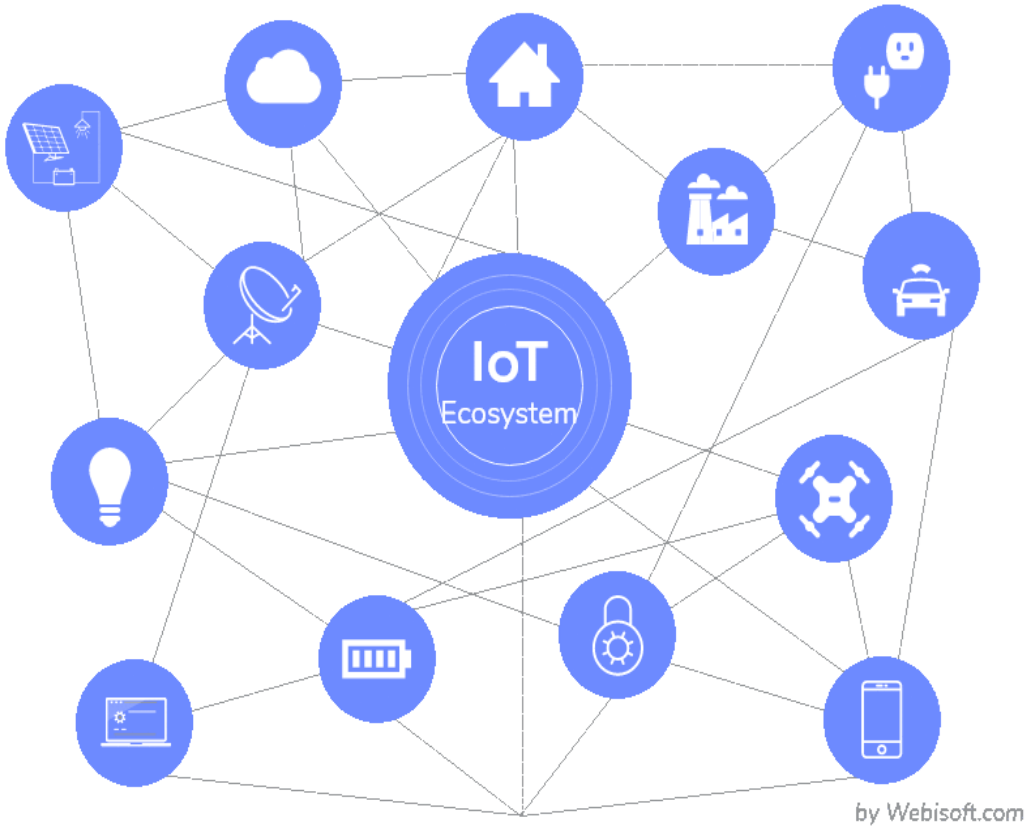
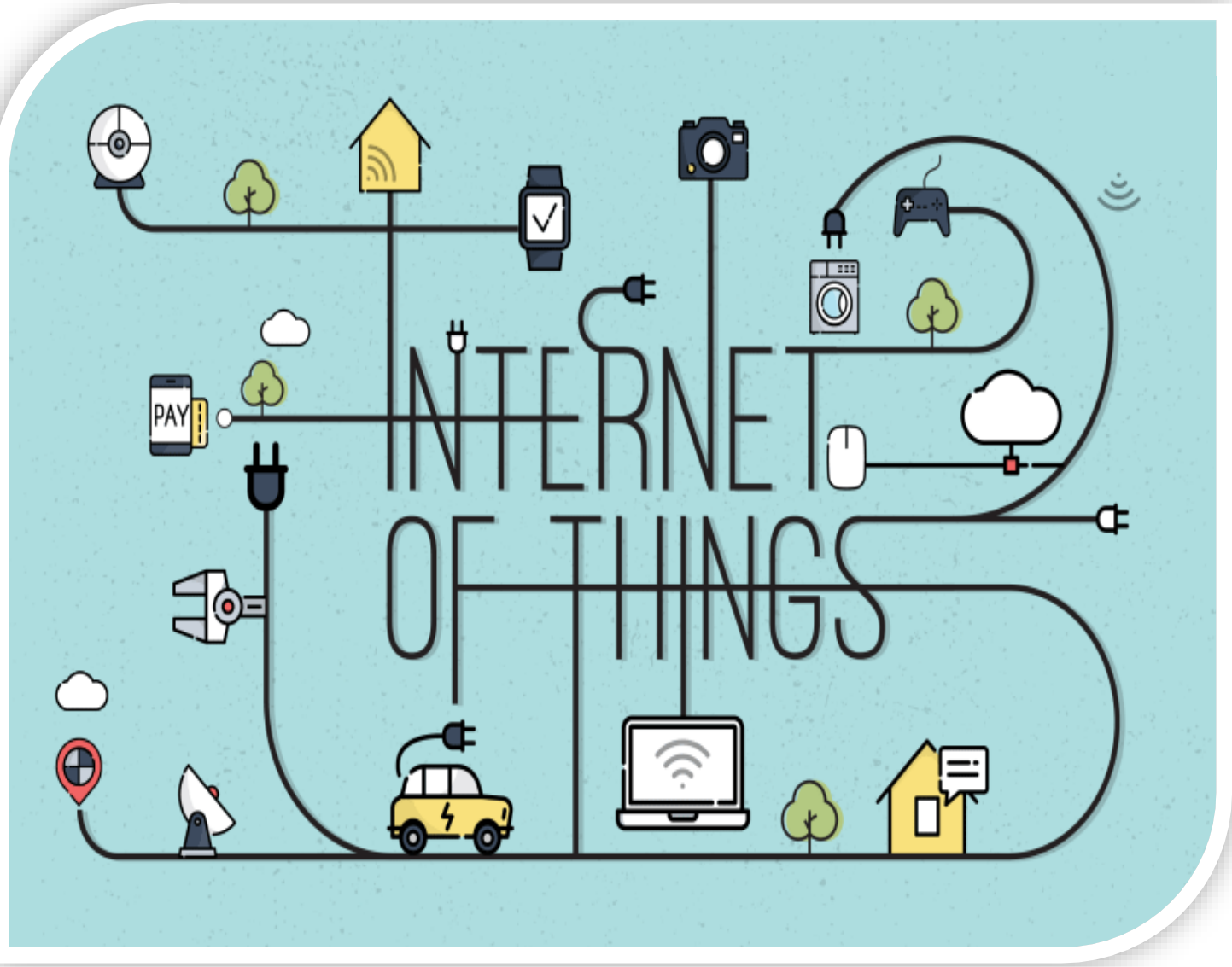
Unit 1:

