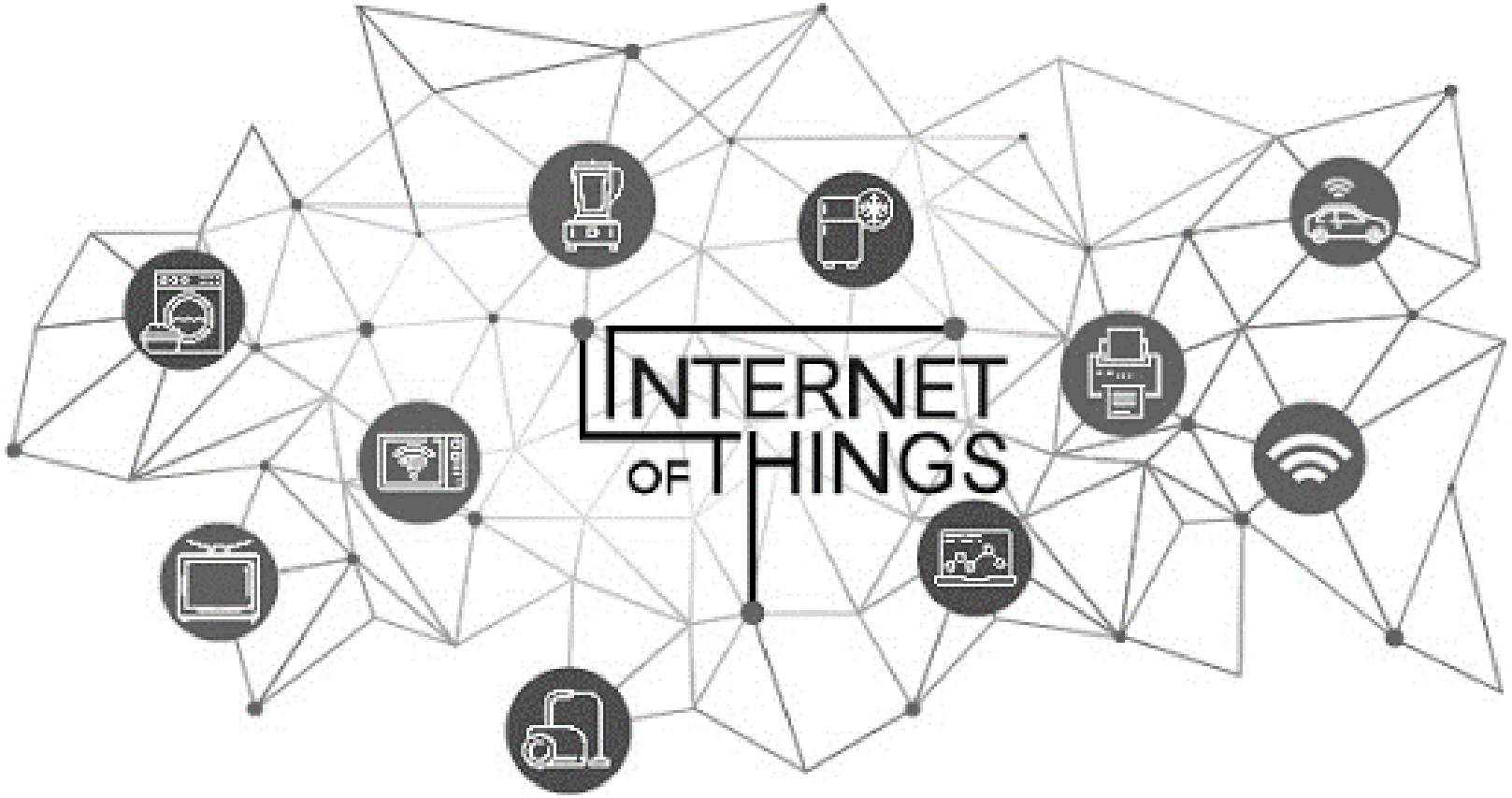
Unit-1

Introduction to Internet of Things

Introduction to Internet of Things (IoT)

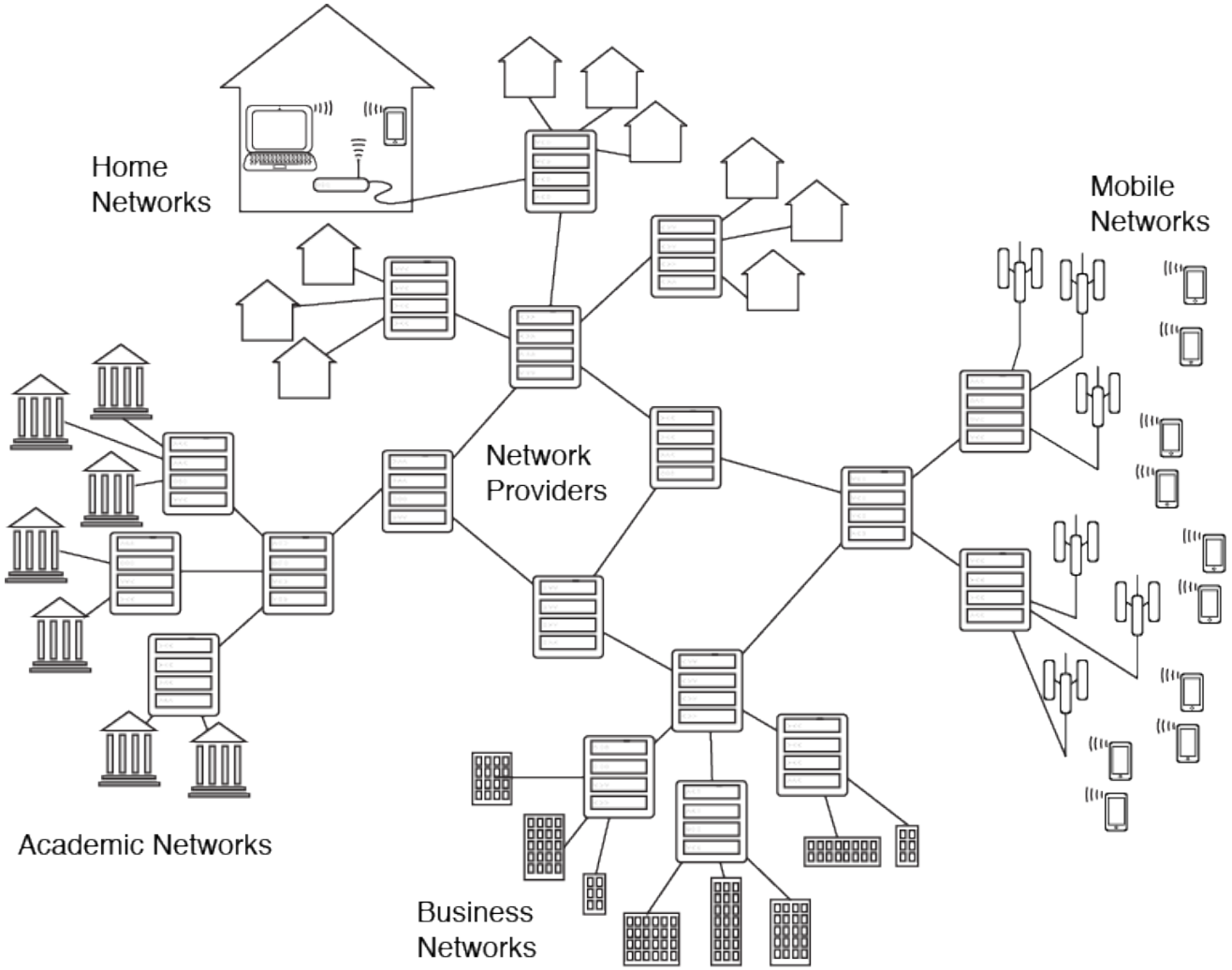
- First of all we should discuss about the name “IoT – Internet of Things” in detail.



- So we have to discuss about the first word “Internet” and then everything about the “Things”.

Introduction to Internet of Things (IoT)

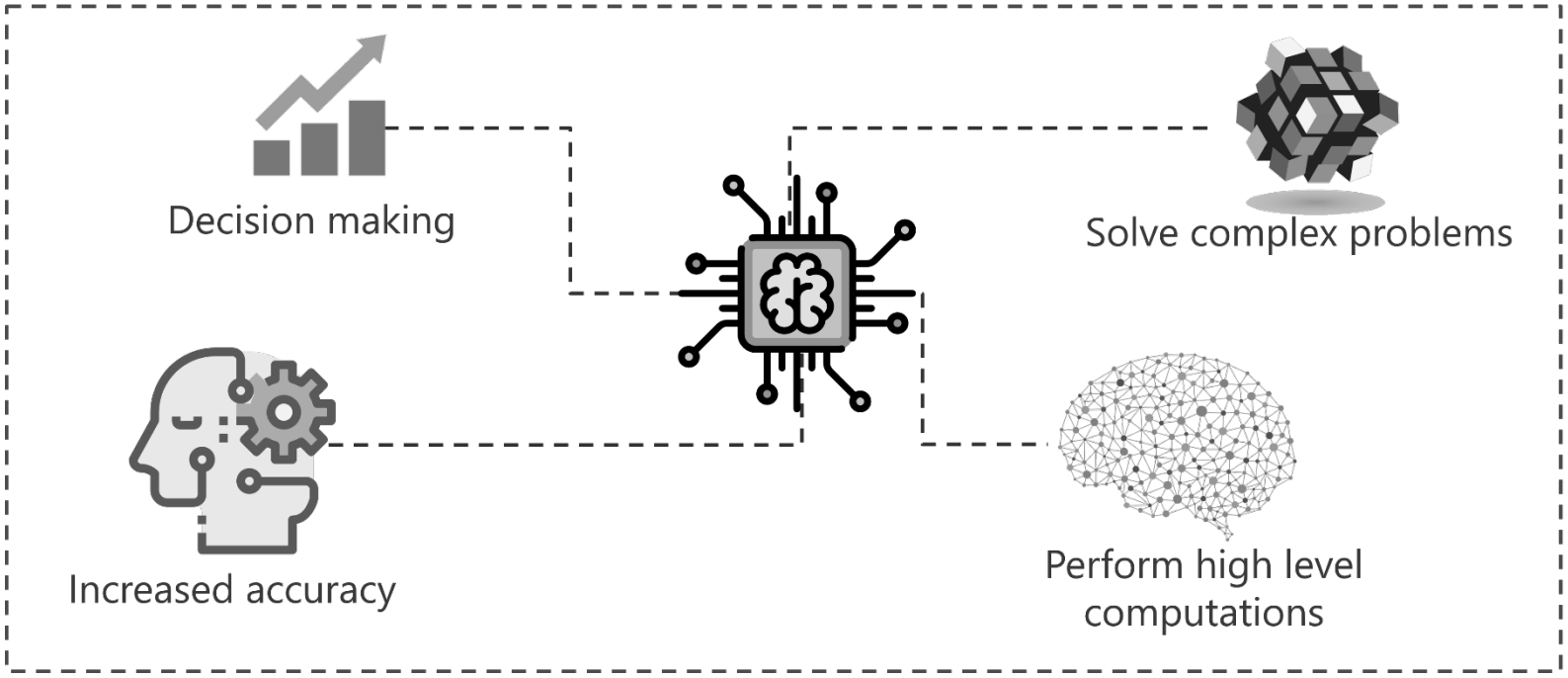
- What is Internet?



- In simple word, it's a Network of Networks or Interconnected LANs.
- So here we have to discuss about the Network, and we already learned everything about network in the last semester, Right?
- What is Network?, Requirement for networking

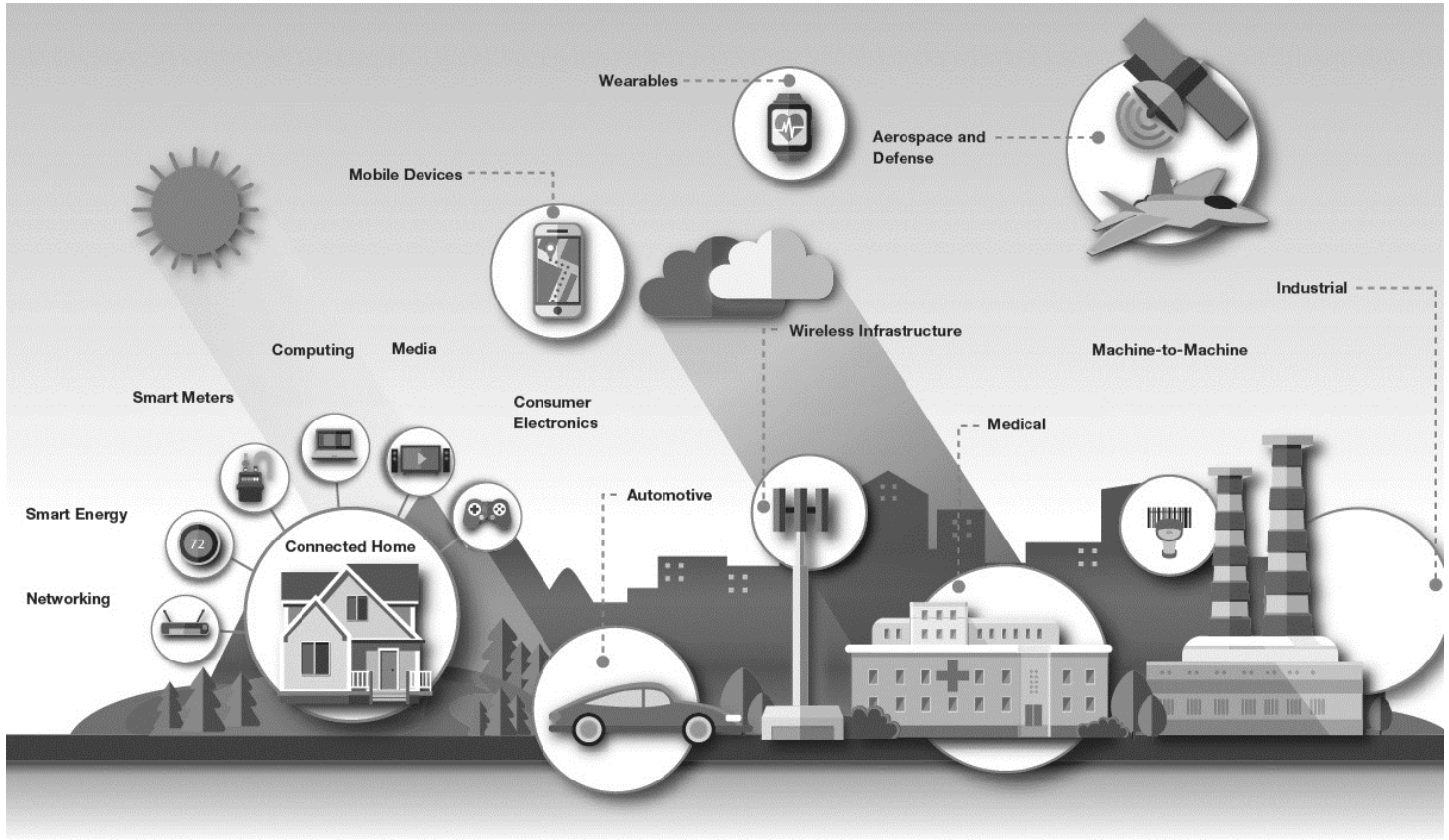
Introduction to Internet of Things (IoT)

- Nowadays The term Internet of Things (IoT) is an emerged the popular terms.
- There are multiple ways to define IoT, but the basic of all the definitions remains the same.
- IoT is network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data.
- The IoT is not just limited to the connected or networked devices, but in a broad way IoT devices exchange meaningful information from one device to another to get desire result.



Introduction to Internet of Things (IoT)

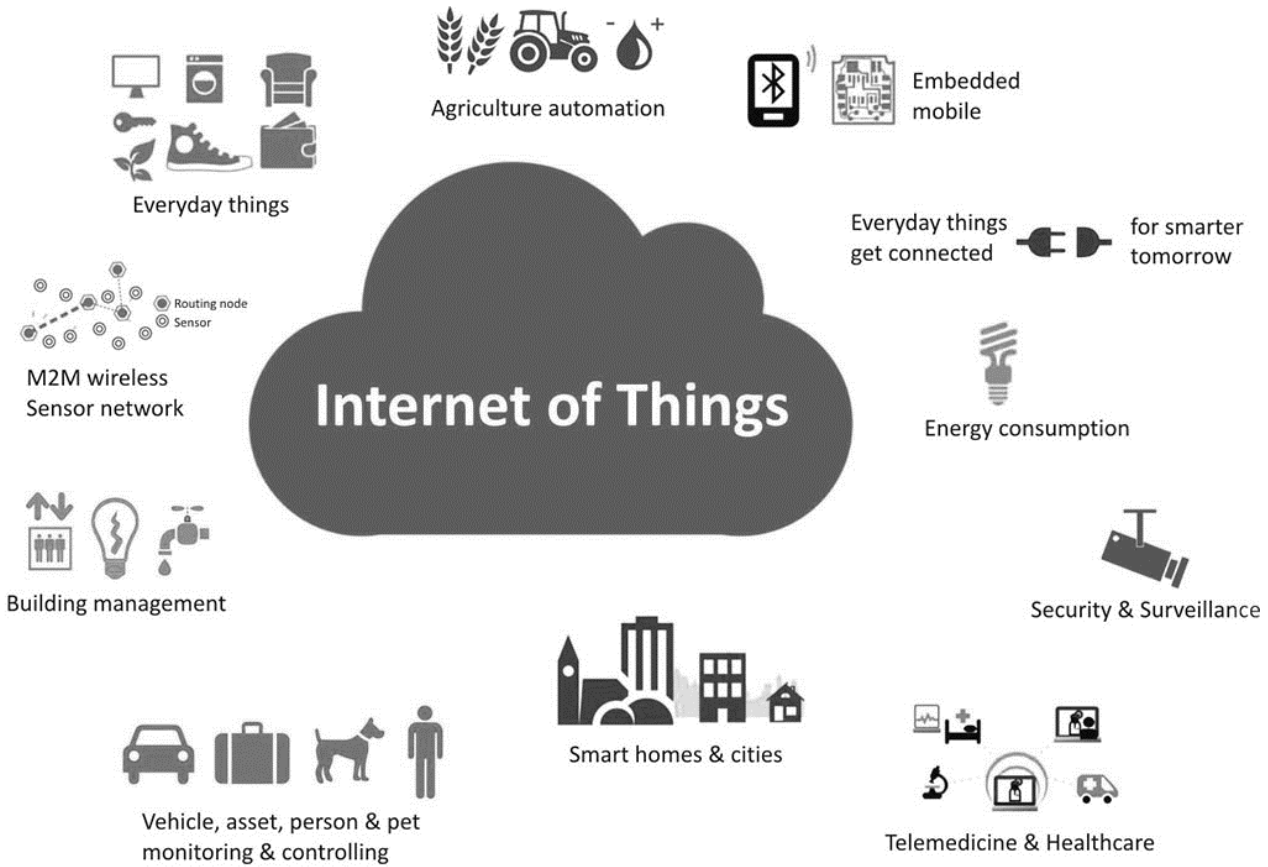
- IoT is not a single technology, it's a combination of technologies and domain knowledge.
- As a result, engineers from different domains have to work together for building a complete IoT product.



