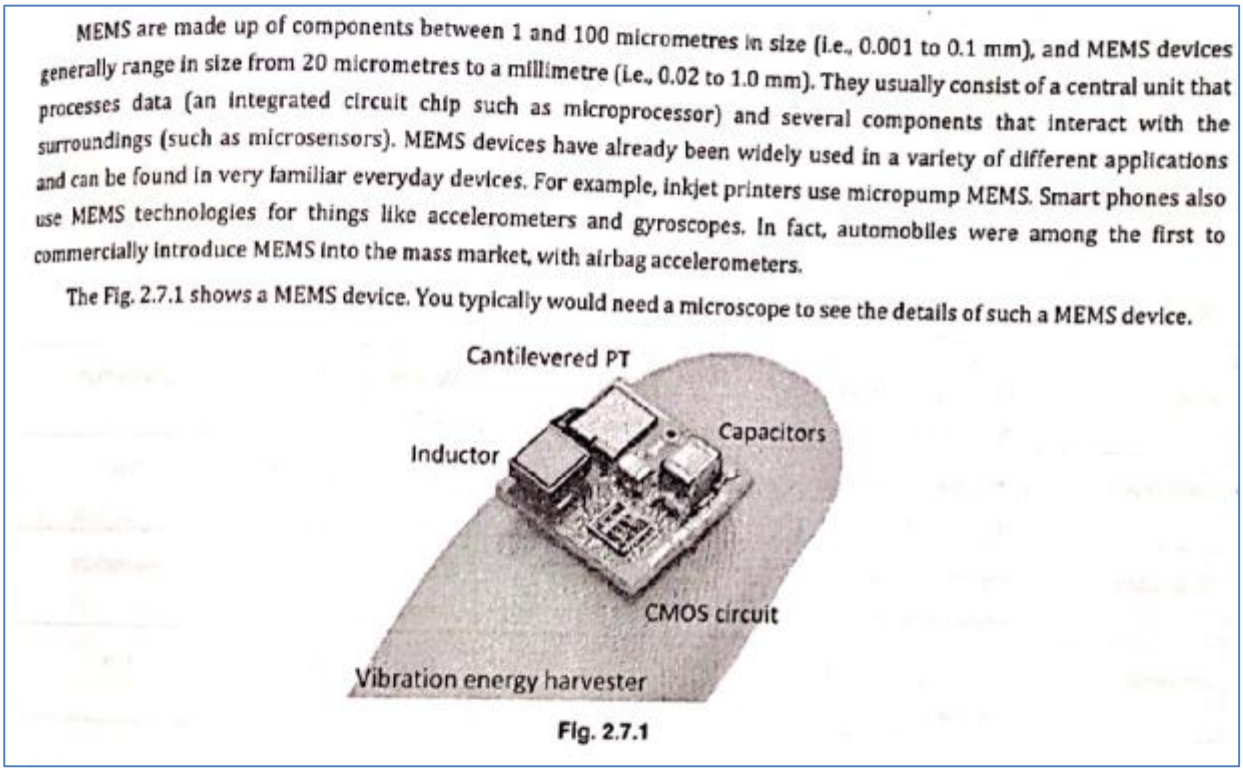
The absence of a unified IoT framework is something that has been a major challenge for the IoT industry for a long time. The fact that not many companies work around a shared central platform, affects the adoption process to a huge extent.

6.Increased consumer adoption

One of the prime IoT market trends and the time to come will see IoT being used for not just personal or consumer based use but also industrial use. A validation of this can be seen in the numbers that the IoT connecting devices were set to grow to over 3.7 billion by 2019 and to over 50 billion by the time next year ends.

✳Micro-Electro-Mechanical Systems (MEMS):