Introduction to IoT



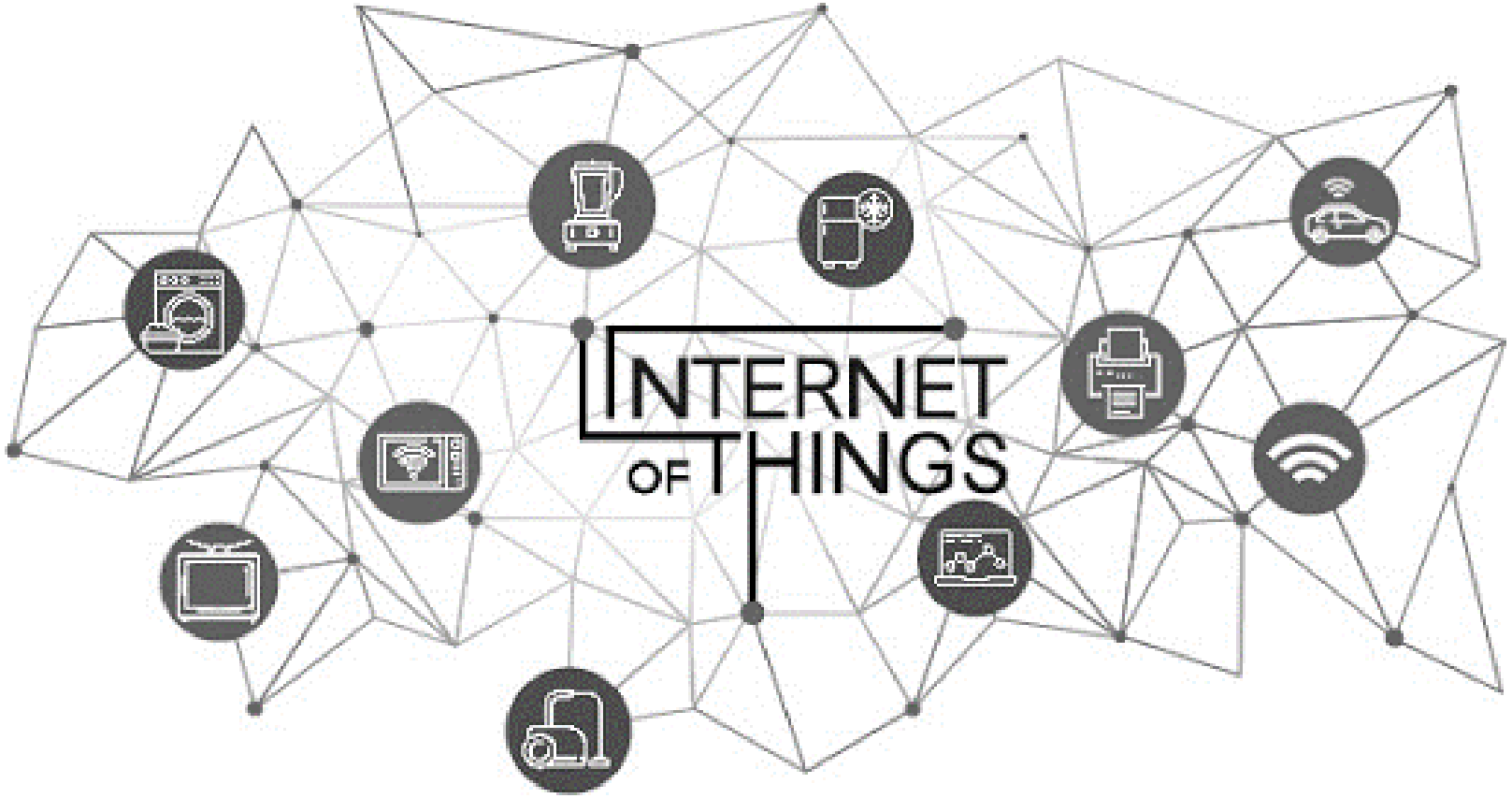
Unit Outlines:

- Introduction to IoT
- Things in IoT
- Characteristics of IoT Things
- Characteristics of IoT
- Application areas of IoT
- IoT Protocol Structures
- Enabling Technologies
- IoT Challenges
- IoT Levels
- Physical Design of IoT
- Logical Design of IoT



Introduction to Internet of Things (IoT)