- Life would be governed entirely by Internet and IoT in the near future.

Application areas of IoT

- The scope and application areas of IoT is very huge.
- IoT can be used to build applications for…

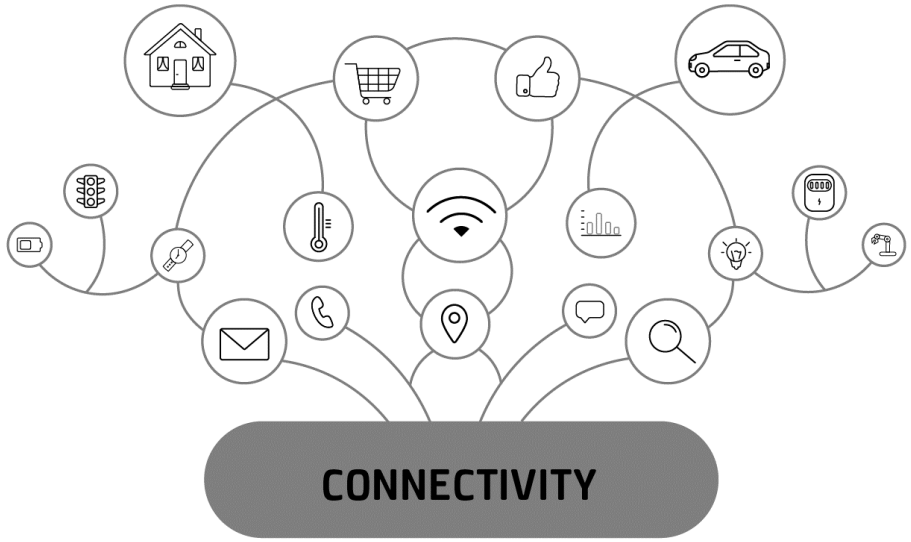


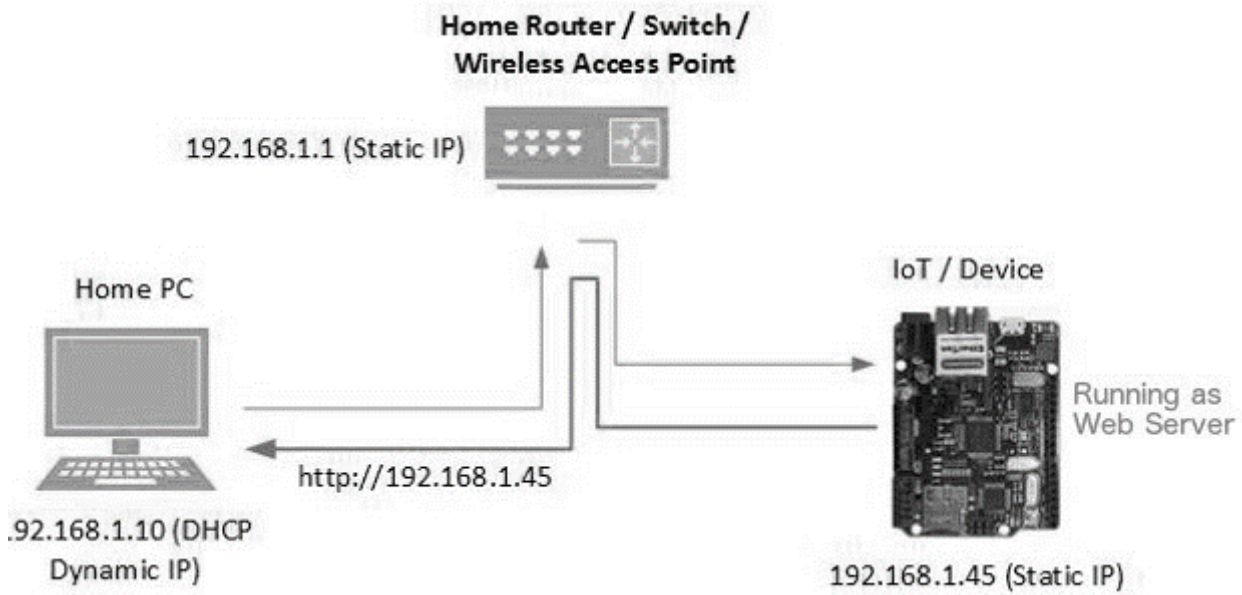
- Agriculture
- Assets Tracking
- Energy Sector
- Defense
- Embedded Applications
- Education
- Waste Management
- Healthcare Products
- Telemedicine
- Safety And Security Sector
- Smart City Applications etc.

Characteristics of IoT

Connectivity:

- Connectivity is an important and first requirement of IoT infrastructure.
- Every Things in IoT should be connected to the IoT infrastructure.
- Connectivity should be guaranteed at anywhere and anytime.





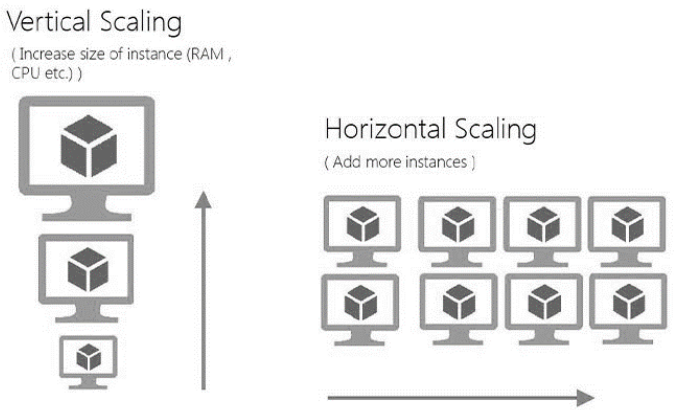
Identity:

- Each IoT device has a unique identity (e.g., an IP address).
- This identity is helpful in communication, tracking and to know status of the things.

Characteristics of IoT

Intelligence:

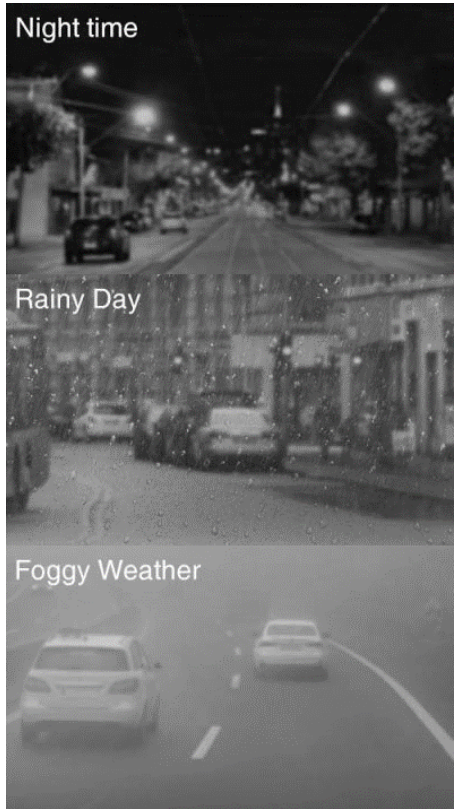
- Just data collection is not enough in IoT, extraction of knowledge from the generated data is very important.
- For example, sensors generate data, but that data will only be useful if it is interpreted properly.
- So intelligence is one of the key characteristics in IoT.



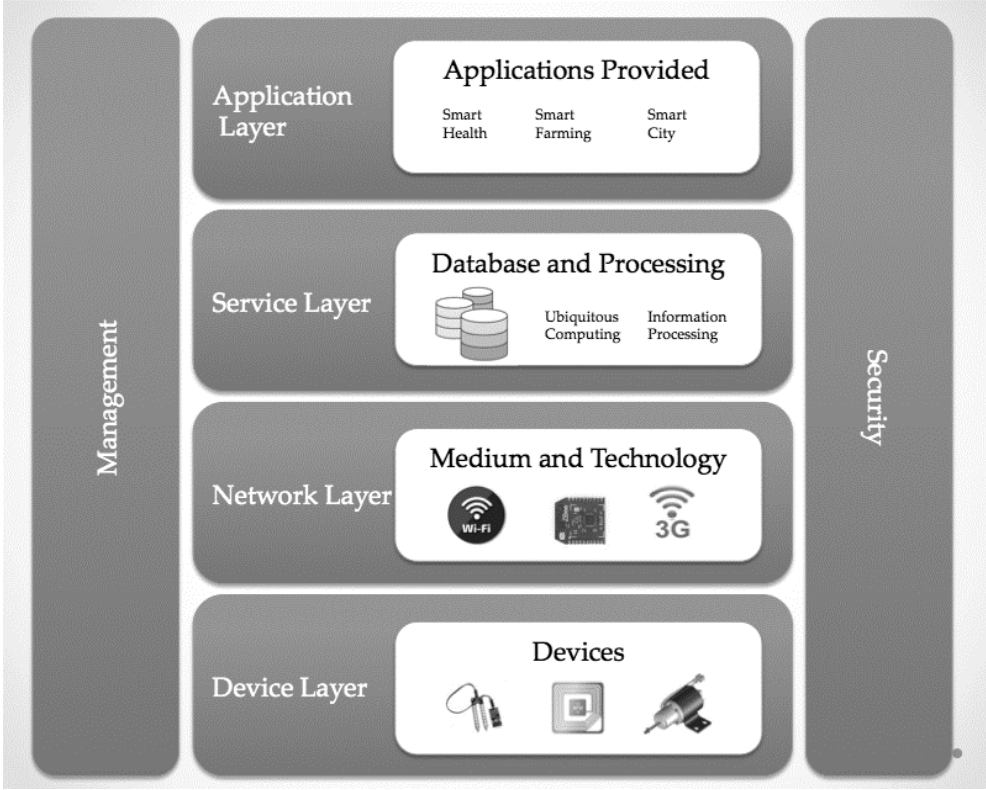
Scalability:

- The number of elements (devices) connected to IoT zone is increasing day by day.
- Therefore, an IoT setup should be capable of handling the expansion.
- It can be either expand capability in terms of processing power, Storage, etc as vertical scaling or horizontal scaling by multiplying with easy cloning

Characteristics of IoT



- **Dynamic and self-adapting (complexity):**
  - IoT devices should dynamically adapt themselves to the changing surroundings.
  - For example surveillance camera. It should be flexible to work in different weather conditions and different light situations (morning, afternoon, or night).
- **Architecture:**
  - IoT architecture is yet not uniformed and standardized.
  - It should be hybrid, supporting different manufacturer's products to function in the IoT network.



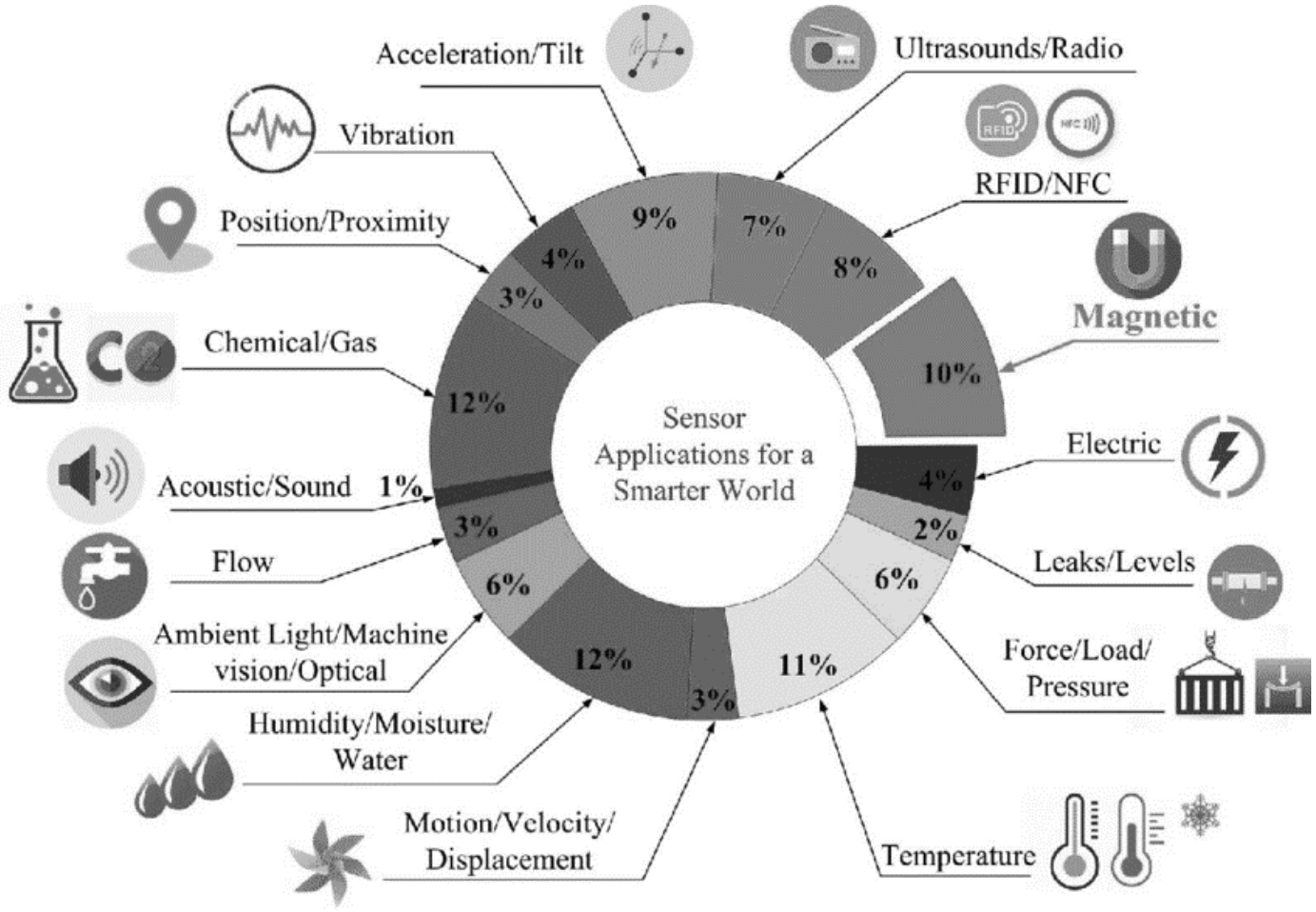
Characteristics of IoT

- **Safety:**
  - Sensitive personal details of a user might be compromised when the devices are connected to the Internet.
  - So data security is a major challenge.
  - This could cause a loss to the user.
  - Equipment in the huge IoT network may also be at risk.
  - Therefore, equipment safety is also critical.

Things in IoT

- In the IoT, things refer to a variety of devices. It can be anything even humans in it become a thing.
- For something to qualify as a “thing”, it requires identity of its existence.
- The “thing” in a network can be monitored/measure. For example, a temperature sensor could be a thing.
- Things are capable of exchanging data with other connected devices in the system.
- The data could be stored in a centralized server (or cloud), processed there and a control action could be initiated.
- The devices having all the above characteristics are known as things.

Things in IoT



- Some of the famous “things” are temperature sensors, pressure sensors, humidity sensors, etc.
- The data from these sensors are collected and sent it to the cloud or stored it in local server for data analysis.
- Based on the data analysis, the control action would be taken.
- For example, switching off the water heater remotely when the water is heated as per requirement.