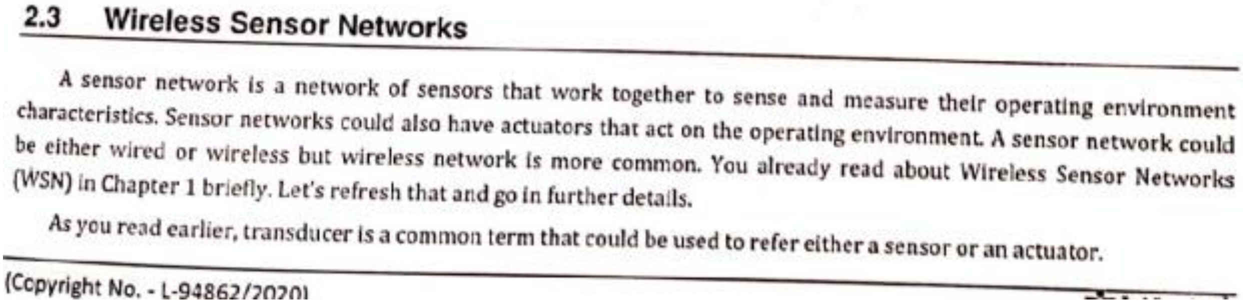
- Micro-electromechanical systems (MEMS) are a process technology used to create tiny integrated devices or systems that combine mechanical and electrical components.
- They are fabricated using integrated circuit (IC) batch processing techniques and can range in size from a few micrometres to millimetres.
- These devices (or systems) have the ability to sense, control and actuate on the micro scale, and generate effects on the macro scale.
- The combination of tiny size, low cost, and the ability to mass produce MEMS an attractive option for a huge of, a IOT applications.



MEMS are made up of components between 1 and 100 micrometres in size (i.e., 0.001 to 0.1 mm), and MEMS devices generally range in size from 20 micrometres to a millimetre (i.e., 0.02 to 1.0 mm). They usually consist of a central unit that processes data (an integrated circuit chip such as microprocessor) and several components that interact with the surroundings (such as microsensors). MEMS devices have already been widely used in a variety of different applications and can be found in very familiar everyday devices. For example, inkjet printers use micropump MEMS. Smart phones also use MEMS technologies for things like accelerometers and gyroscopes. In fact, automobiles were among the first to commercially introduce MEMS into the mass market, with airbag accelerometers.

The Fig. 2.7.1 shows a MEMS device. You typically would need a microscope to see the details of such a MEMS device.

Fig. 2.7.1



2.3 Wireless Sensor Networks

A sensor network is a network of sensors that work together to sense and measure their operating environment characteristics. Sensor networks could also have actuators that act on the operating environment. A sensor network could be either wired or wireless but wireless network is more common. You already read about Wireless Sensor Networks (WSN) in Chapter 1 briefly. Let's refresh that and go in further details.

As you read earlier, transducer is a common term that could be used to refer either a sensor or an actuator.

Definition : Wireless Sensor Network (WSN) is a large collection of sensor devices that can monitor several physical conditions.

Each sensor device is called a sensor node. A sensor node can monitor several physical conditions such as temperature, air pressure, illumination of light, movement of people, wind speed, humidity, etc.

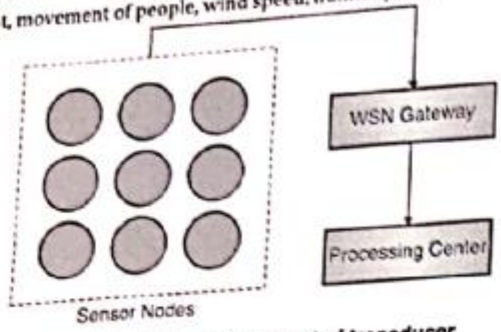


Fig. 2.3.1 : WSN - The Internet of transducer

The collected information is sent to the processing center via the WSN gateway. WSN gateway can also be called base station or a sink node. The processing center evaluates the information received from the various sensor nodes (via the WSN gateway) and then sends the instructions to the connected devices to act suitably.

WSNs typically use IEEE 802.15.4 standards. ZigBee is a popular WSN technology. WSNs are commonly used for area monitoring, weather prediction, security and industrial operations. IoT devices also use WSN technology as a foundational pillar for connecting several devices in a network.

2.3.1 WSN Topologies

WSNs are commonly deployed in the topologies shown in Fig. 2.3.2 (ways or configuration).