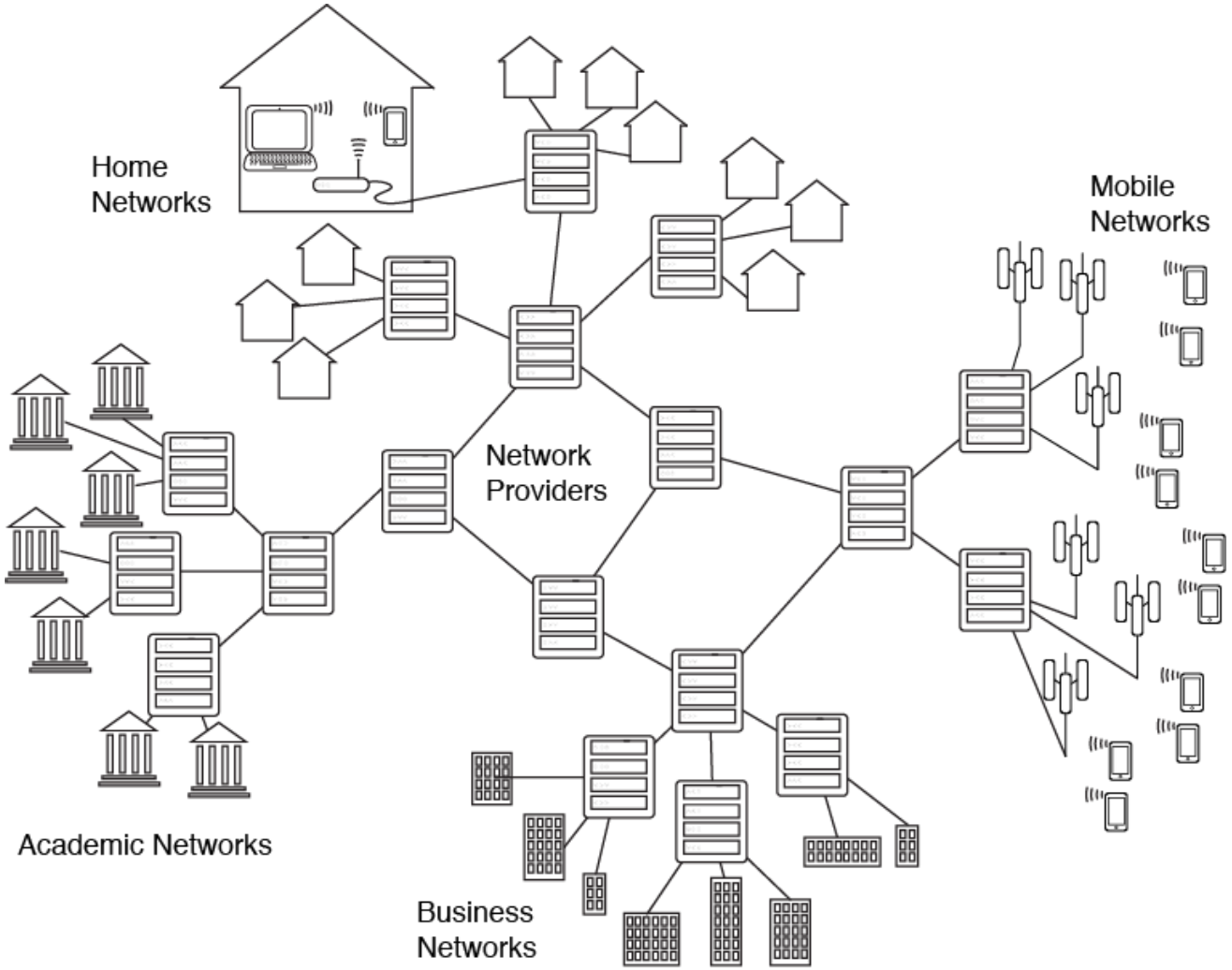
- First of all we should discuss about the name “IoT – Internet of Things” in detail.



- 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?

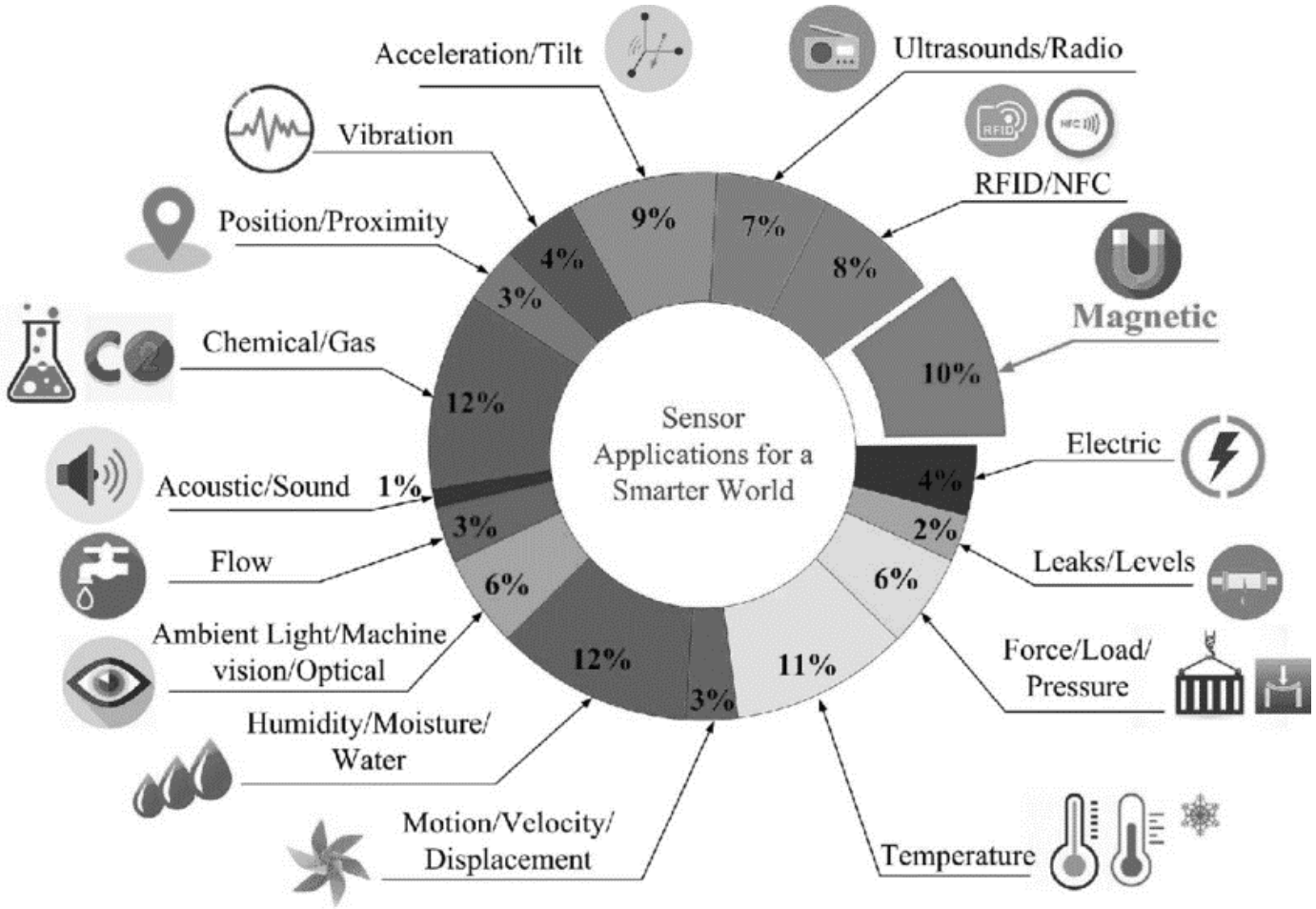


- In simple word, it's a Network of Networks or Interconnected LANs.
- What is Network?, Requirement for networking