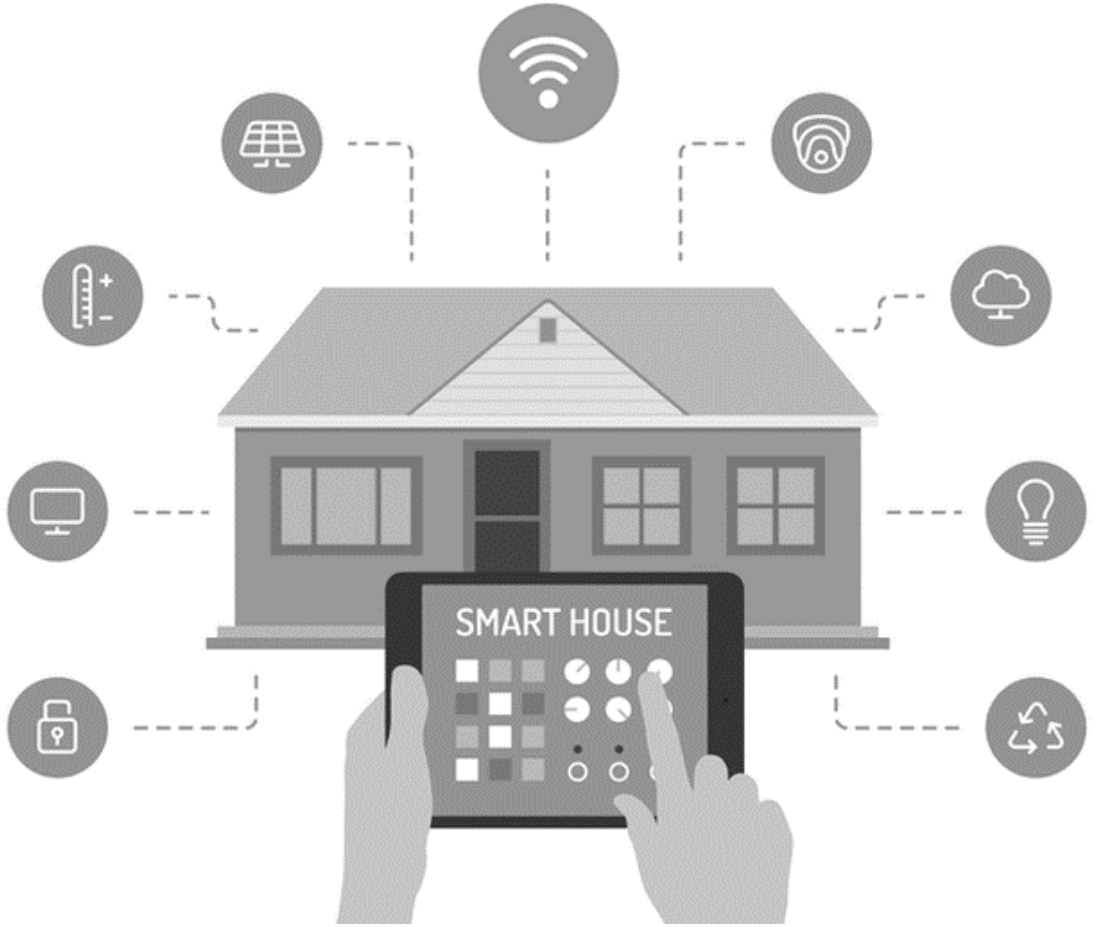
Things in IoT

- Not just sensors, the following can also be called as things:

- Industrial motors
- Wearables (e.g., watch)
- Vehicles
- Shoes
- Heart monitoring implants (e.g., pacemaker, ECG real-time tracking)
- Biochip transponders (for animals in farms)
- Automobiles with built-in sensors (automobile feature real-time monitoring)
- Food/perishables quality measuring

Things in IoT

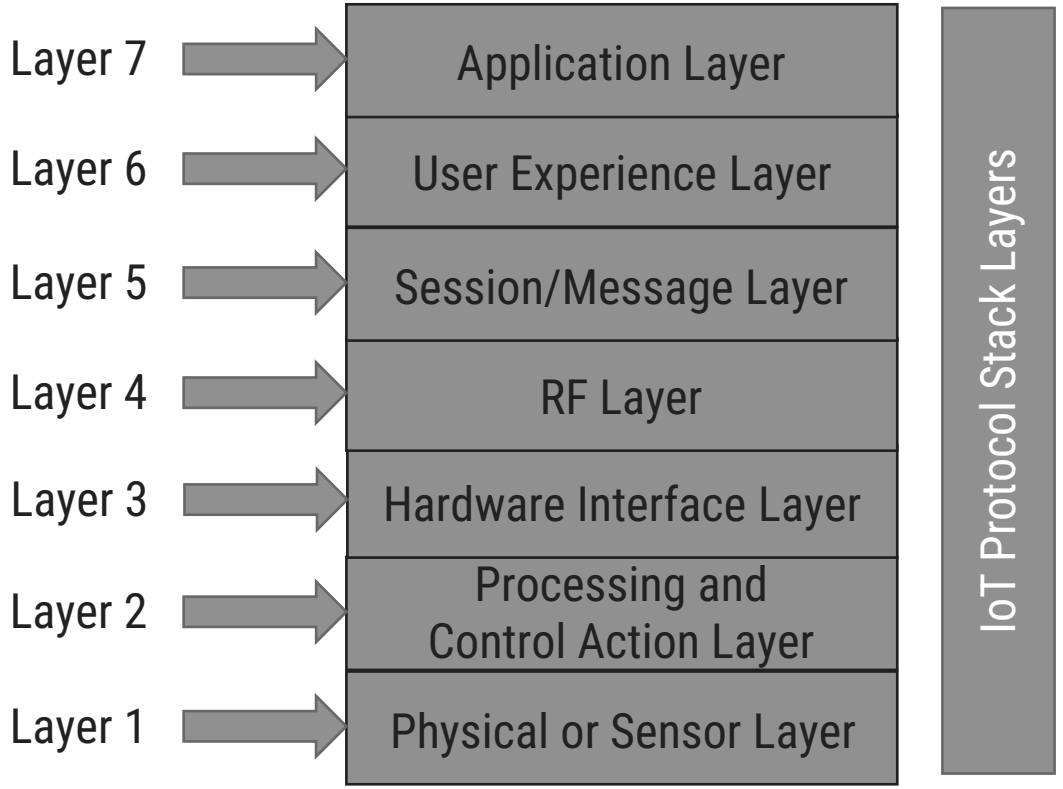
- In IoT-based home automation, the “things” could be the following
  - Lighting control and automation devices
  - Ventilation devices
  - Air conditioning [heating, ventilation and air conditioning (HVAC)] systems
  - Appliances such as washer/dryer
  - Air purifiers
  - Ovens or refrigerators/freezers that use Wi-Fi for remote monitoring
  - Security cameras
  - Smart phones



IoT Stack

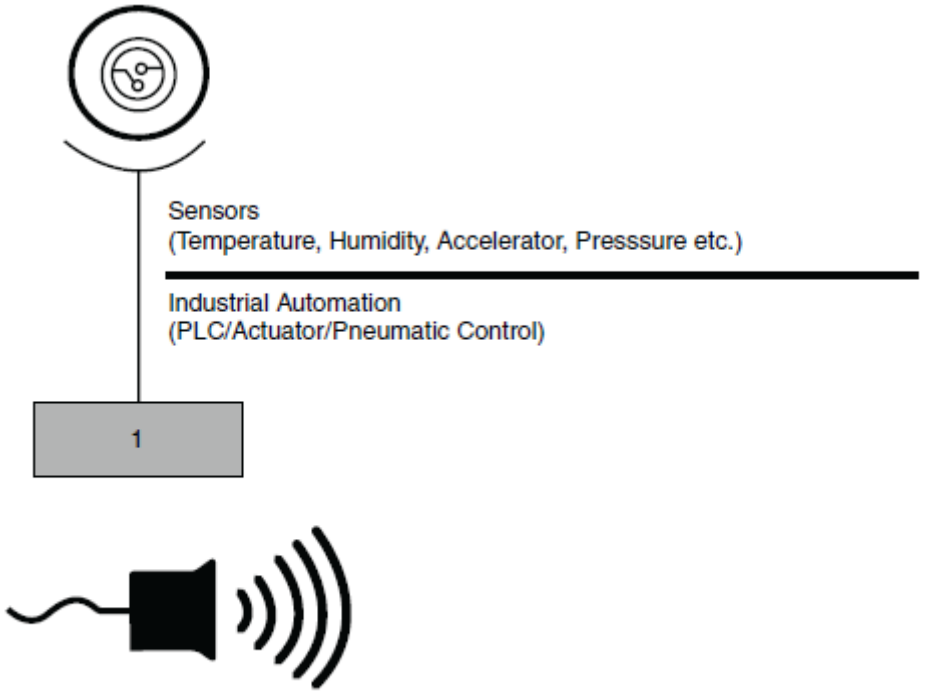
- Like other digital technology IoT has stack layers.

- Following are the identified seven layers in IoT stack.
  - Layer 1 (Physical or Sensor Layer)
  - Layer 2 (Processing and Control Action layer)
  - Layer 3 (Hardware Interface Layer)
  - Layer 4 (RF Layer)
  - Layer 5 (Session/Message Layer)
  - Layer 6 (User Experience Layer)
  - Layer 7 (Application Layer)



IoT Stack - Layer 1 (Physical or Sensor Layer)

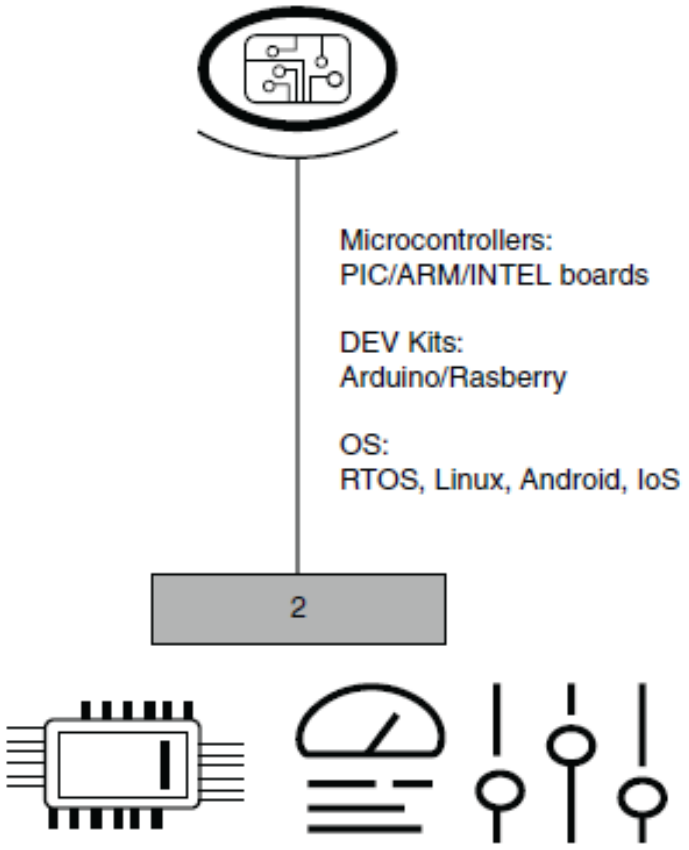
- This layer is concerned about the physical components, which mainly includes sensors.
- In this layer, the sensors are the core component.
- Temperature sensor, pressure sensor, humidity sensor, etc. can all be referred as physical layer components.
- In industrial automation, PLC, actuator, etc. are considered as physical layer components.
- This layer is responsible for data collection and action execution.
- Selection of sensors is important and choosing an appropriate sensor is the challenge in this layer.
- Action execution, sensing and data collection happens here.



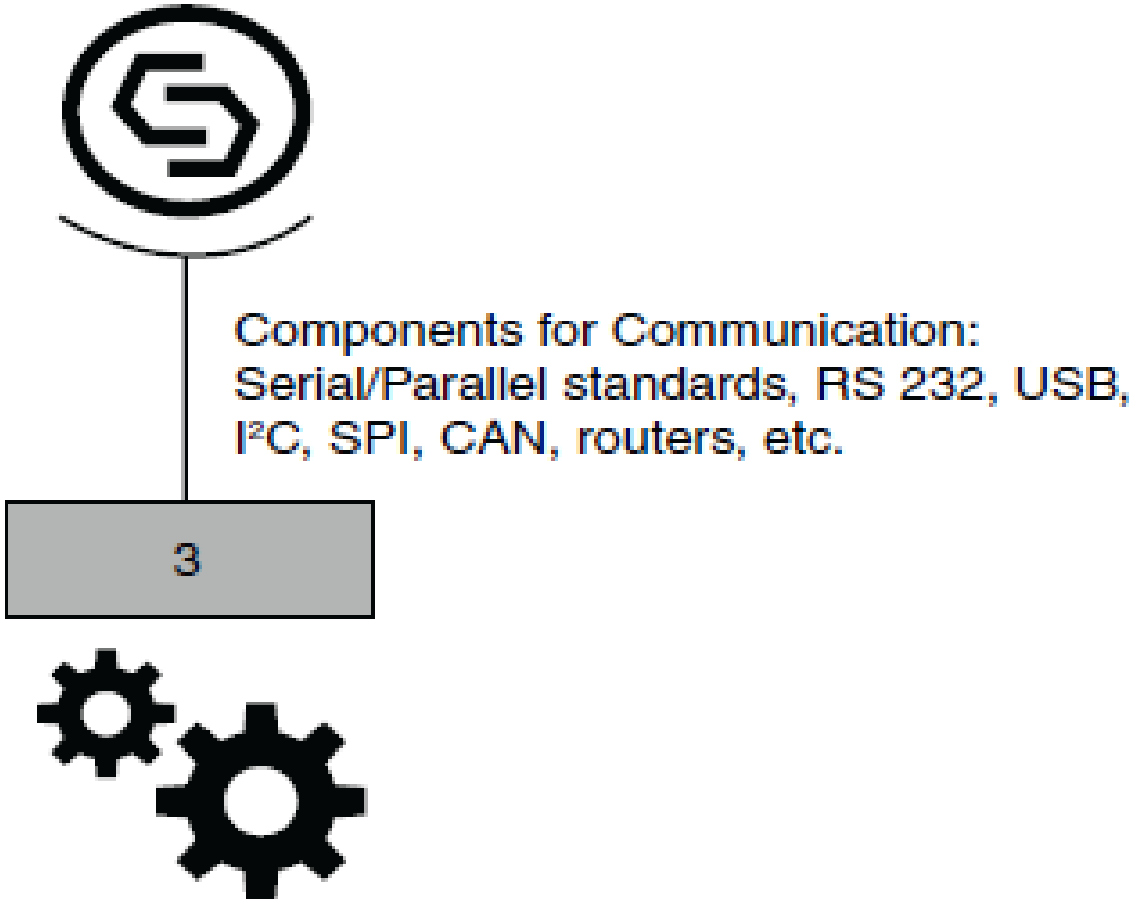
Layer 1: Sensor layer (physical layer); data collection happens here.

IoT Stack - Layer 2 (Processing and Control Action Layer)

- This important layer contains core components of IoT system.
- The microcontrollers or processors are found in this layer.
- The data is received by the microcontrollers from the sensors.
- A variety of development kits are available in the market; like Arduino, Raspberry Pi, Node MCU, PIC, ARM development boards, etc.
- Microcontroller/Processor and operating system play vital role at this layer
- Data collected from the sensors is processed in this layer.

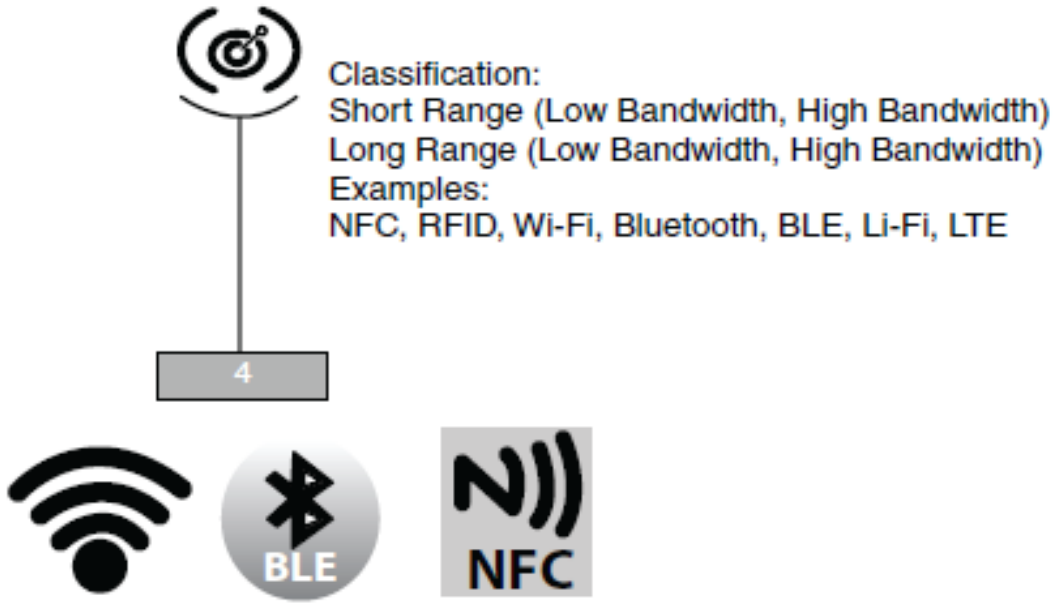


IoT Stack - Layer 3 (Hardware Interface Layer)



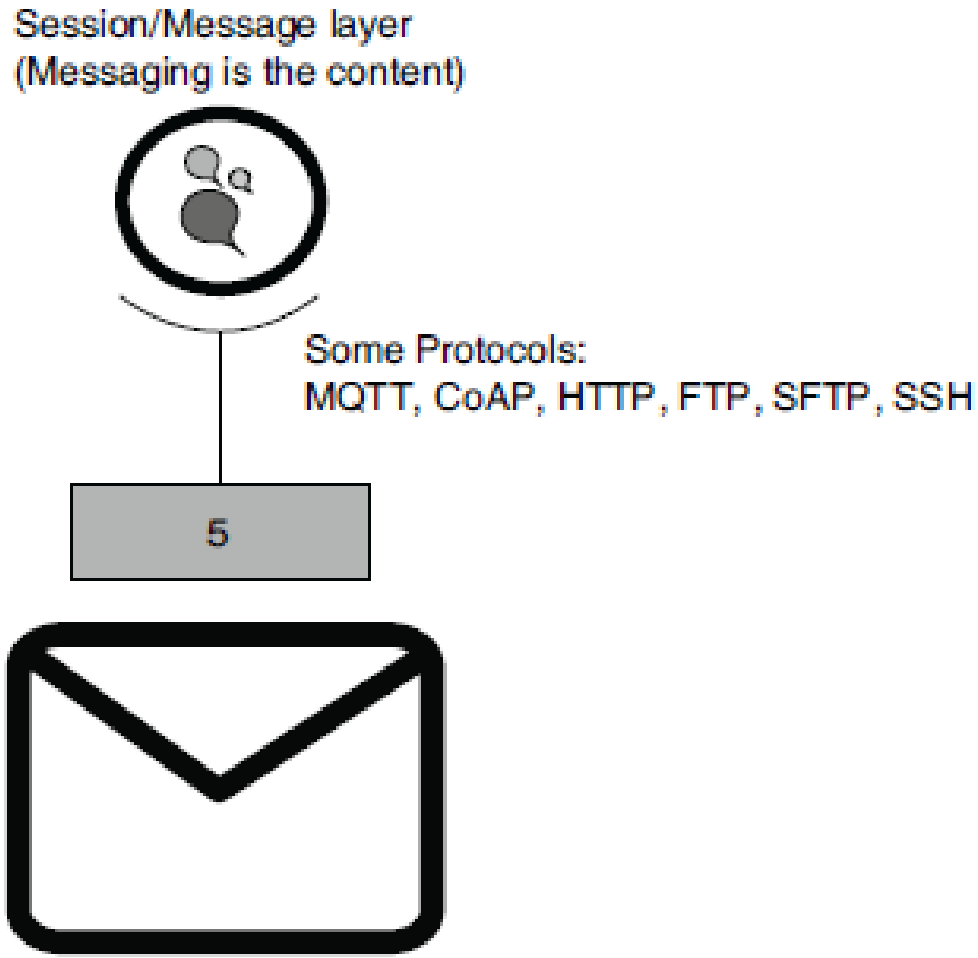
- The 3rd layer in the stack is the Hardware Interface Layer.
- Hardware components and communication standards such as RS232, CAN, SPI, SCI, I 2C, etc. occupy this layer.
- All these components ensure flawless communication
- Handshake happens here.