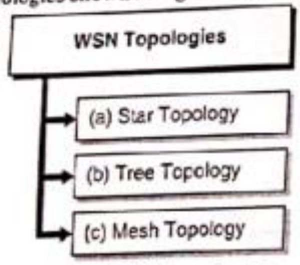


Fig. 2.3.2 : WSN topologies

1. Star Topology

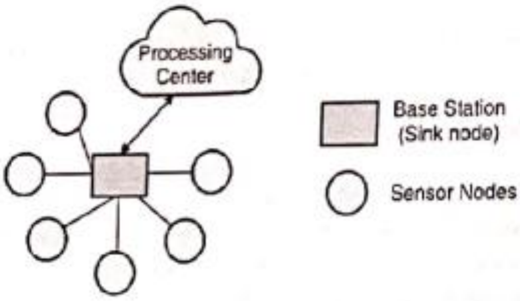


Fig. 2.3.3 : Star topology

In star topology, there is a single base station or sink node which acts as a hub and every sensor node in the network is connected to it. The base station sends the data to the processing center where the received data could be stored, analysed or processed as appropriate. The processing center could either be local or remote (say in the cloud). Star topology is very easy to implement, design and expand. As all the data flows through the single base station, it could be a single point of failure and could result into failure of the entire network.

2. Tree Topology

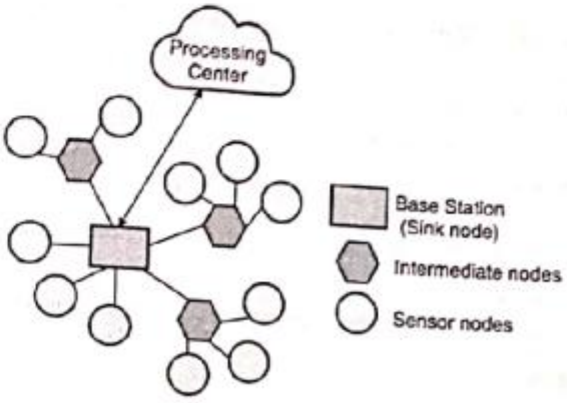


Fig. 2.3.4 : Tree topology

Fig. 2.3.4 : Tree topology

A tree topology is a hierarchical network where there is a single base station or sink node called root node. The root node is connected to many sensor nodes directly or could have another level of intermediate nodes that act as base stations for the respective sensor nodes that they manage. The hierarchy could be continued as desired.

The processing power, energy consumption and intelligence is highest at the root node and keeps on decreasing as you go down the hierarchical order.

3. Mesh Topology

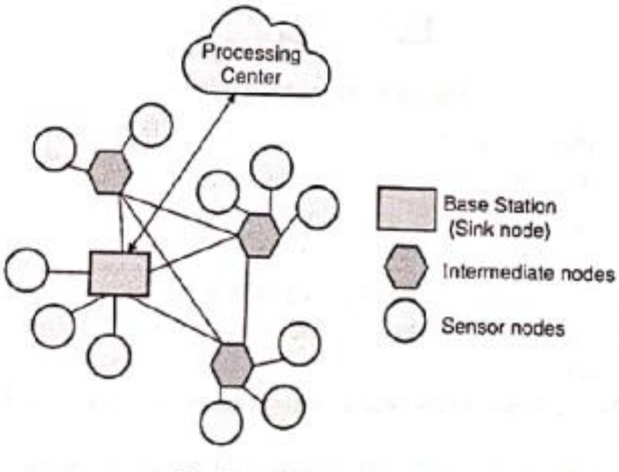


Fig. 2.3.5 : Mesh topology

In mesh topology, apart from transmitting its own data, each node could also act as a relay for transmitting data of other connected nodes. Mesh topologies are further divided into fully connected mesh (where each node is connected to every other node in the network) and partially connected mesh (where only a few nodes are interconnected to each other).

Mesh topology is complex to deploy but could be effective in building distributed networks and avoiding single point of failure.

Sensor Network Architecture is used in Wireless Sensor Network (WSN). It can be used in various places like schools, hospitals, buildings, roads, etc for various applications like disaster management, security management, crisis management, etc.

There are 2 types of architecture used in WSN: Layered Network Architecture, and Clustered Architecture.

1. Layered Network Architecture:

Layered Network Architecture makes use of a few hundred sensor nodes and a single powerful base station. Network nodes are organized into concentric Layers.

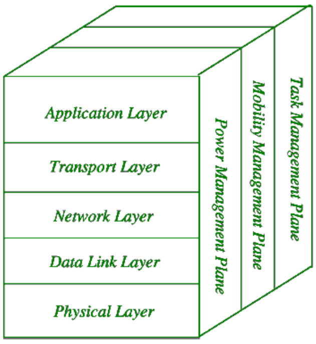
It consists of 5 layers and three cross layers.