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” - **physical devices** that are embedded with **sensors, software, and network connectivity**.
- These devices can collect and share data with other devices and systems over the internet or other communication networks

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:

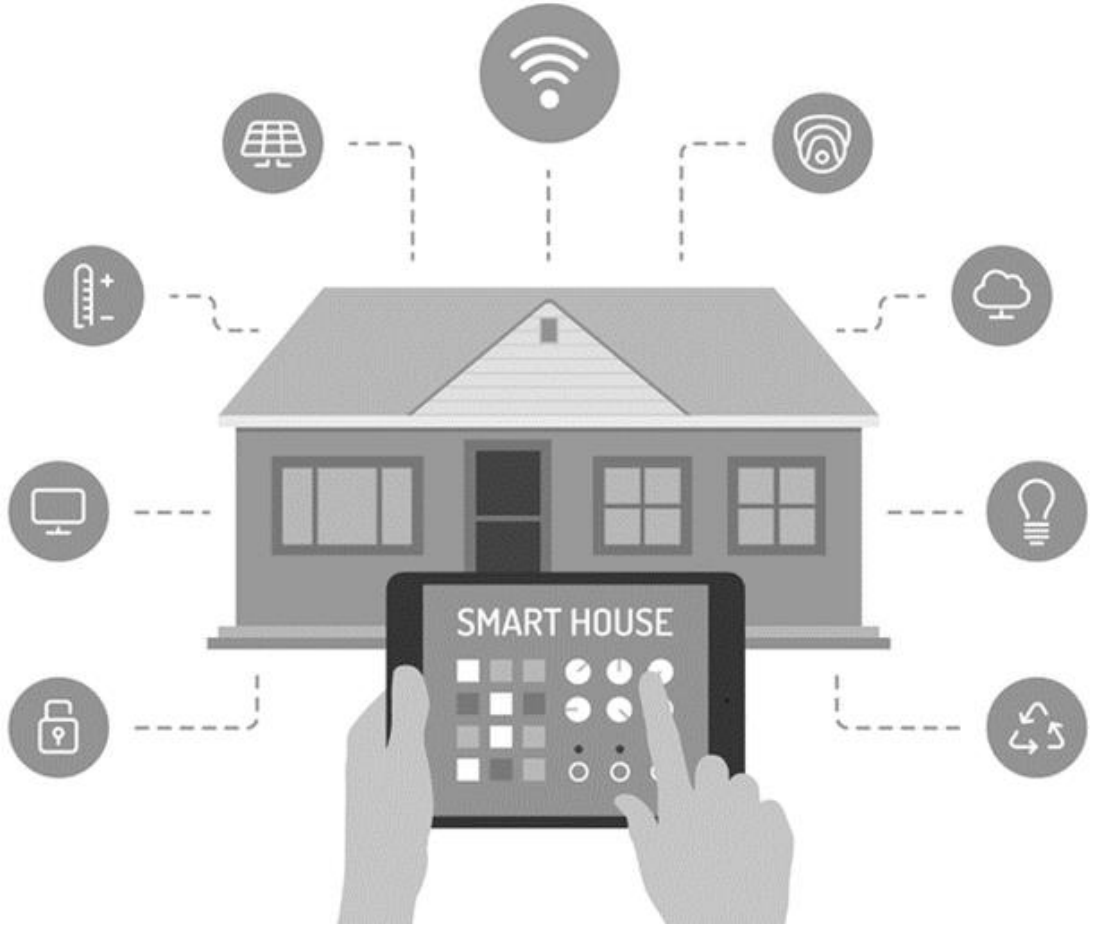
- Industrial motors
- Wearables (e.g., watch)
- Vehicles
- Shoes
- Heart monitoring implants (e.g., pacemaker, ECG real-time tracking)
- Biochip transponders (for animals in farms)
- Automobiles with built-in sensors (automobile feature real-time monitoring)
- Food/perishables quality measuring

Characteristics of Things

- **Connectivity**: IoT devices are equipped with network interfaces that enable them to connect to the internet or other networks.
- **Interactivity**: IoT devices can interact with users and other devices, either directly or through a central hub or cloud service.
- **Data Processing**: Many IoT devices have the capability to process data locally (edge computing) or send data to the cloud for more complex processing.
- **Unique Identity**
- **Self Adapting & Self Configuration**: IoT systems are designed to support a large number of devices, allowing for easy expansion.
- **Energy Efficiency**: Many IoT devices are designed to be energy-efficient, often operating on battery power for extended periods.
- **Dynamic Nature**
- **Heterogeneity**