IoT Stack - Layer 4 (RF Layer)



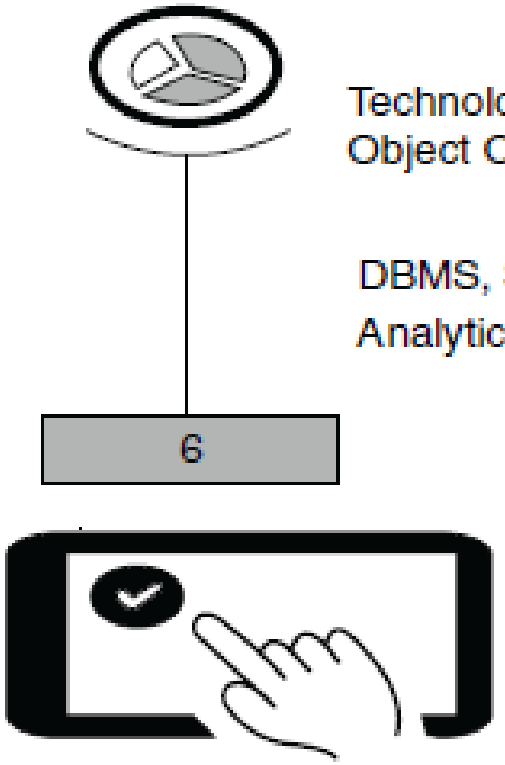
- Whenever one talks about IoT, RF is discussed and comes in picture.
- It plays a major role in the communication channel – whether it is short range or long range.
- Protocols used for communication and transport of data based on RF are listed in this layer.
- Some famous and common protocols are Wi-Fi, NFC, RFID, Bluetooth, Zigbee, etc.
- RF layer does communication of data using radio frequency based Electromagnetic (EM) waves
- This layer can also include Li-Fi; which are effective alternates for RF protocols.

IoT Stack - Layer 5 (Session/Message Layer)



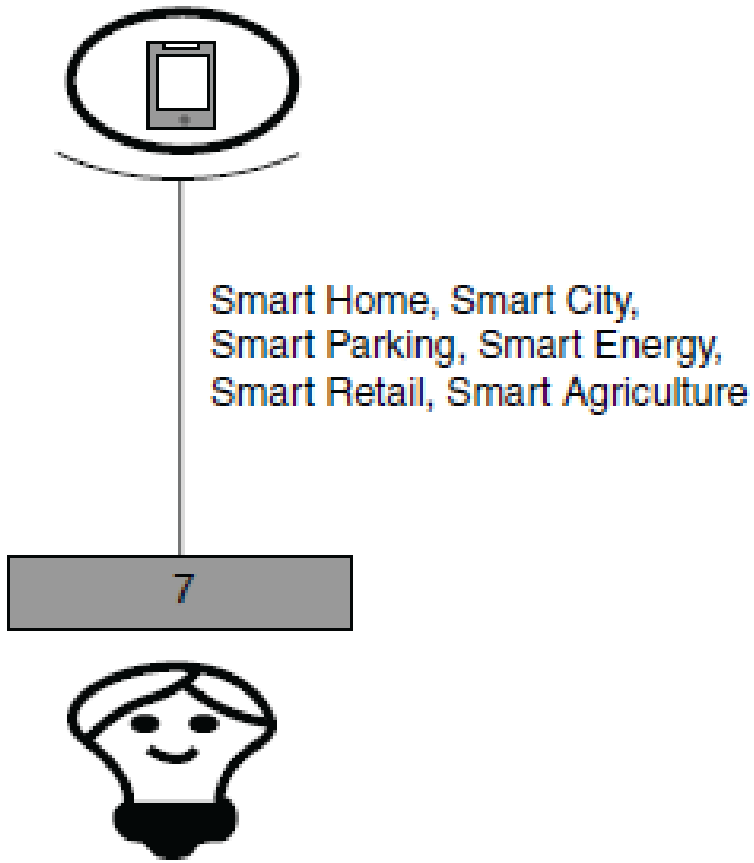
- Like computer network session management is also important in IoT.
- There are many protocols which manage how messages or data are broadcasted to the cloud.
- Layer 5 (session layer) deals with the various messaging protocols as MQTT, CoAP, etc. and also other protocols such as SSH and FTP.

IoT Stack - Layer 6 (User Experience Layer)



- This layer deals with providing best experience to the end users of IoT products.
- The 6th layer takes care of rich UI designs with lots of features, which provide a pleasing experience while using the service/system or product.
- Object-oriented programming languages, scripting languages, analytics tools, etc. all should be included in this layer.
- This is also known as User Experience and Visualization Layer.

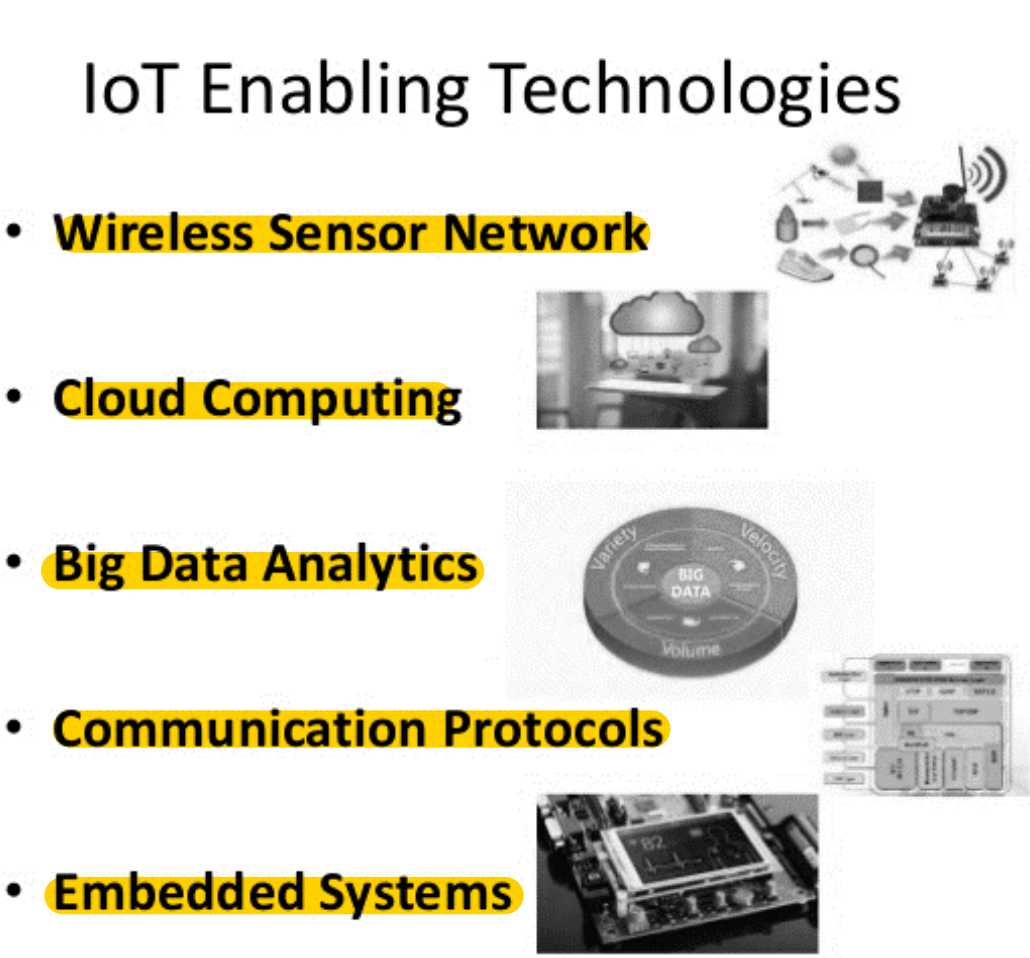
IoT Stack - Layer 7 (Application Layer)



- Everything comes to perfection at this layer.
- This layer utilizes the rest six layers in order to develop desired application.
- It can range from a simple automation application to smart city application.
- After learning about the layers, it is now easier to relate them with an application, for example, vegetable quality monitoring during transport from source to the destination using IoT.

Enabling Technologies

- IoT is a collection or group of many technologies and devices.
- The simplest of sensors, embedded systems, data analytics, communication protocols, security aspects and cloud computing with storage have all become enabling technologies.
- Enabling technologies/devices fall under one of the following categories:
  - Technologies that help in acquiring/sensing data.
  - Technologies that help in analyzing/processing data.
  - Technologies that help in taking control action.
  - Technologies that help in enhancing security/privacy.
- Let's discuss some of the enabling technologies.



Enabling Technologies - Sensors

Temperature Sensor
Precision ±0.3℃
Range - 40 to 85℃
- 40 to 185°F

Humidity Sensor
Precision ±3%RH
Range 0 to 100%

Ambient Light Sensor
Precision ±3%
Rang 0.01 to 83K lux

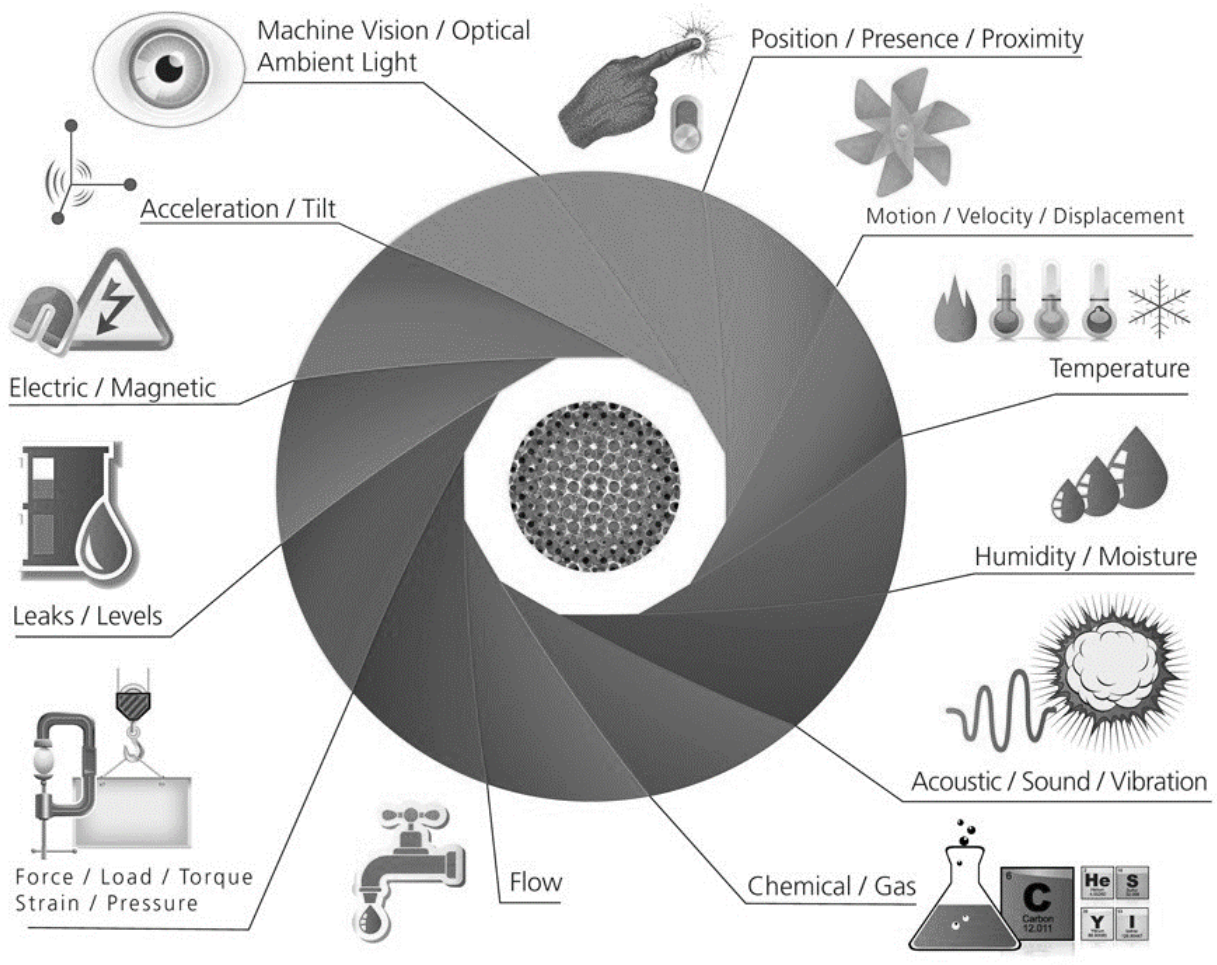
Vibration Index Sensor
Precisio 4mg
Range - 16 to 16g

External Temperature Sensor
Precision ±0.5℃
Range - 55 to 125℃
- 67 to 257°F

- Sensors are at the heart of any IoT application.
- As the name suggests, they sense the environment and retrieve data.
- Sensors are the starting point of any IoT application.
- It fetches data for us to operate on.
- Sensors could be analog or digital.
- Temperature sensor in a thermometer is an example of it. It is used to build temperature monitoring application.

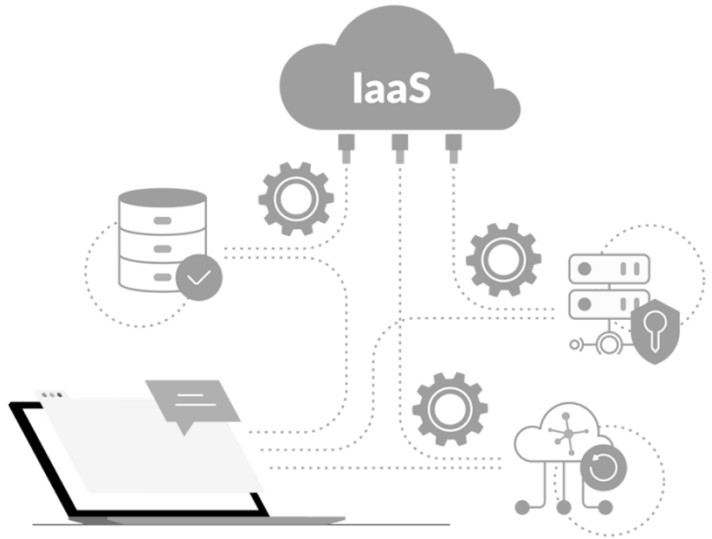
Enabling Technologies - Sensors

- Some examples of sensors that could be regarded as enabling technologies are as follows.
  - Weather tracking system uses temperature/humidity/moisture sensors.
  - Vehicle health monitoring sensors keep track of speed, tyre pressure, etc.
  - On Board Diagnostics (OBDs) used for collecting all critical information from an automobile to detect error.
  - Vibration sensors are used to track the quality of buildings/structures.
  - Water quality is monitored through sensors that measure PH, chloride level, etc.
  - PIR sensor is used in pedestrian signal operation with human presence detection.



Enabling Technologies - Cloud Computing

- The next technology that is highly significant in IoT is cloud computing.
- Cloud has grown much more popular because it serves as an affordable, effective and efficient medium for data storage.
- Data storage plays a major role in IoT.
- Cloud services are categorized as follows:
  - IaaS (Infrastructure-as-a-Service):
    - In this cloud service, one can choose virtual machines over physical machines.
    - It is a form of cloud computing that provides virtualized computing resources over the Internet.
    - The users manage the machines, select the OS and underlying applications, and pay per their use.