The 5 layers are:

1. Application Layer
2. Transport Layer
3. Network Layer
4. Data Link Layer
5. Physical Layer

The cross layers consist of the following:

- Power Management Plane
- Mobility Management Plane
- Task Management Plane



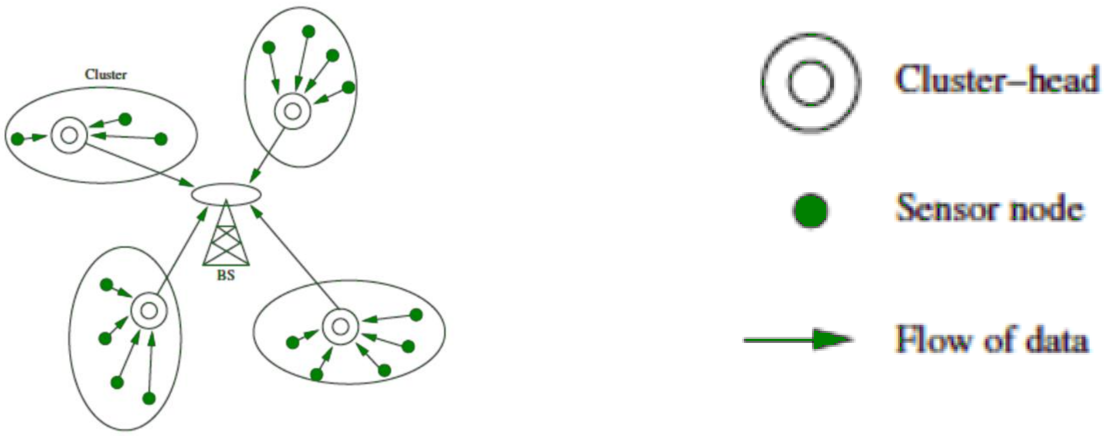
The advantage of using Layered Network Architecture is that each node participates only in short-distance, low power transmissions to nodes of the neighbouring nodes because of which power consumption is less as compared to other Sensor Network Architecture. It is scalable and has a higher fault tolerance.

2. Clustered Network Architecture:

In Clustered Network Architecture, Sensor Nodes autonomously clubs into groups called clusters. It is based on the Leach Protocol which makes use of clusters. Leach Protocol stands for Low Energy Adaptive Clustering Hierarchy.

Properties of Leach Protocol:

- It is a 2-tier hierarchy clustering architecture.
- It is a distributed algorithm for organizing the sensor nodes into groups called clusters.
- The cluster head nodes in each of the autonomously formed clusters create the Time-division multiple access (TDMA) schedules.
- It makes use of the concept called Data Fusion which makes it energy efficient.



Clustered Network Architecture is a very useful sensor network because of the property of Data Fusion. Inside each cluster, each node communicates with the cluster head to gather the information. All the clusters which are formed share their gathered information to the base station. The cluster formation and selection of cluster head inside each cluster is an independent and autonomous distributed process.

✳Advantages of Wireless Sensor Networks (WSN):

1. **Low cost**: WSNs consist of small, low-cost sensors that are easy to deploy, making them a cost-effective solution for many applications.
2. **Wireless communication**: WSNs eliminate the need for wired connections, which can be costly and difficult to install. Wireless communication also enables flexible deployment and reconfiguration of the network.
3. **Energy efficiency**: WSNs use low-power devices and protocols to conserve energy, enabling long-term operation without the need for frequent battery replacements.
4. **Scalability**: WSNs can be scaled up or down easily by adding or removing sensors, making them suitable for a range of applications and environments.
5. **Real-time monitoring**: WSNs enable real-time monitoring of physical phenomena in the environment, providing timely information for decision making and control.