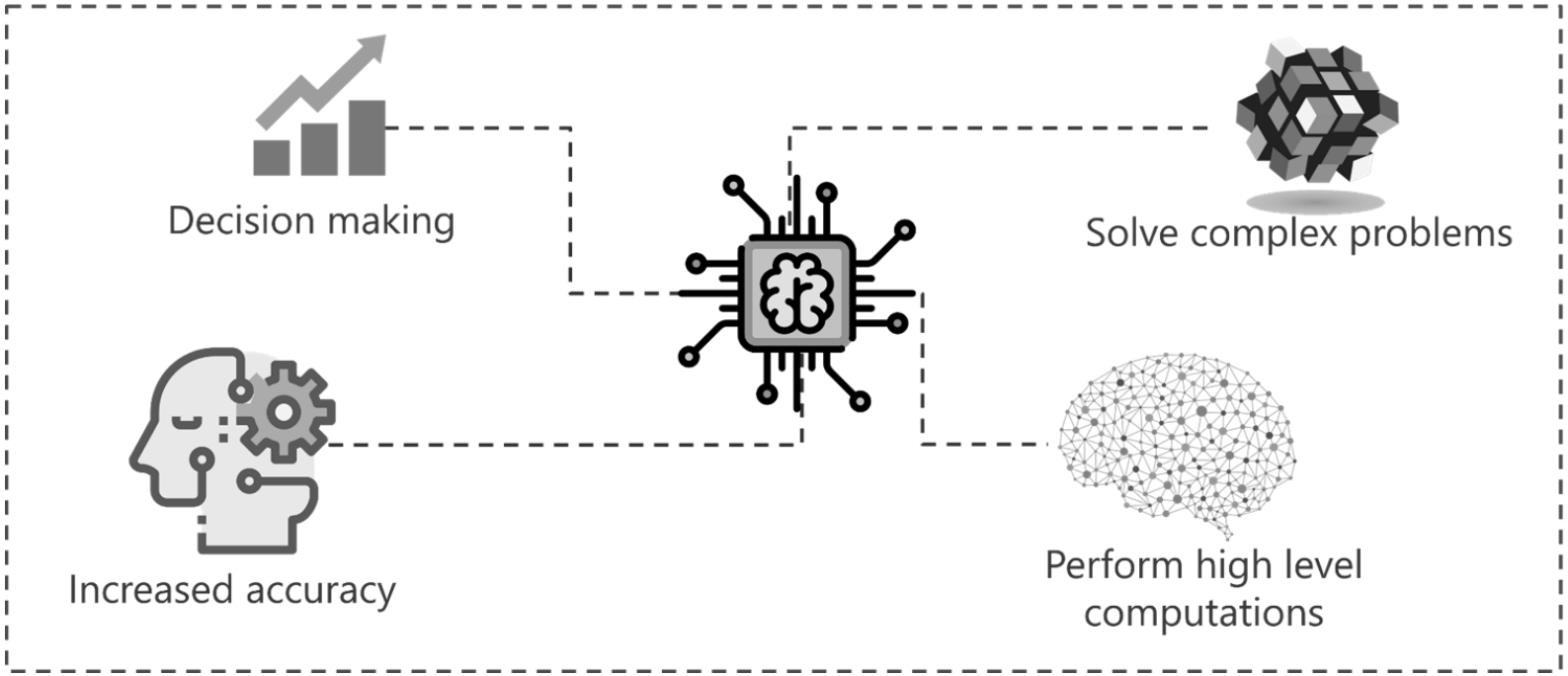
Things in IoT

- 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



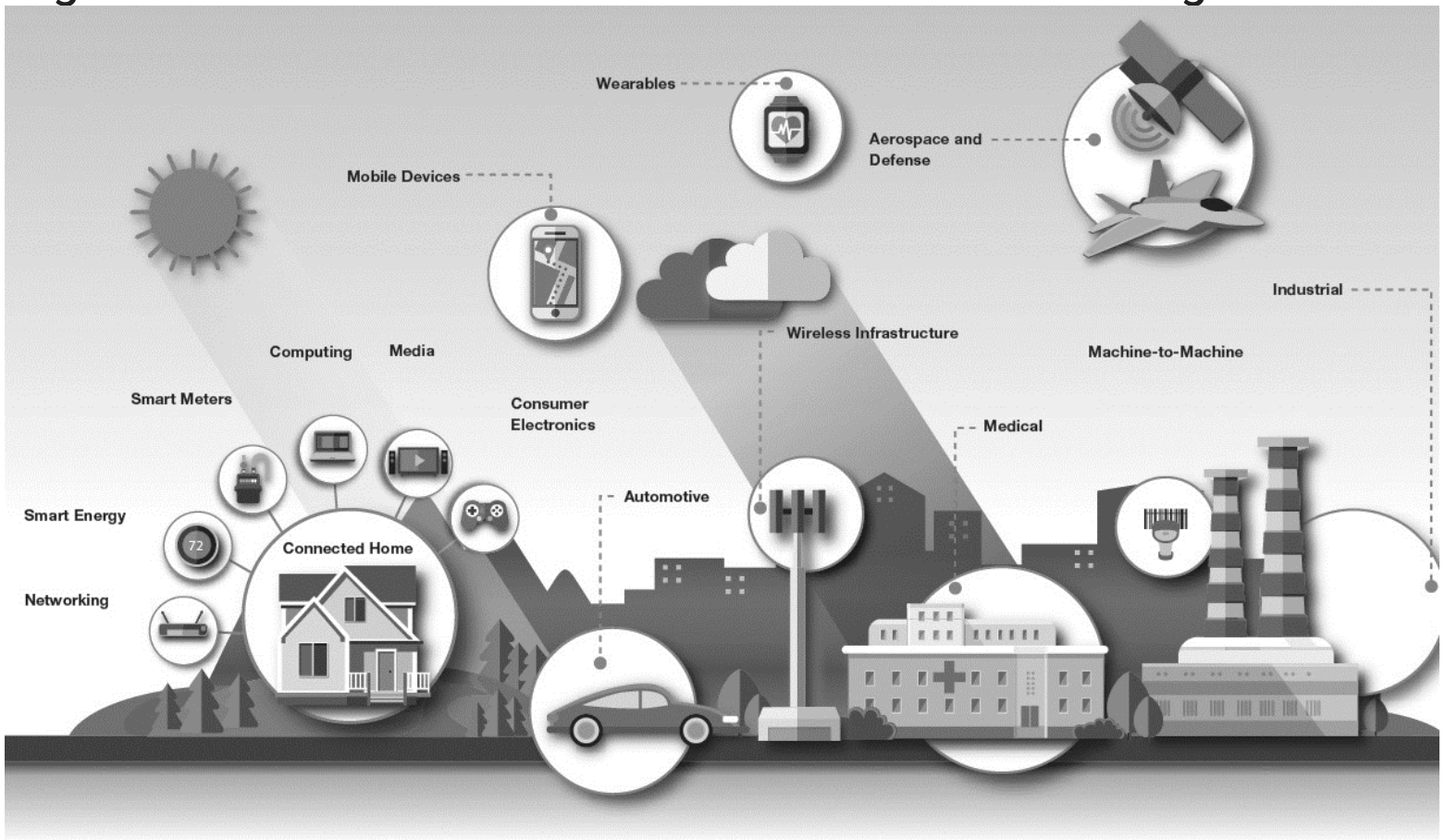
Introduction to Internet of Things (IoT)