Enabling Technologies - Cloud Computing

- **PaaS (Platform-as-a-Service):**
  - This is a cloud computing model in which the cloud service provider delivers hardware and software tools needed for application development to users over the Internet.
  - A PaaS provider hosts the hardware and software on its own infrastructure. Users have to build, manage and maintain the applications as per their requirement.

- **SaaS (Software-as-a-Service):**
  - In this model, a complete software application is provided to the user.
  - It can also be called application as a service. This service can be availed by paying a monthly, yearly, etc., subscription.
  - Some well-known service providers in the market are Amazon web services, Azure and Adafruit.

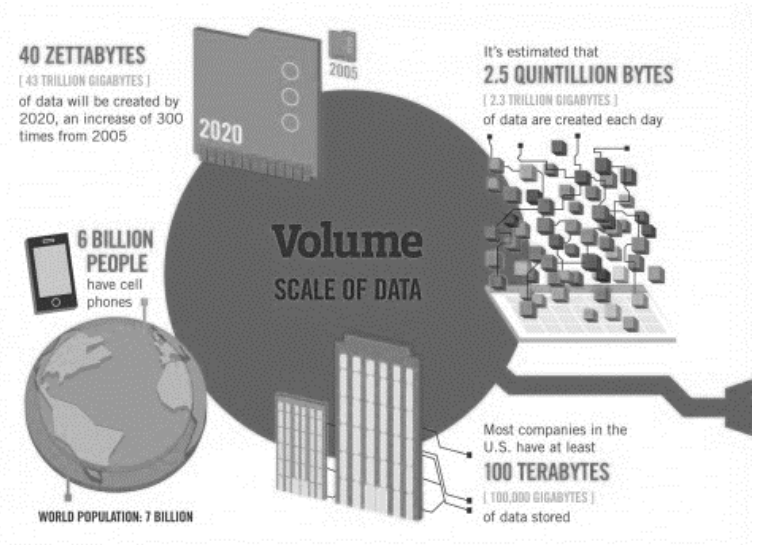
Enabling Technologies - Big Data Analytics

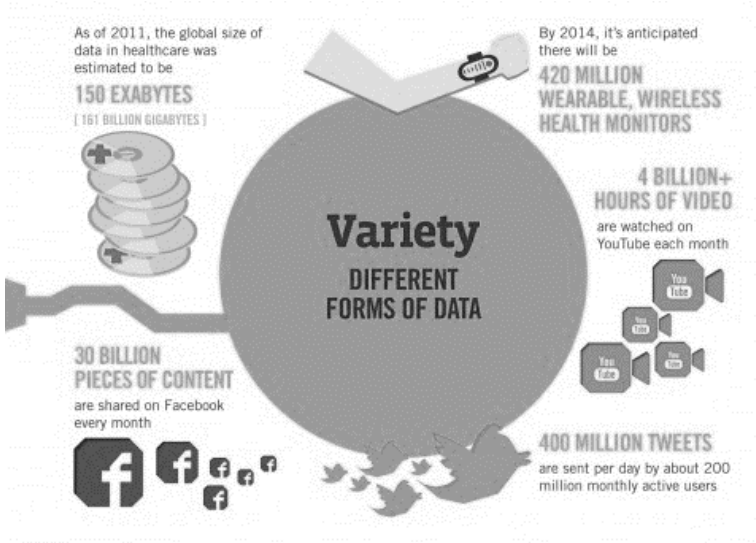
- Data is everywhere, and from every function or operation we get more data.
- IoT is all about collecting data from various sensory nodes.
- Handling the huge data is fundamental to make the application a success.
- The biggest challenge with big data is 4Vs. Volume, Variety, Speed (Velocity) at which it comes and its Veracity.

Enabling Technologies - Big Data Analytics

Scale (Volume):

- Huge volume of data is generated every minute.
- Storage has become inexpensive and hence, cost-related challenges have reduced.
- Cloud storage and hardware storage both have become affordable because of the tremendous growth in the semiconductor industry.





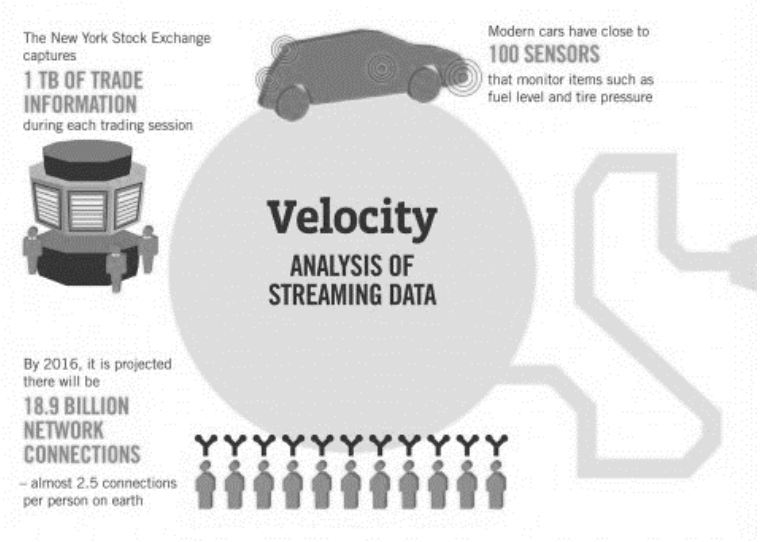
Complexity (Variety):

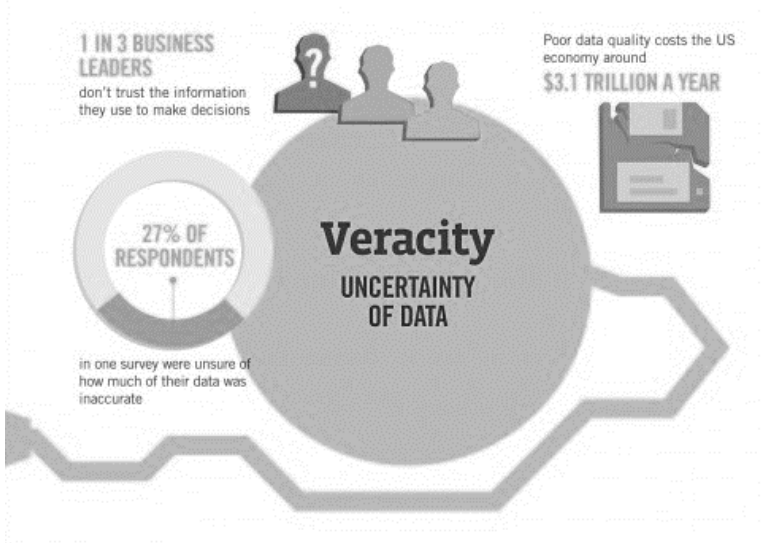
- Data no longer comes from one single source.
- It also comes in different formats (e.g., audio, video, text and image) and has to be interpreted systematically.
- Varieties of data becomes a huge challenge.

Enabling Technologies - Big Data Analytics

Speed (Velocity):

- The rate at which data is generated very fast.
- Also, data dynamics changes very frequently.
- Nowadays, data comes from anywhere – from fit bit watches to refrigerators.
- All the data pours in at a very high speed, which makes it very challenging.



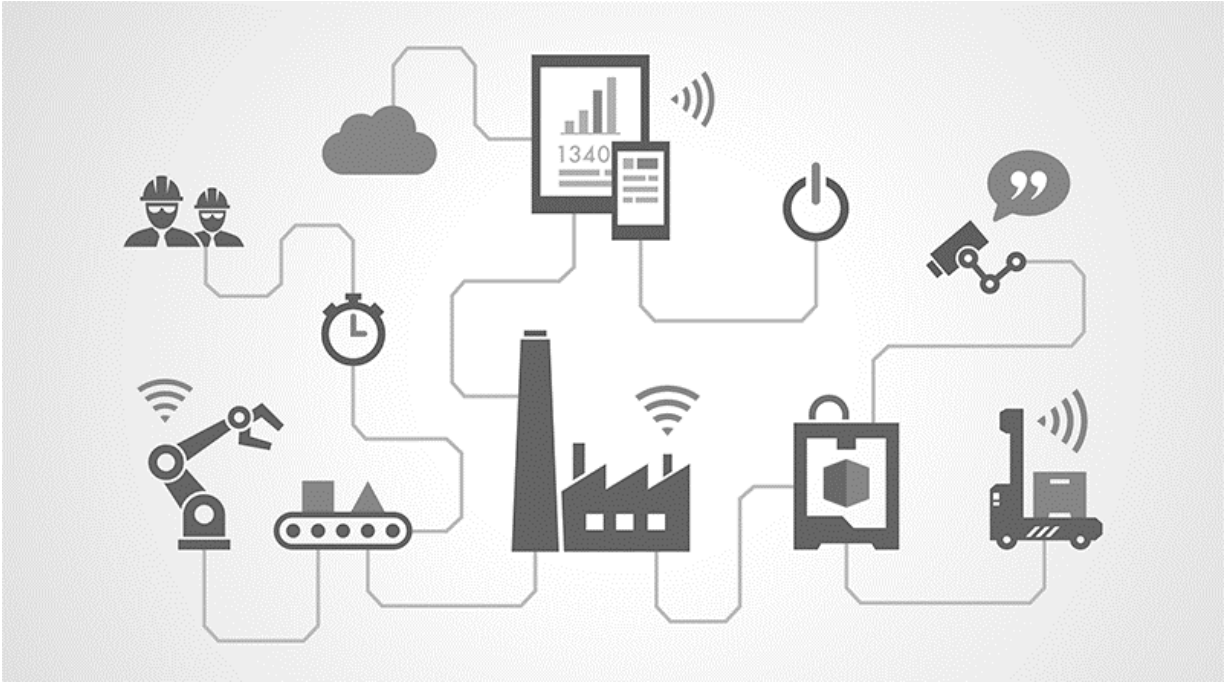


Data in doubt (Veracity):

- How accurate is all this data anyway?
- Because we are now rely on it
- The data's nature alters dynamically and uncertainty is often seen.
- So, it would be challenging to process this unstable data.

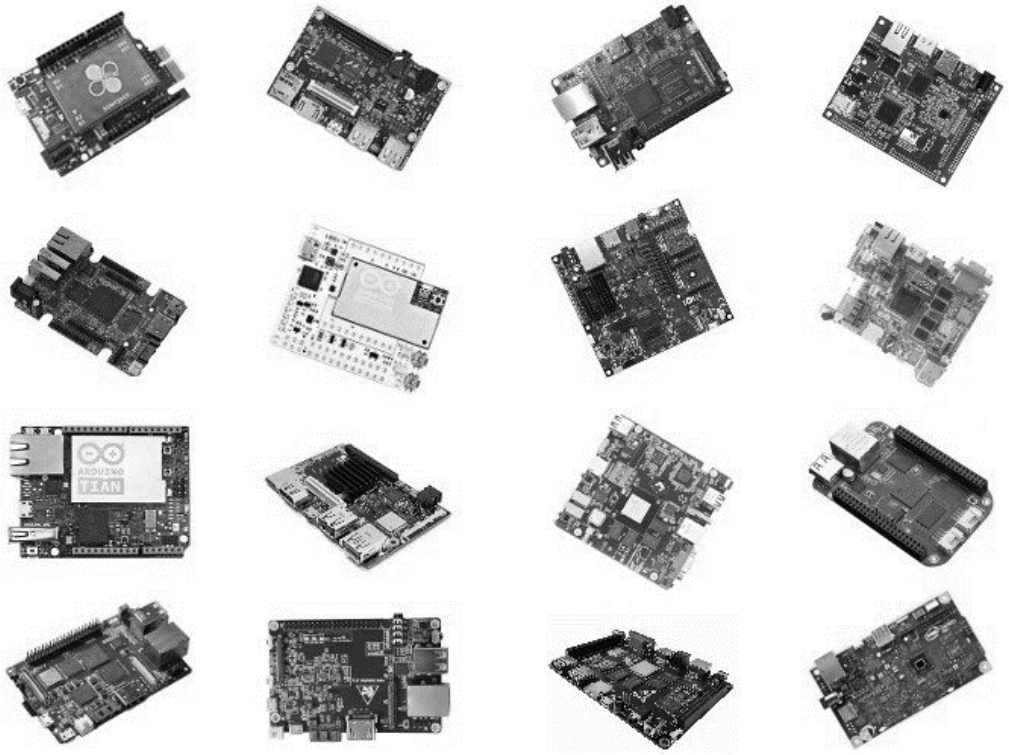
Enabling Technologies - Big Data Analytics

- So the question is: “Who is generating all this data?” A partial list to answer this is as follows:
  - Sensors from security systems.
  - Sensors from weather monitoring systems.
  - Sensors from car/navigation systems.
  - Sensors from water quality monitoring systems.
  - Data from wearables (e.g., bands).
  - Data from industrial equipment (e.g., motor health).
  - Sensors from bridges/roads about traffic density and other factors.
  - Social media (e.g., tweets, photo uploads, etc.).
- In IoT data is everything. so, data analytics is one of the enabling technologies for building a complete and IoT application.



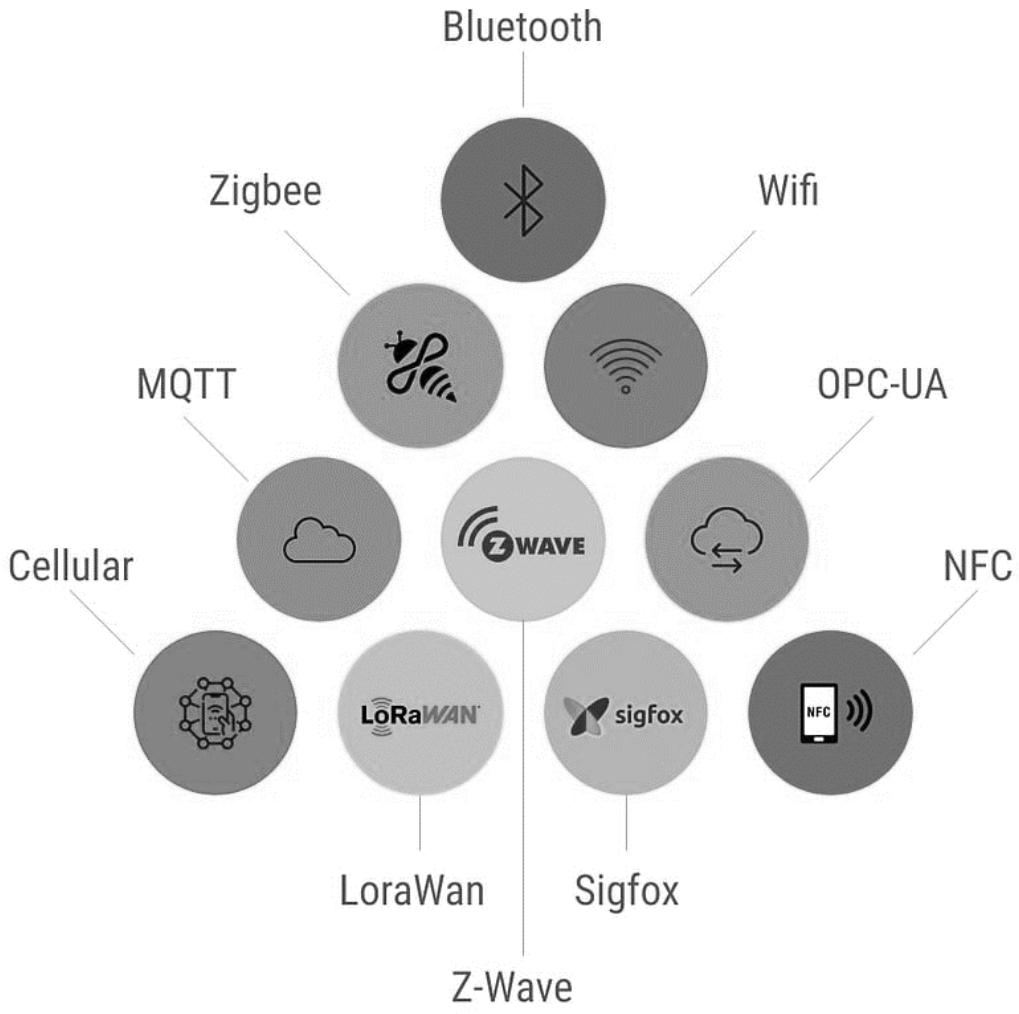
Enabling Technologies - Embedded Computing Boards

- An embedded computing board a very important component to bring IoT design to reality.
- For making the prototype the computing boards play vital role.
- The computing boards available in the market are driven by microcontrollers or processors.
  - Some of the boards are as follows:
    - Raspberry Pi.
    - Arduino (many variants).
    - NodeMCU.
    - Intel Edison.
- All these boards are small, yet smart.
- Also, the cost involved is very minimal and one can get these boards at cheap rate.