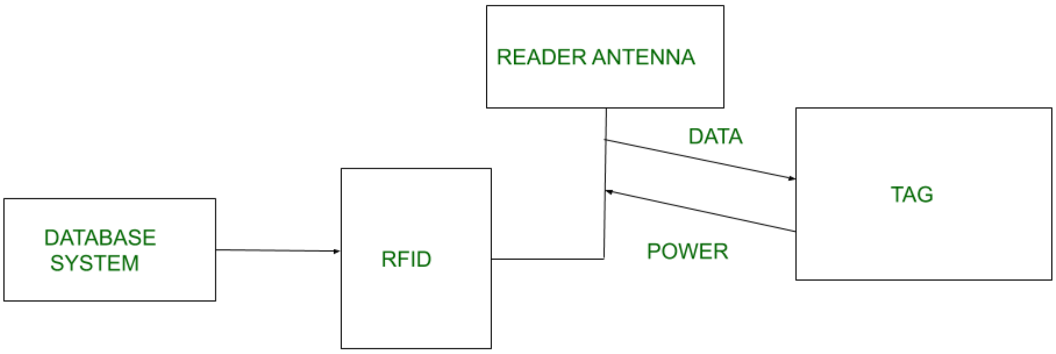
Disadvantages of Wireless Sensor Networks (WSN):

- **Limited range**: The range of wireless communication in WSNs is limited, which can be a challenge for large-scale deployments or in environments with obstacles that obstruct radio signals.
- **Limited processing power**: WSNs use low-power devices, which may have limited processing power and memory, making it difficult to perform complex computations or support advanced applications.
- **Data security**: WSNs are vulnerable to security threats, such as eavesdropping, tampering, and denial of service attacks, which can compromise the confidentiality, integrity, and availability of data.
- **Interference**: Wireless communication in WSNs can be susceptible to interference from other wireless devices or radio signals, which can degrade the quality of data transmission.
- **Deployment challenges**: Deploying WSNs can be challenging due to the need for proper sensor placement, power management, and network configuration, which can require significant time and resources.
- while WSNs offer many benefits, they also have limitations and challenges that must be considered when deploying and using them in real-world applications.

Radio Frequency Identification (RFID):

- Radio Frequency Identification (RFID) is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person.
- It uses radio frequency to search ,identify, track and communicate with items and people.
- it is a method that is used to track or identify an object by radio transmission uses over the web. Data digitally encoded in an RFID tag which might be read by the reader.
- This device work as a tag or label during which data read from tags that are stored in the database through the reader as compared to traditional barcodes and QR codes.

- It is often read outside the road of sight either passive or active RFID.



Kinds of RFID :

UHF RHID (Ultra-High Frequency RFID). It is used on shipping pallets and some driver's licenses. Readers send signals in the 902-928 MHz band. Tags communicate at distances of several meters by changing the way they reflect the reader signals; the reader is able to pick up these reflections. This way of operating is called backscatter.

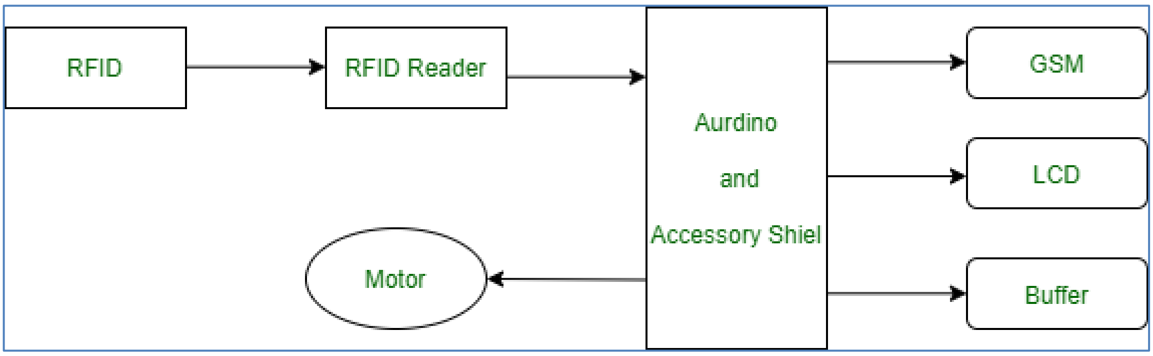
HF RFID (High-Frequency RFID). It operates at 13.56 MHz and is likely to be in your passport, credit cards, books, and noncontact payment systems. HF RFID has a short-range, typically a meter or less because the physical mechanism is based on induction rather than backscatter.

There are also other forms of RFID using other frequencies, such as LF RFID(Low-Frequency RFID), which was developed before HF RFID and used for animal tracking.

Working Principle of RFID :

Generally, RFID uses radio waves to perform AIDC function. AIDC stands for Automatic Identification and Data Capture technology which performs object identification and collection and mapping of the data.