- 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)

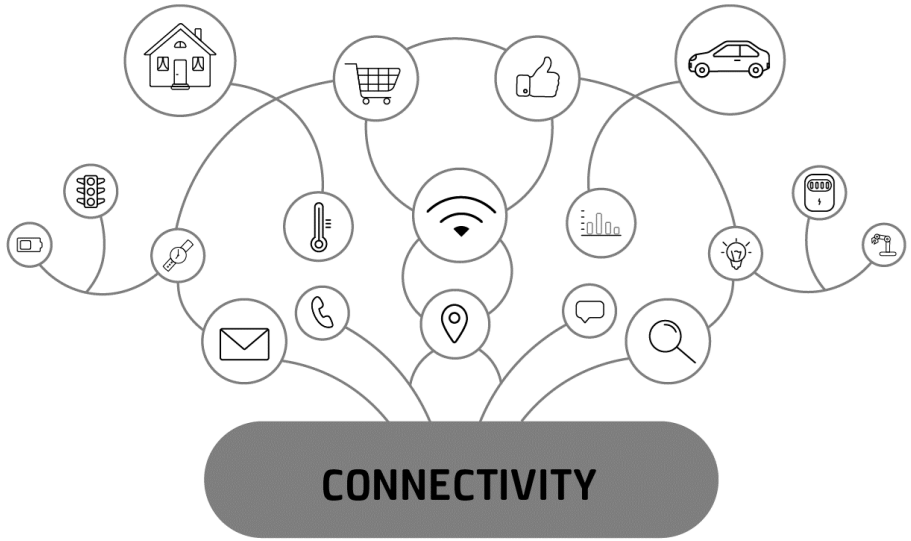
- IoT is not a single technology, it's a combination of technologies and domain knowledge.
- As a result, engineers from different domains have to work together for building a complete IoT product.

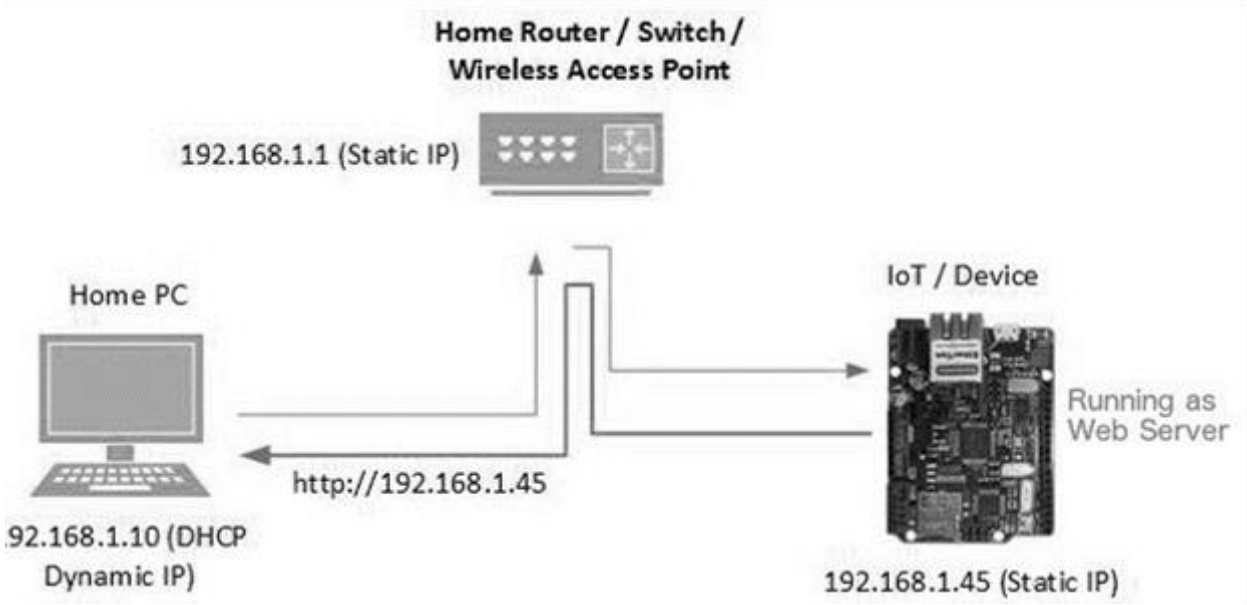


- Life would be governed entirely by Internet and IoT in the near future.

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.

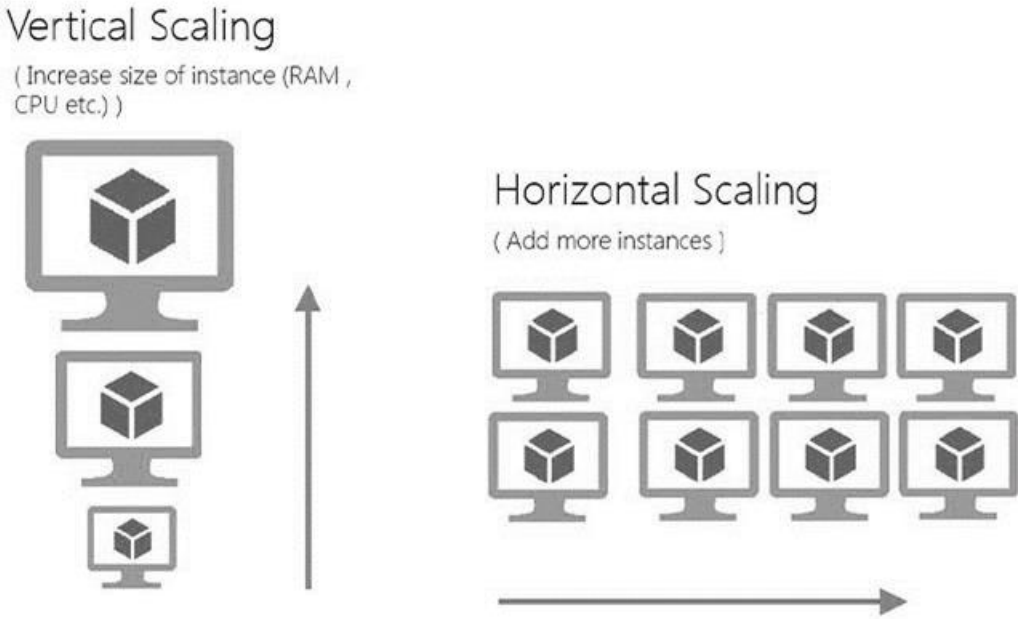




- Identity:
  - Each IoT device has a unique identity (e.g., an IP address).
  - This identity is helpful in communication, tracking and to know status of the things.