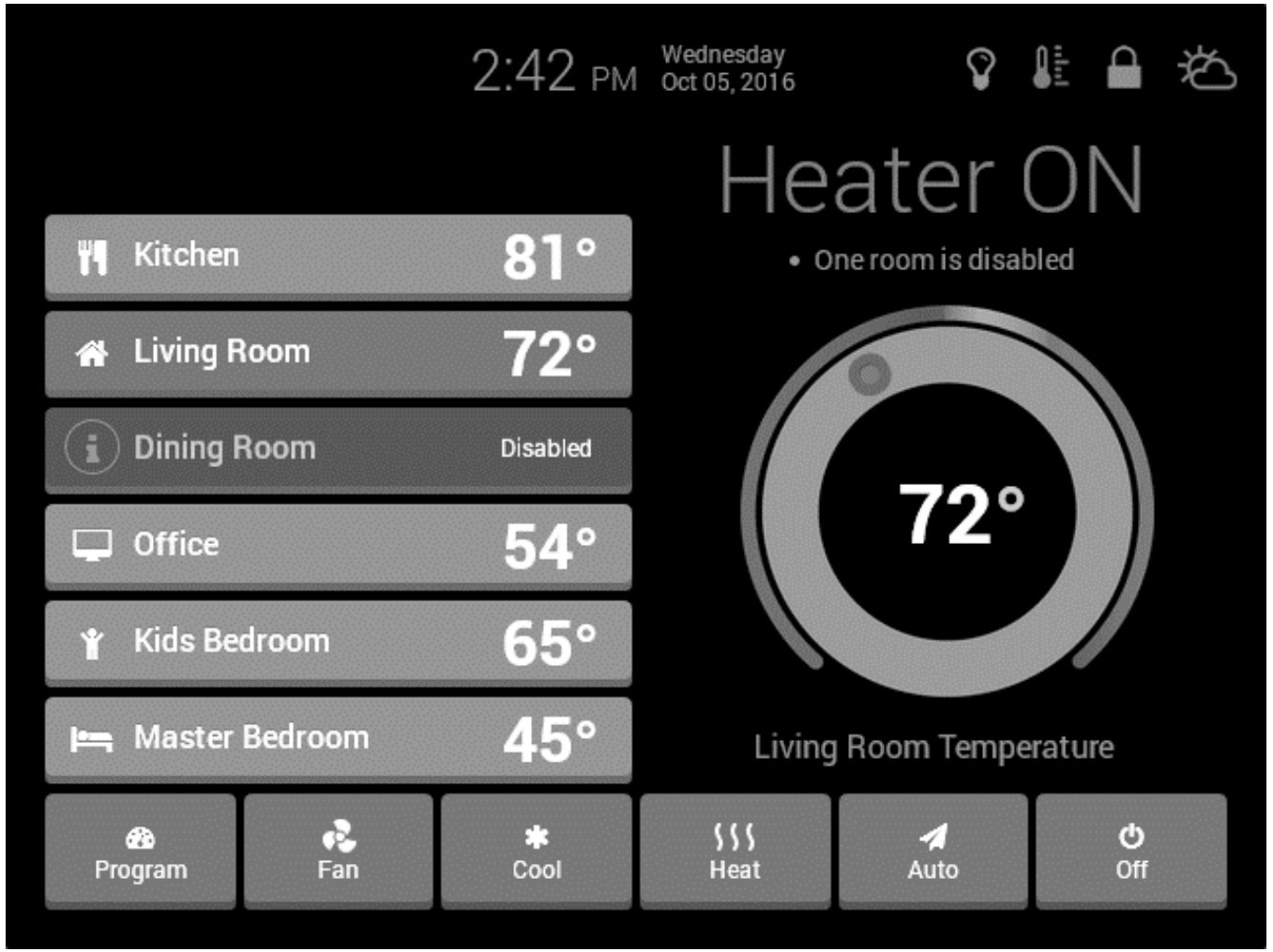
Enabling Technologies - Communication Protocols

- Protocols are the pillars for good IoT infrastructure and hence are very important in communication.
- Data exchange happens through these protocols, which take care of the following:
  - Addressing.
  - Format of the messages.
  - Message security (encryption and decryption).
  - Routing.
  - Flow control.
  - Error monitoring.
  - Sequencing.
  - Retransmission guidelines.
  - Segmentation of the data packets.



Enabling Technologies - User Interfaces

- All devices should have an intuitive user interface.
- IoT devices/services should be designed in such a way that accessing and handling the services are easier and comfortable for the end user.
- Generally , the end user shall be provided “mobile application or web application”.
- The application should be stable and elegant.



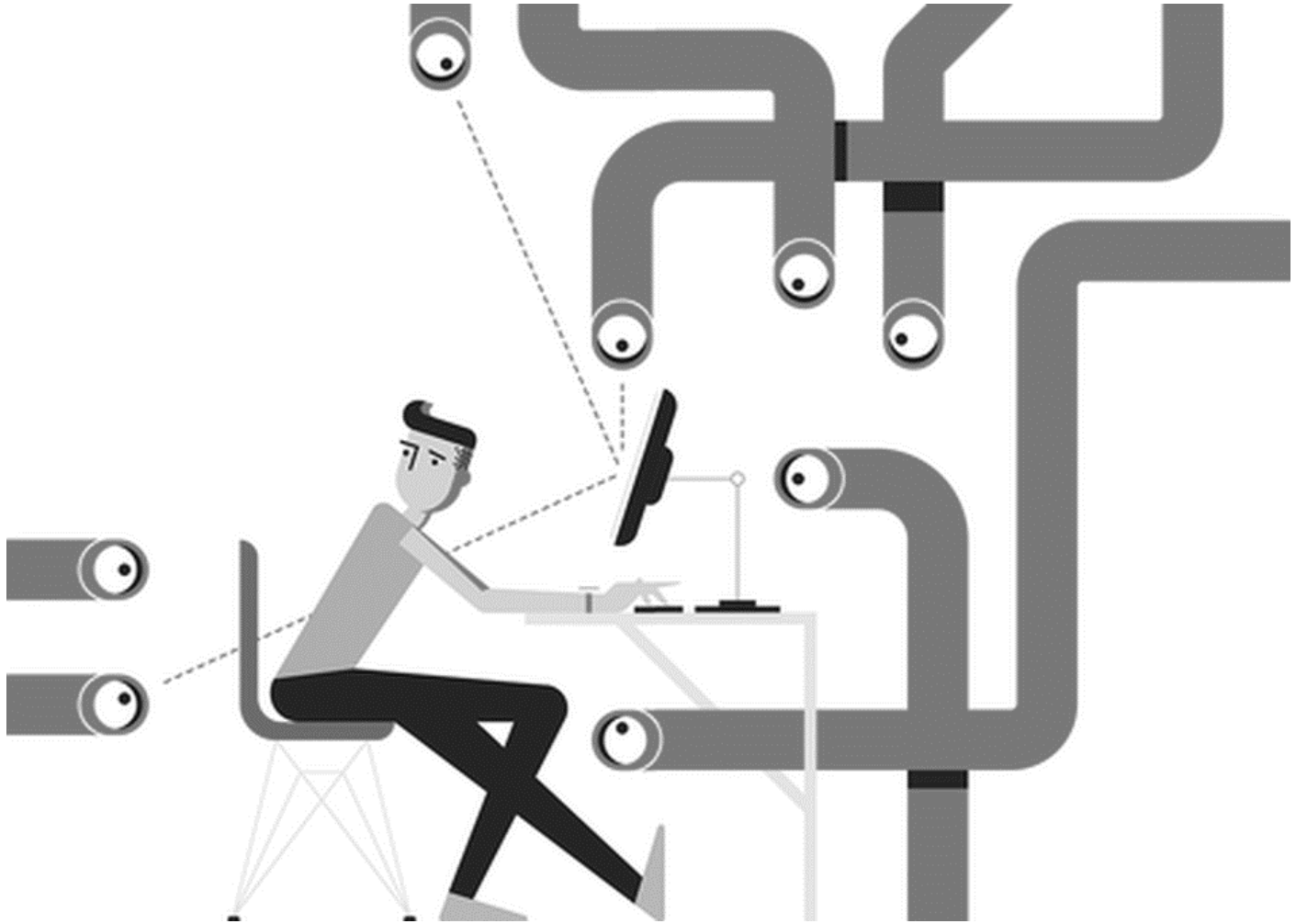
IoT Challenges

- The following are some of the challenges - technical and non-technical during building an IoT application .

1. **Security/Personnel safety:**
   - Security is one of the most significant challenges.
   - Number of IoT devices are gradually increasing, so user data becomes more vulnerable to theft.
   - Poor security features can let attackers damage the whole network and the rest of the devices could also become vulnerable.
   - People's personal safety is also a concern and challenge.
   - The implants and wearable used by people should be safe even from physical harm.

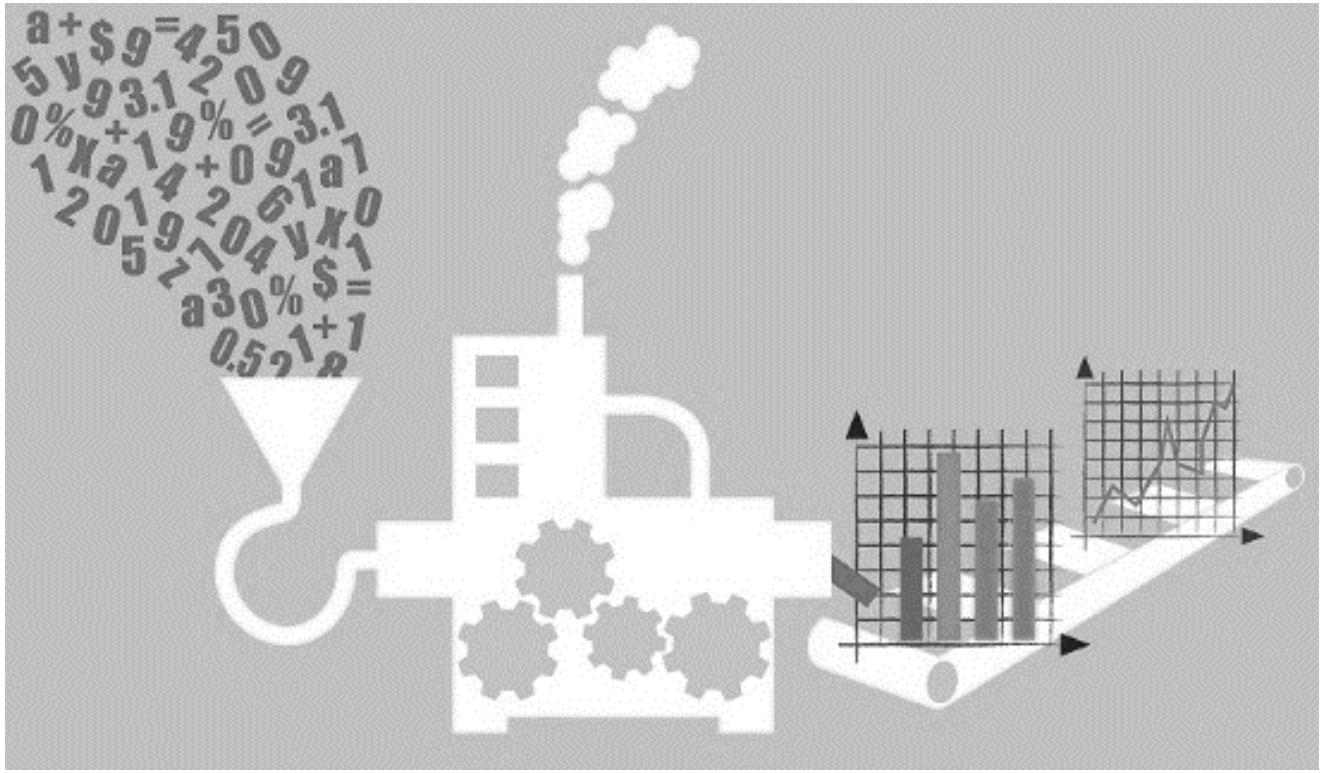
IoT Challenges

2. Privacy:
   - One could be tracked/monitored by anyone, as we are connected 24 × 7 to the Internet.
   - So, there is a threat on user data and raises a question on user privacy.
   - “How do we ensure that the data that is sensed and collected from the user is with their permission?”



IoT Challenges

3. Data extraction with consistency from complex environments:
   - It is a huge challenge to sense and extract data from complex environments.
   - For Example, variation in temperature could also damage the products being transported.
   - Maintained the temperature is very critical and should be accurately monitored.
   - If the temperature is about to change, then the corrective action has to be taken.
   - Data extraction and storage in the cloud could be more challenging if the internet is not available.
   - Extracting data inside a room is different from extracting data from an open environment.

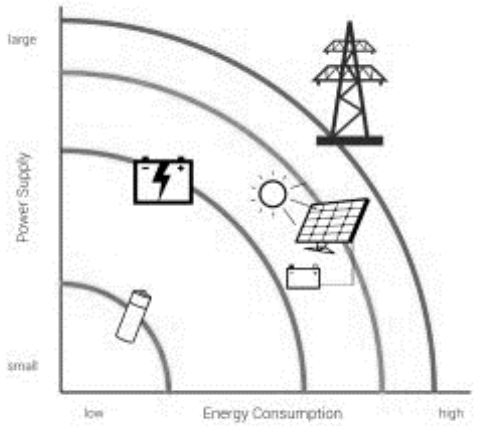


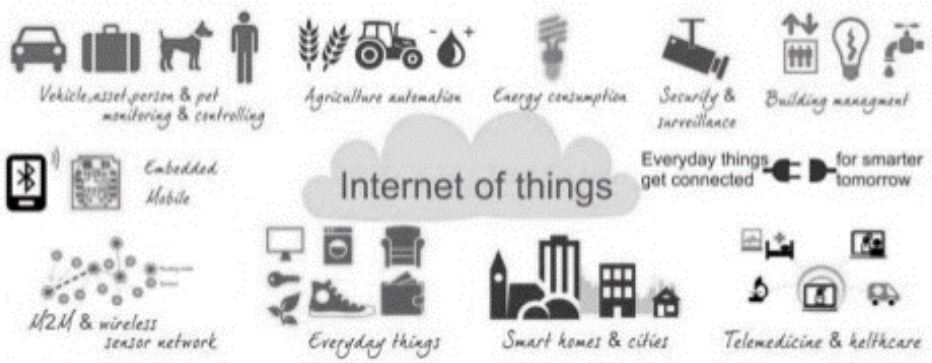
IoT Challenges

4. Connectivity:
   - This is a serious challenge that the IoT world must acknowledge.
   - Since the Internet is itself a giant collection of networks and devices and IoT is a part of it. So requirement of wired and wireless connectivity is a necessity.
   - The usage of frequency / spectrum is also to be noted.
   - There are spectrum regulations to be followed based on the country for which the application is being developed.
   - 2.4 GHz band is the ideal band everywhere.

IoT Challenges

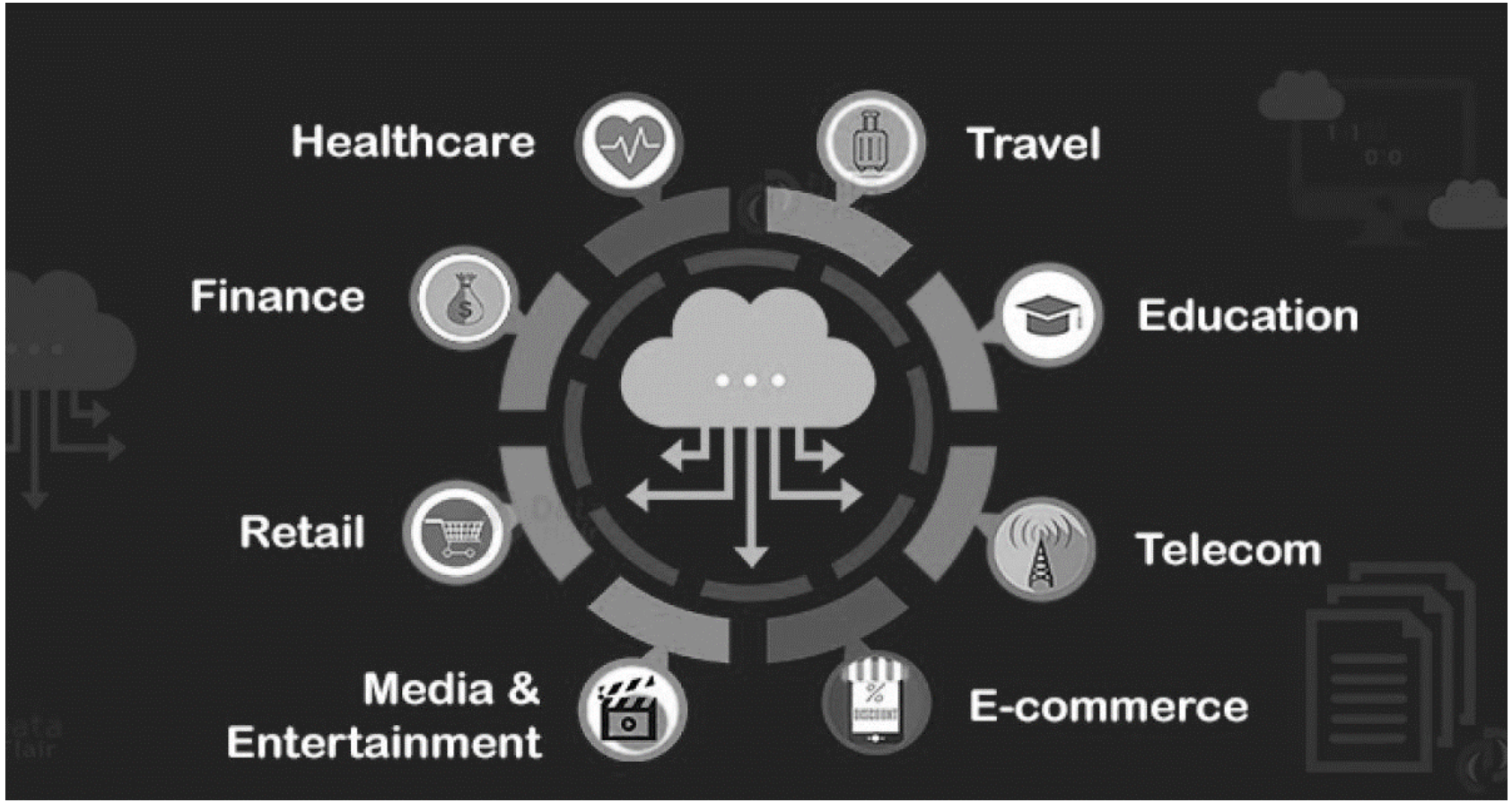
5. **Power requirements:**
   - All the IoT devices require power and most of them are battery operated.
   - Even though we now have long-lasting batteries that are economical, demand for power is on the rise.
   - Usage of green power sources such as solar and wind should be motivated.
   - If the power requirements are met appropriately, IoT can be even more powerful.
6. **Complexity involved:**
   - IoT is not easy. It needs a lot of different domains to integrate into a cohesive system.
   - There is very limited expertise available in the market, but the growth is very rapid.
   - The toolkits, software and hardware are not abundant and real skill is required to build an application.