An antenna is an device which converts power into radio waves which are used for communication between reader and tag. RFID readers retrieve the information from RFID tag which detects the tag and reads or writes the data into the tag. It may include one processor, package, storage and transmitter and receiver unit.



Working of RFID System :

Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers — fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

The transponder is in the RFID tag itself. The read range for RFID tags varies based on factors including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers. Tags that have a stronger power source also have a longer read range.

Features of RFID :

- An RFID tag consists of two-part which is an microcircuit and an antenna.
- This tag is covered by protective material which acts as a shield against the outer environment effect.
- This tag may active or passive in which we mainly and widely used passive RFID.

Application of RFID :

- It utilized in tracking shipping containers, trucks and railroad, cars.
- It uses in Asset tracking.
- It utilized in credit-card shaped for access application.
- It uses in Personnel tracking.
- Controlling access to restricted areas.
- It uses ID badging.
- Supply chain management.
- Counterfeit prevention (e.g., in the pharmaceutical industry).

Advantages of RFID :

- It provides data access and real-time information without taking to much time.
- RFID tags follow the instruction and store a large amount of information.
- The RFID system is non-line of sight nature of the technology.
- It improves the Efficiency, traceability of production.
- In RFID hundred of tags read in a short time.

Disadvantages of RFID :

- It takes longer to program RFID Devices.
- RFID intercepted easily even it is Encrypted.
- In an RFID system, there are two or three layers of ordinary household foil to dam the radio wave.
- There is privacy concern about RFID devices anybody can access information about anything.
- Active RFID can costlier due to battery.

NFC

- NFC stands for Near Field Communication.
- It enables short range communication between compatible devices.
- At least one transmitting device and another receiving device is needed to transmit the signal.
- Many devices can use the NFC standard and are considered either passive or active.

NFC devices can be classified into 2 types:

Passive NFC devices –

These include tags, and other small transmitters which can send information to other NFC devices without the need for a power source of their own. These devices don't really process any information sent from other sources, and can not connect to other passive components. These often take the form of interactive signs on walls or advertisements.

Active NFC devices –

These devices are able to both the things i.e. send and receive data. They can communicate with each other as well as with passive devices. Smartphones the best example of active NFC device. Card readers in public transport and touch payment terminals are also good examples of the technology.

How does NFC work?

Like other wireless signals Bluetooth and WiFi, NFC works on the principle of sending information over radio waves. Near Field Communication is another standard for wireless data transition which means devices must adhere to certain specifications in order to communicate with each other properly. The technology used in NFC is based on older technology which is the RFID (Radio-frequency identification) that used electromagnetic induction in order to transmit information.

This creates one major difference between NFC and Bluetooth/WiFi. NFC can be used to induce electric currents within passive components rather than just send data. This means that their own power supply is not required by passive devices. Instead they can be powered by the electromagnetic field produced by an active NFC component when it comes into range. NFC technology unfortunately does not command enough inductance to charge our smartphones, but QI charging is based on the same principle.

The transmission frequency is 13.56 megahertz for data across NFC. Data can be sent at either 106, 212, or 424 kilobits per second which is quick enough for a range of data transfers like contact details to swapping pictures and music.

The NFC standard currently has three distinct modes of operation to determine what sort of information will be exchanged between devices.

- The most common used in smartphones is the peer-to-peer mode. Exchange of various piece of information is allowed between 2 devices. In this mode both devices switch between active when sending data and passive when receiving.
- The second mode i.e. read/write mode is a one-way data transmission. The active device, possibly your smartphone, links up with another device in order to read information from it. NFC advertisement tags use this mode.
- The third mode of operation is card emulation. The NFC device can function as a smart or contactless credit card and make payments or tap into public transport systems.

Benefits of NFC

NFC has several real-world benefits, including the following:

- increases operational efficiency for payment processors;
- ensures more security than traditional credit cards for payments;
- allows users to choose from multiple cards dynamically;
- difficult to intercept NFC communications from a distance;
- ease of use for consumers in paying for goods

Limitations of NFC

- Challenges of NFC technology include the following:
- very short range of only a few inches precludes many use cases;
- slower than other protocols;
- can limit usability for apps that require sensitive data on a smartphone;
- app innovation stymied by Apple and Google restrictions and tech implementations;
- not suitable for location tracking;