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

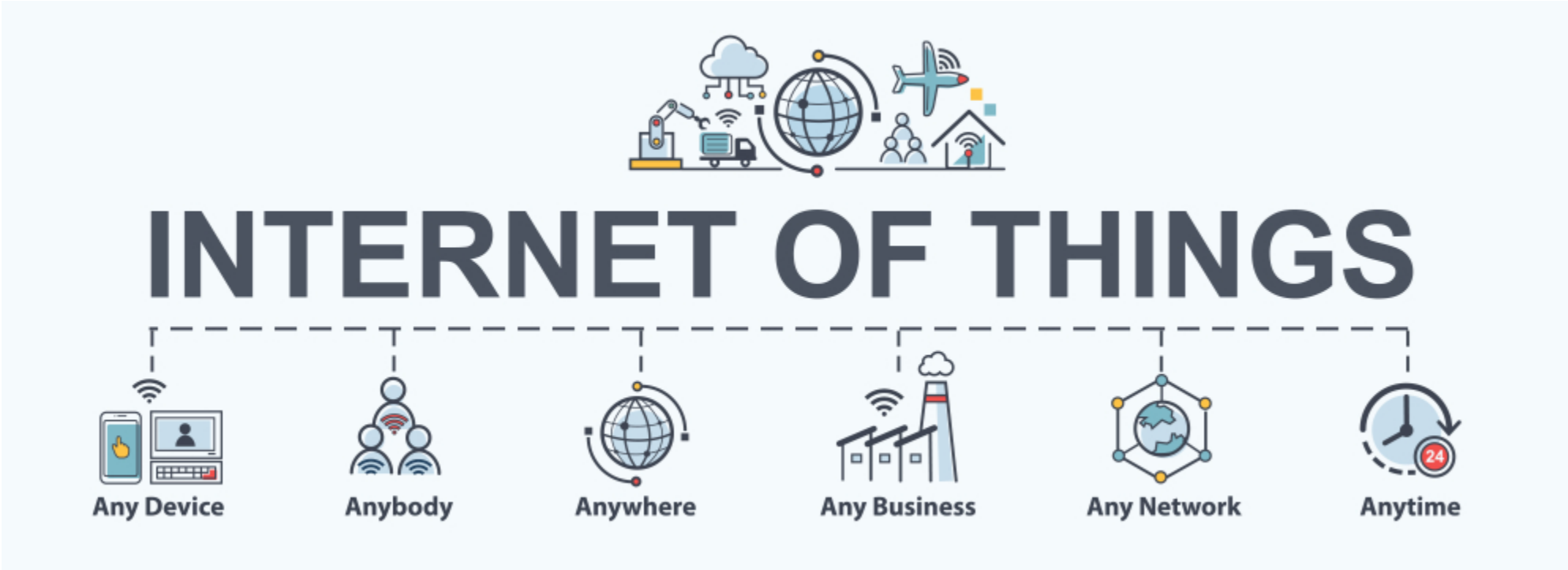
- Dynamic and self-adapting (complexity):
  - IoT devices should dynamically adapt themselves to the changing surroundings.
  - For example surveillance camera. It should be flexible to work in different weather conditions and different light situations (morning, afternoon, or night).