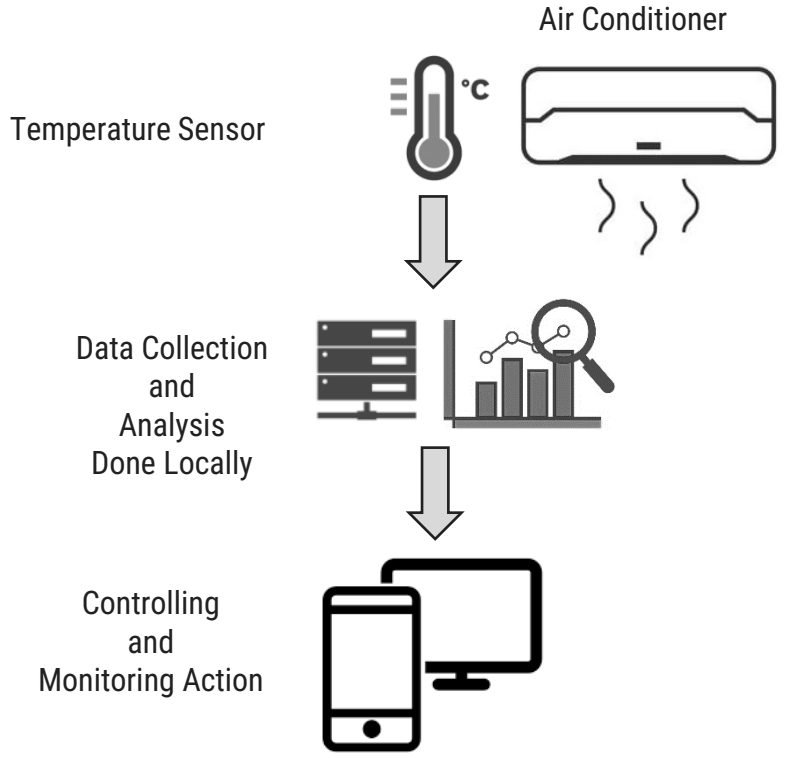
IoT Challenges

7. Storage:
   - Cloud is becoming mandatory for the data to be stored and analyzed.
   - The challenge with respect to this aspect is connected to the following points:
     - Which cloud do we use (private, public, or hybrid)?
     - How do we identify the service provider?
     - How much does it cost?
     - Do we really need cloud?



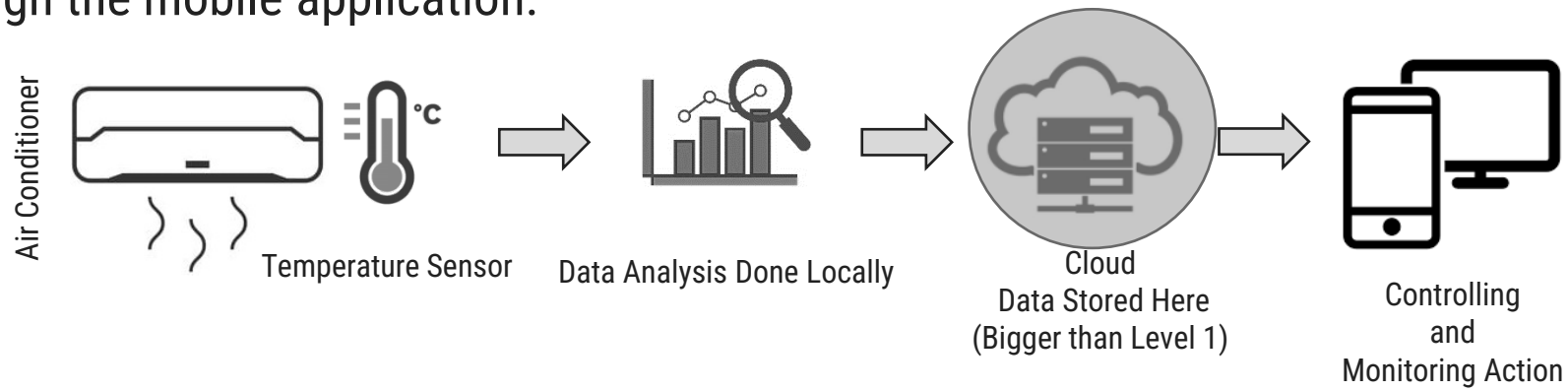
IoT Levels

- Based on the architectural approach, IoT can be classified in five levels: Level 1 to Level 5.
- Level 1
  - It is of minimal complexity.
  - The application has one sensor (temperature sensor, pressure sensor, etc).
  - The data sensed is stored locally and the data analysis is done locally.
  - Monitoring / control is done through an application.
  - This is used for simple applications.
  - Data generated in this level application is not huge.
  - For example, a temperature sensor senses the room temperature and the data is stored and analyzed locally.
  - Based on the analysis, the control action can be triggered through mobile application or it can help in monitoring the status.



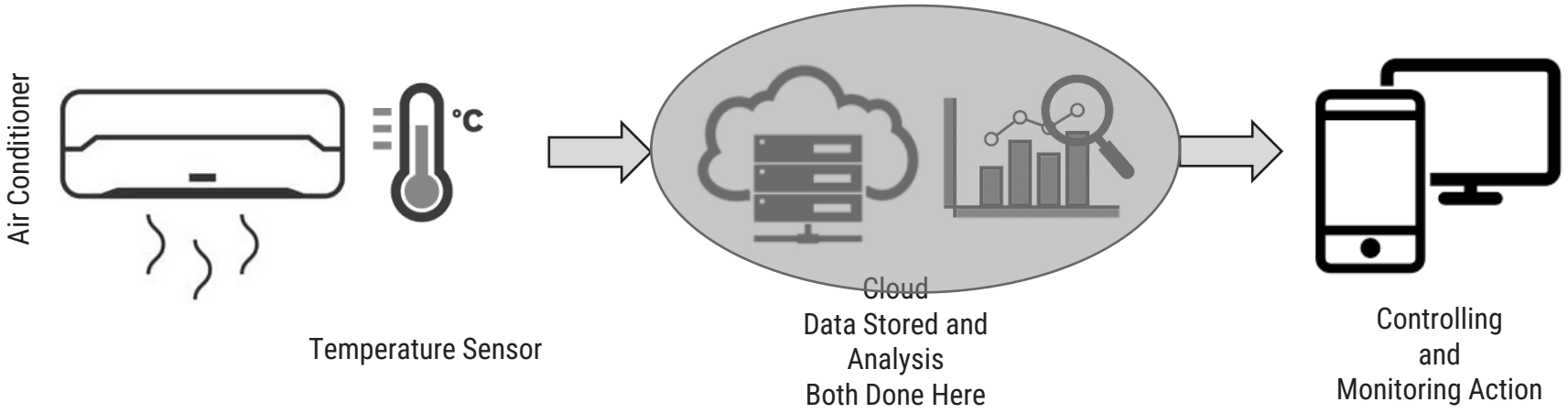
IoT Levels

- Level 2
  - The second level is slightly more complex than the previous level.
  - The data is more voluminous and hence, cloud storage is preferred.
  - The frequency of sensing done by the sensor is faster.
  - The number of times sensing is done would be much more than Level 1.
  - The analysis is carried out locally, while cloud is meant for storage only.
  - Based on the data analysis, the control action can be triggered through the web application or mobile application.
  - Some examples are agriculture applications, room freshening solutions based on odor, etc.
  - IoT application of an air conditioner. The sensor reads the room temperature at a better pace and rate than Level 1; the data then goes on to the cloud for storage. Analysis is done locally and the action is triggered through the mobile application.



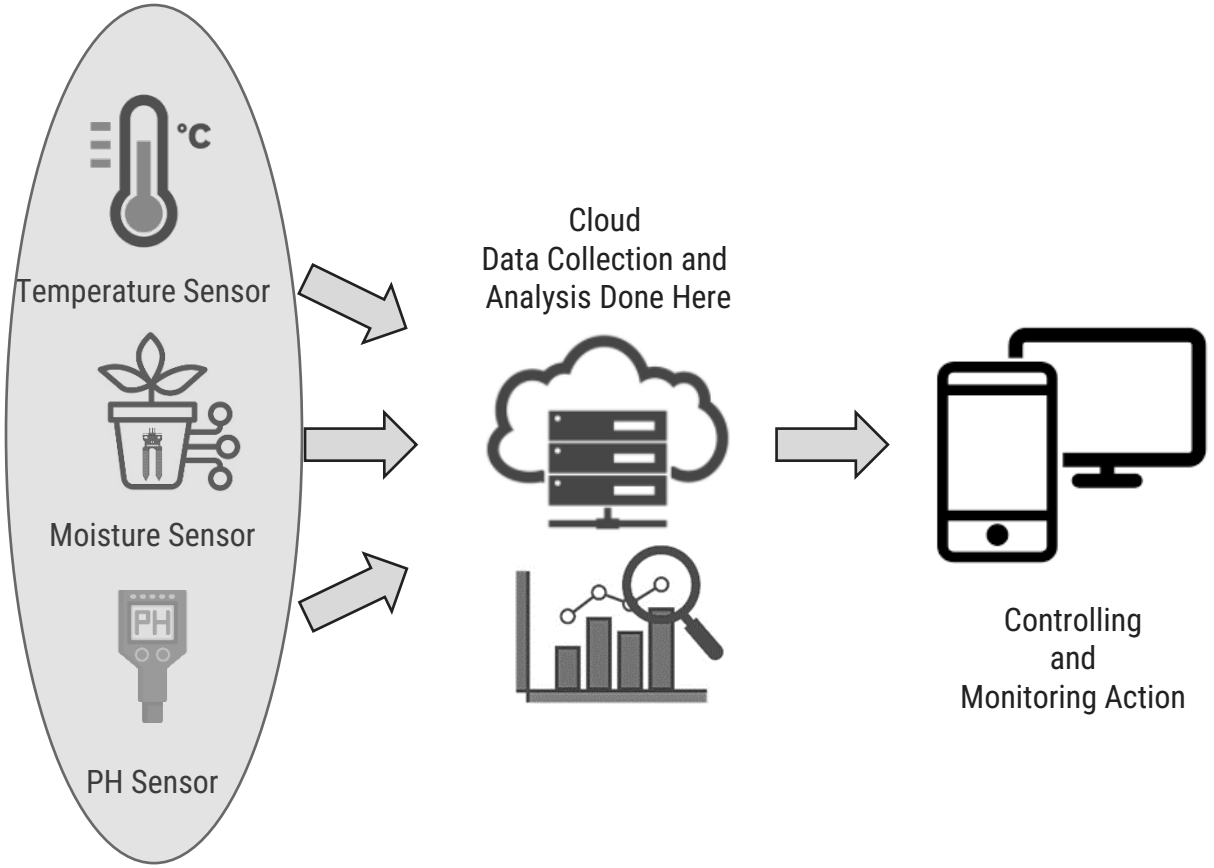
IoT Levels

- Level 3
  - The data is huge, frequency of sensing done by the sensor is faster and the data is stored on cloud.
  - The difference is that the analysis is also carried out on cloud.
  - Based on the data analysis, the control action can be triggered through the web application or mobile application.
  - Some examples are agriculture applications, room freshening solutions based on odor, etc., where analysis of data occurs in the cloud.



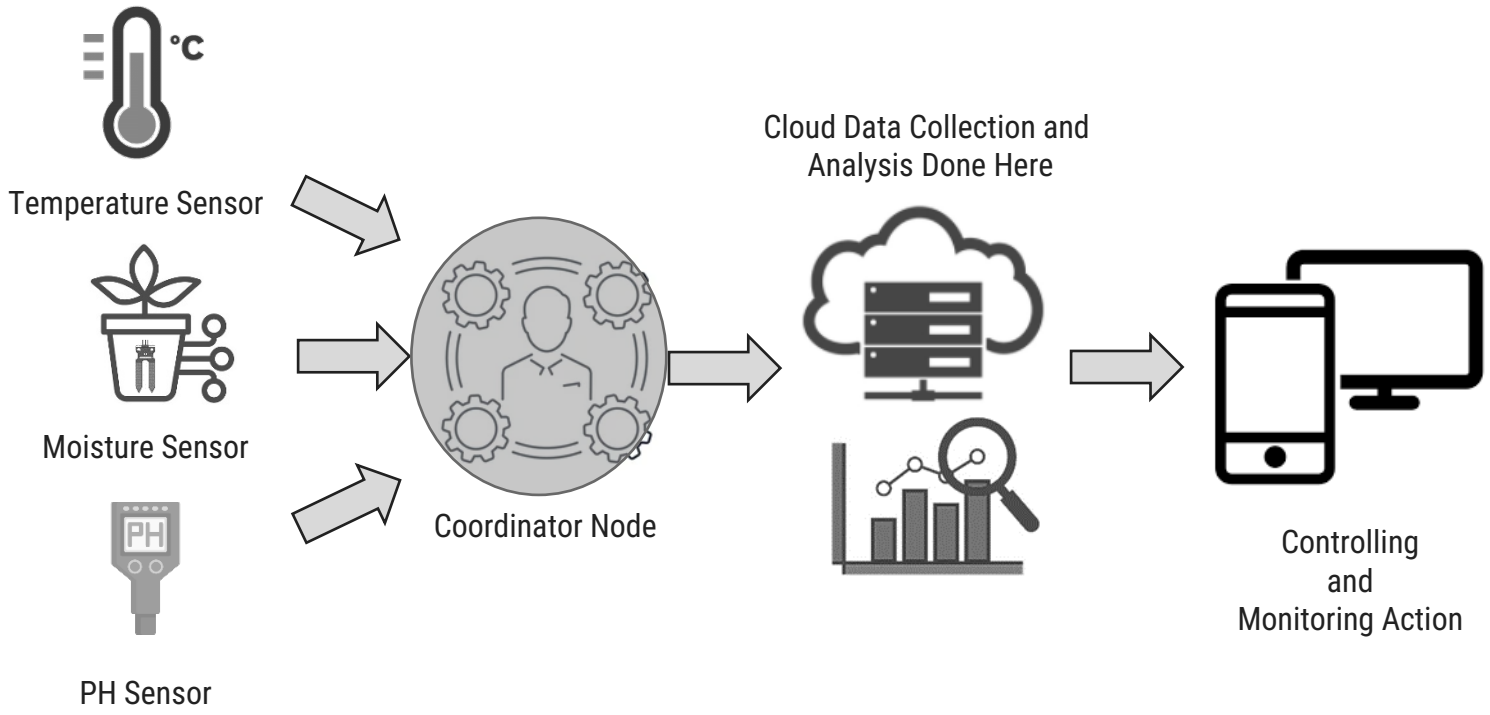
IoT Levels

- Level 4
  - With every passing level, the volume of data increases and hence the rate at which it is sensed also increases.
  - At this level, multiple nodes are present which are independent of each other.
  - These nodes upload data to the cloud.
  - All the sensors upload the read sensory inputs on cloud storage.
  - Analysis is also carried out on the cloud.
  - Based on the analysis carried out, the control action shall be triggered through a web application or mobile application.



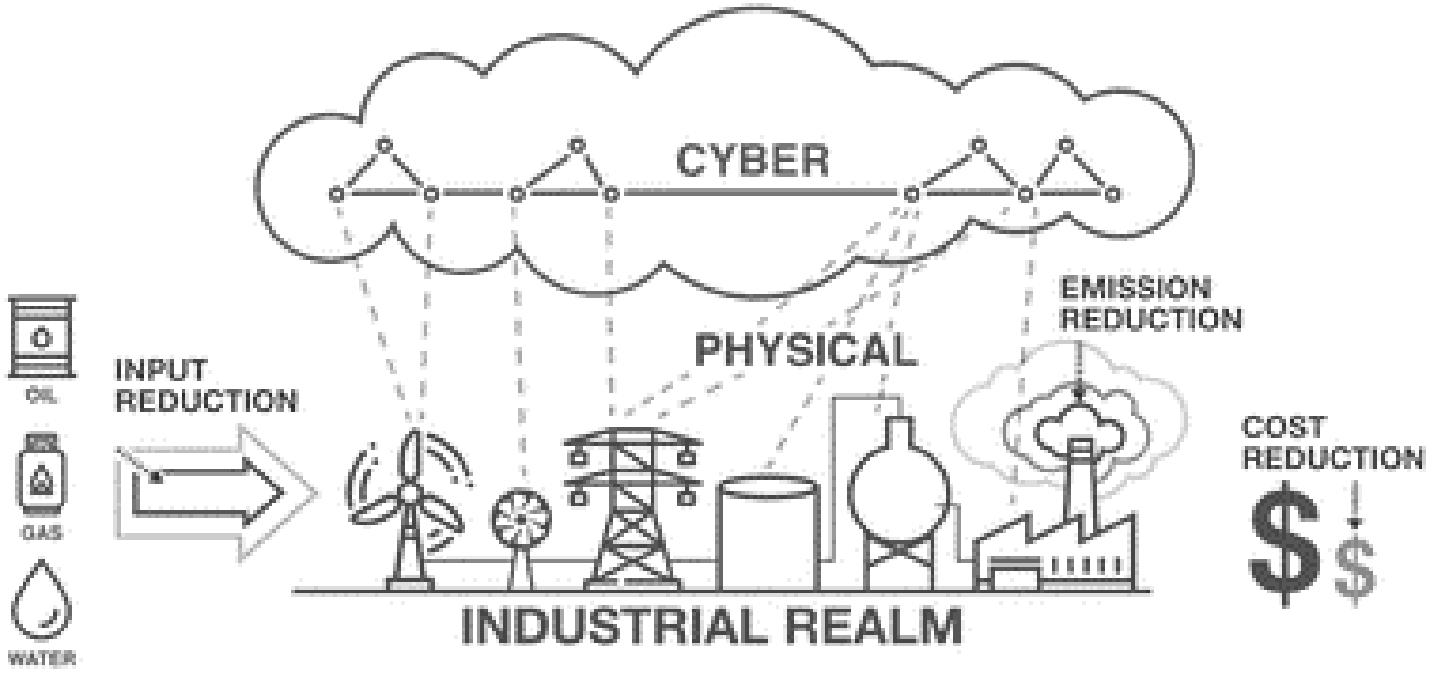
IoT Levels

- Level 5
  - At this level, the amount of data is extensive and is sensed much faster.
  - Multiple nodes are involved in the applications categorized under Level 5 and these nodes are independent of each other.
  - The sensing of data and its storage is the same as in all the previous levels.
  - When an application is completely cloud oriented, it is computationally intensive in real time.
  - Based on the data analysis, the control action can be triggered through web application or mobile application as in all other levels.



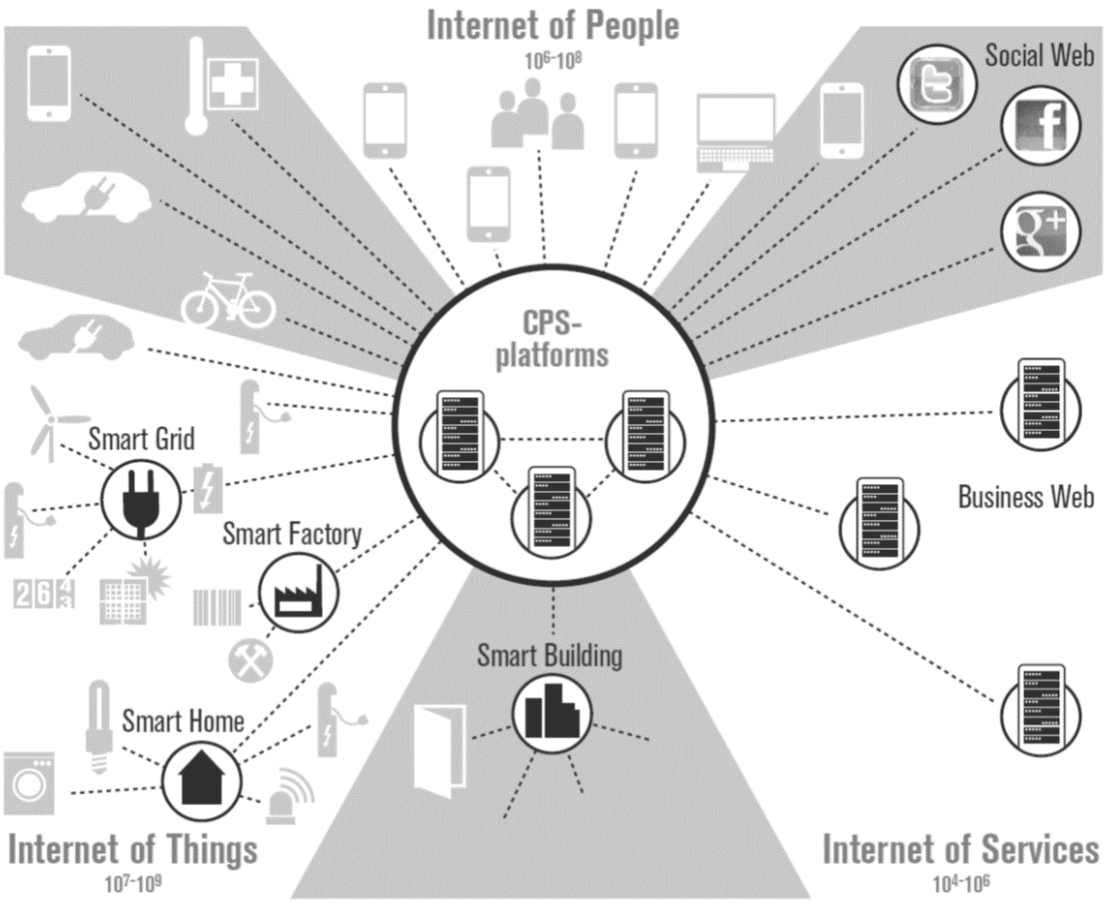
Cyber Physical System versus IoT

- An important question is, Is IoT same as Cyber Physical System (CPS)?
  - There is a misconception that both the terms are the same.
  - We have learned the definition of IoT. The “thing” can also be accessed from anywhere, anytime by an authorized party.
  - The information or the sensed data of the things can be simple.
  - So complexity involved in the IoT applications is minimal.
  - For complex levels of operation and to address larger network of “things”, a new term called Cyber Physical System or CPS, has been introduced.



Cyber Physical System versus IoT

- It is important to note that CPS is not IoT.
- CPS is more complex than IoT and is much more challenging.
- CPS has IoT as one of its components.
- It is a combination of multiple engineering domains coming together.
- The flight of an aero plane can be seen as a CPS which involves multiple domains of engineering.
- CPS is much more autonomous than IoT, taking appropriate decisions as and when needed.
- It is not just about identifying “things”; it is more about understanding and taking decisions in a more dynamic way.
- CPS is mainly concerned about the collaborative activity of sensors or actuators to achieve a certain goal.
- For that CPS uses an IoT system to achieve the collaborative work of the distributed systems.



A Cyber-Physical System (CPS) is a system that integrates physical and computational components to monitor and control the physical processes seamlessly.

In other words, A cyber-physical system is a collection of computing devices communicating with one another and interacting with the physical world via sensors and actuators in a feedback loop.

These systems combine the sensing, actuation, computation, and communication capabilities, and leverage these to improve the physical systems' overall performance, safety, and reliability.

Examples: CPS includes self-driving cars, The STARMAC is a small quadrotor aircraft.

Features of Cyber-Physical System

in terms of the cyber-physical system, there are some features that are classified.

1. **Reactive Computation:** Reactive systems, on the other hand, continuously interact with the environment through inputs and outputs. As a classic example of reactive computation, consider a car cruise control program.
2. **Network Connectivity:** CPS systems must utilize the network connectivity basis of communication between the cyber and physical world.
3. **Robustness & Reliability:** In order to ensure safe and effective operation in dynamic environments, CPS must need efficient reliability.
4. **Concurrency:** In cyber-physical systems refers to the simultaneous execution of multiple tasks or processes in a coordinated manner.
5. **Real-Time Computation:** CPS systems have real-time computation capabilities that allow for dynamic decision-making based on physical real-world data.
6. **Safety-Critical Application:** In terms of the CPS applications where the safety of our systems higher priority over the performance and development of the system.

Characteristics

- It is a combination of Physics with cyber Components networked which is interconnected.
- CPS systems are to monitor and control physical processes in a seamless manner.
- In CPS systems sensors and Actuators work in the feedback loop.
- In CPS systems devices are designed to interact with physical processes and control them.
- The CPS systems are more complex compared then IoT devices.

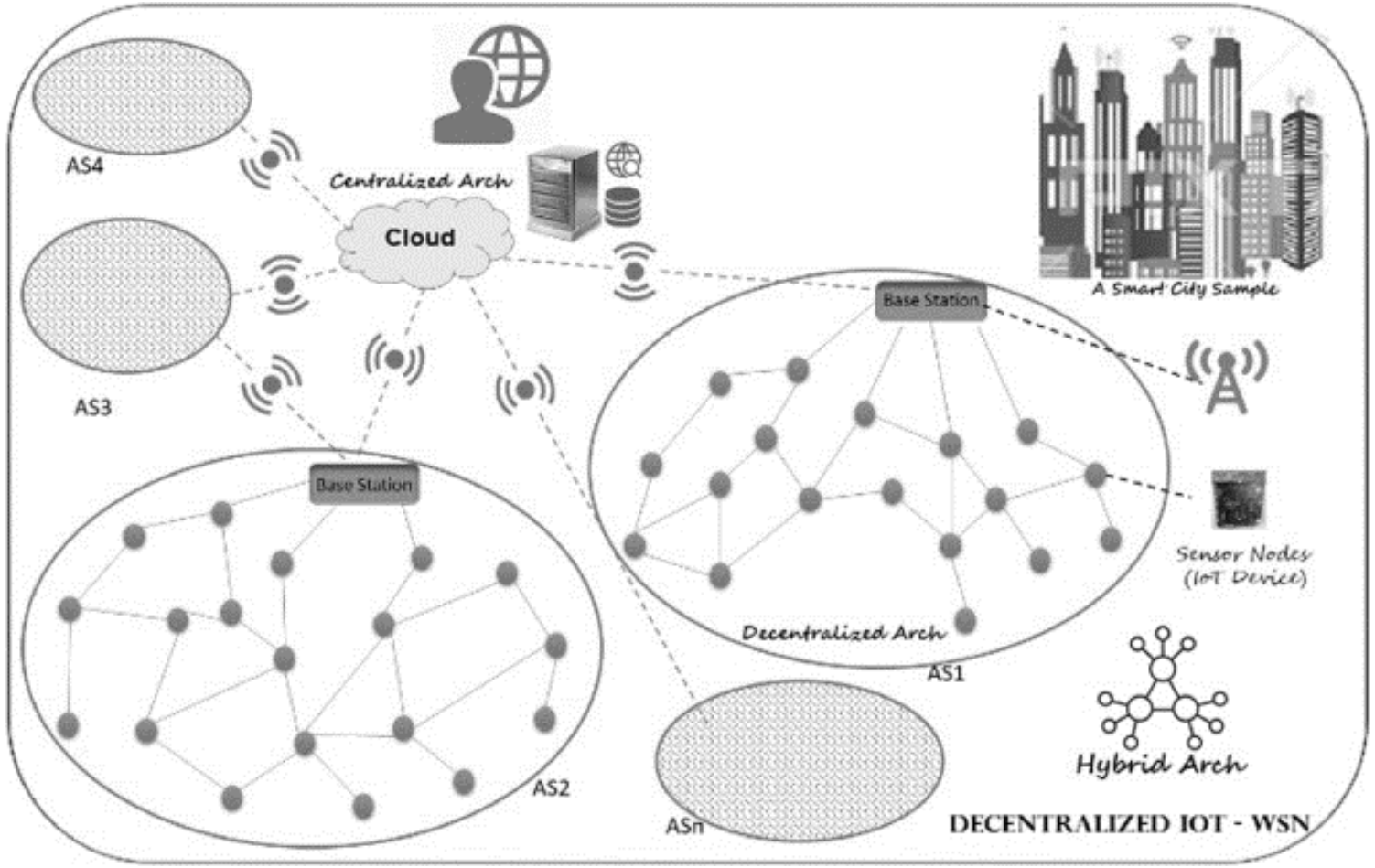
Application of Cyber-Physical System

Cyber-Physical systems have the widest application in the real world with technology, cps is mostly applied in many fields as you can see-

- **Agriculture:** Through the cps systems we can develop such kinds of sensors and tractors or harvesters that provide information on soil type and condition.
- **Aeronautics:** Aeronautics is one area that can benefit from CPS integration. In Aeronautics, CPS can be used to improve aircraft control and safety and improve performance and efficiency.
- **Healthcare and Personalized Medicine:** CPS systems have the technology which involves the use of connected medical devices and wearables to monitor patients' health data.
- **Civil Infrastructure:** Cyber-physical systems are using infrastructure improvement with some new efficiency technology. Advanced digital technology like IoT and sensors etc.
- **Manufacturing:** In manufacturing CPS can monitor and control the production process in real-time, improving quality and reducing scrap.
- **Transportation:** In transportation, CPS can improve safety and efficiency through intelligent traffic management systems, vehicle-to-vehicle communications, and self-driving vehicles.

Wireless Sensor Network versus IoT

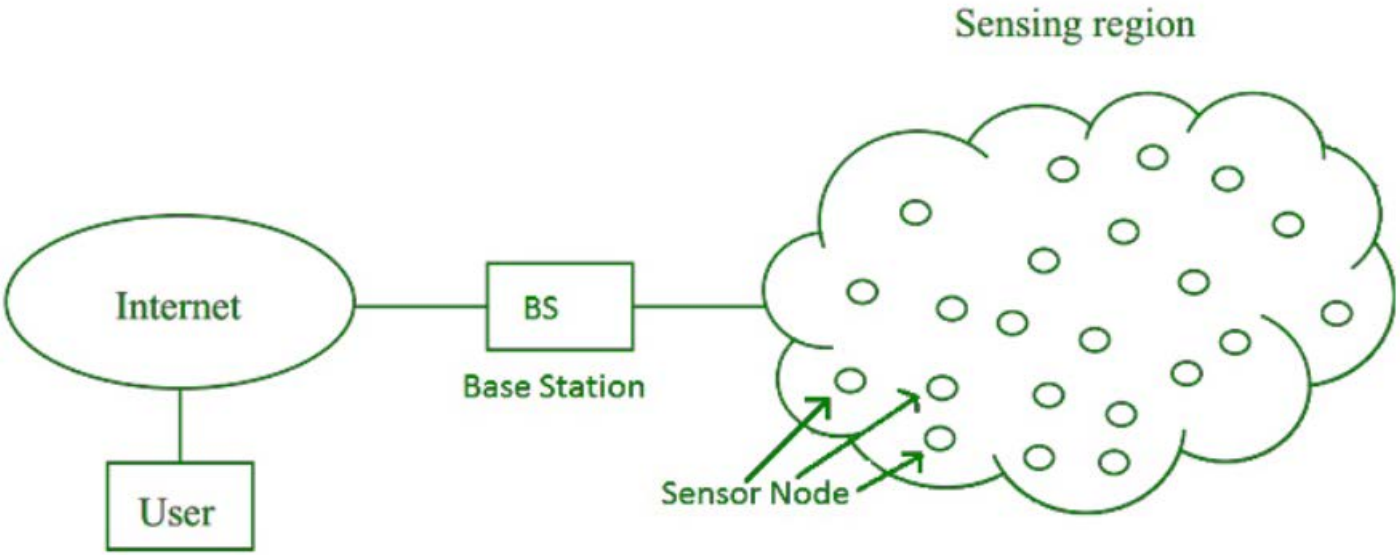
- WSN is a network of multiple autonomous sensors/nodes.
- Each node has one or more sensors.
- All the sensed data are passed to a centrally located server.
- The data passing happens in a coordinated pattern.
- We can say that WSN is all about coordinated data collection.
- On the other hand, IoT is much more than just data collection and the systems are more intelligent.



Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.

Base Station in a WSN System is connected through the Internet to share data.



WSN can be used for processing, analysis, storage, and mining of the data.

Applications of WSN:

1. Internet of Things (IoT)
2. Surveillance and Monitoring for security, threat detection
3. Environmental temperature, humidity, and air pressure
4. Noise Level of the surrounding
5. Medical applications like patient monitoring
6. Agriculture
7. Landslide Detection

Challenges of WSN:

1. Quality of Service
2. Security Issue
3. Energy Efficiency
4. Network Throughput
5. Performance
6. Ability to cope with node failure
7. Cross layer optimisation
8. Scalability to large scale of deployment

A modern Wireless Sensor Network (WSN) faces several challenges, including:

- **Limited power and energy:** WSNs are typically composed of battery-powered sensors that have limited energy resources. This makes it challenging to ensure that the network can function for long periods of time without the need for frequent battery replacements.
- **Limited processing and storage capabilities:** Sensor nodes in a WSN are typically small and have limited processing and storage capabilities. This makes it difficult to perform complex tasks or store large amounts of data.
- **Heterogeneity:** WSNs often consist of a variety of different sensor types and nodes with different capabilities. This makes it challenging to ensure that the network can function effectively and efficiently.
- **Security:** WSNs are vulnerable to various types of attacks, such as eavesdropping, jamming, and spoofing. Ensuring the security of the network and the data it collects is a major challenge.
- **Scalability:** WSNs often need to be able to support a large number of sensor nodes and handle large amounts of data. Ensuring that the network can scale to meet these demands is a significant challenge.
- **Interference:** WSNs are often deployed in environments where there is a lot of interference from other wireless devices. This can make it difficult to ensure reliable communication between sensor nodes.
- **Reliability:** WSNs are often used in critical applications, such as monitoring the environment or controlling industrial processes. Ensuring that the network is reliable and able to function correctly in all conditions is a major challenge.

Components of WSN:

1. **Sensors:**
   Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.
2. **Radio Nodes:**
   It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.
3. **WLAN Access Point:**
   It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.
4. **Evaluation Software:**
   The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

Advantages of Wireless Sensor Networks (WSN):

Low cost: WSNs consist of small, low-cost sensors that are easy to deploy, making them a cost-effective solution for many applications.

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.

Energy efficiency: WSNs use low-power devices and protocols to conserve energy, enabling long-term operation without the need for frequent battery replacements.

Scalability: WSNs can be scaled up or down easily by adding or removing sensors, making them suitable for a range of applications and **environments.**

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.