Characteristics of IoT

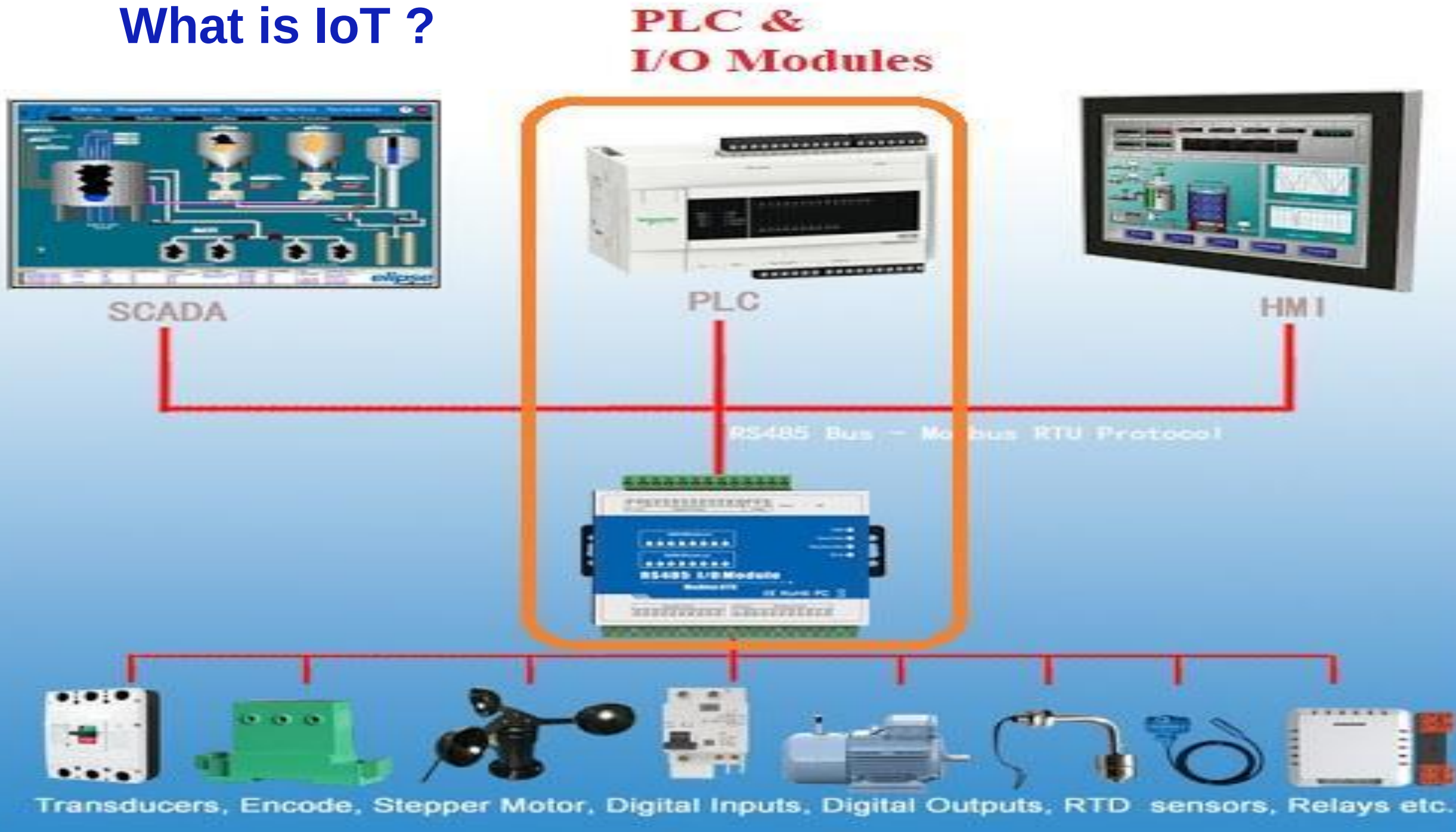
- Safety:
  - Sensitive personal details of a user might be compromised when the devices are connected to the Internet.
  - So data security is a major challenge.
  - This could cause a loss to the user.
  - Equipment in the huge IoT network may also be at risk.
  - Therefore, equipment safety is also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

What is IoT ?

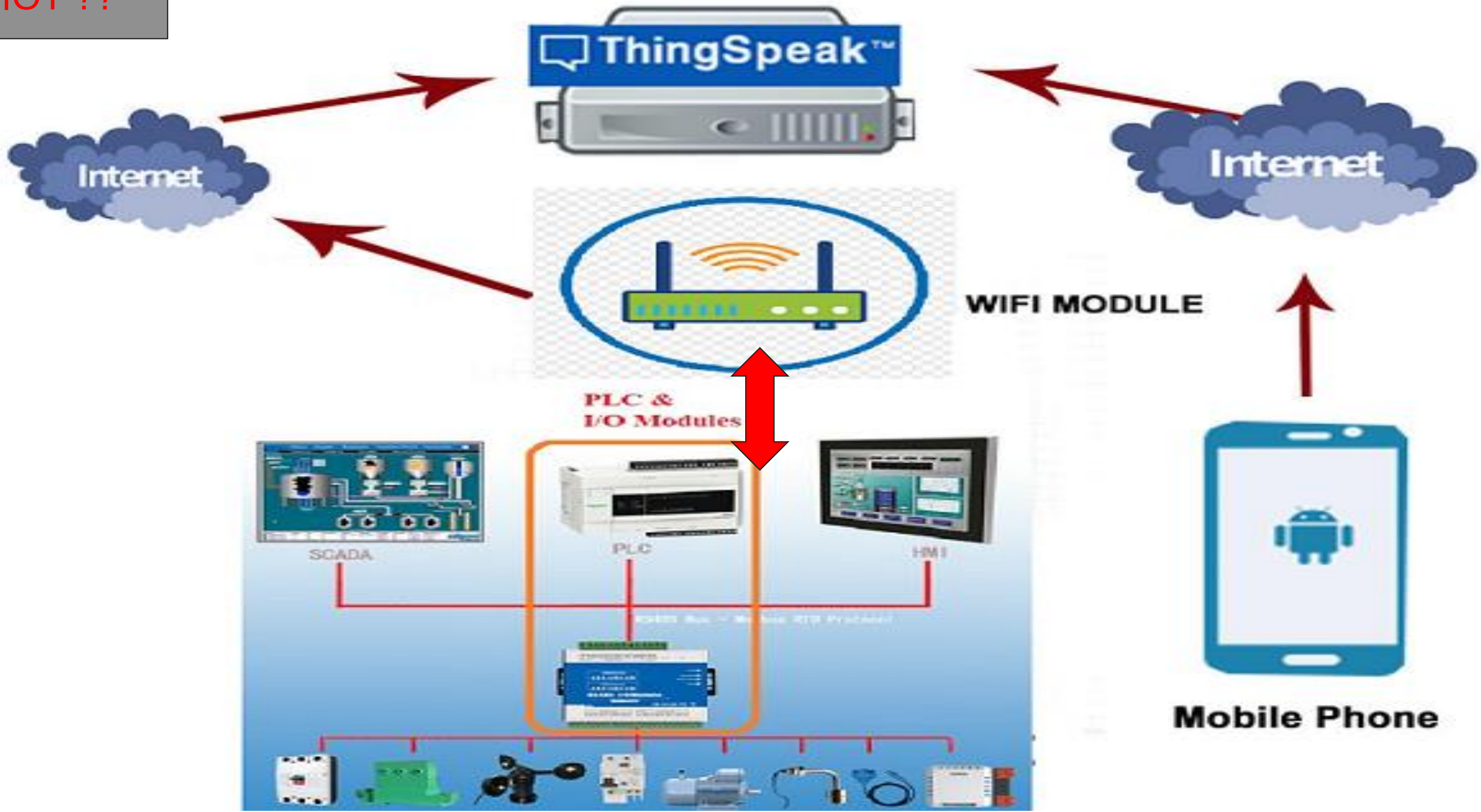
Cyber physical embedded systems using which we can control anything from anywhere.



What is IoT ?

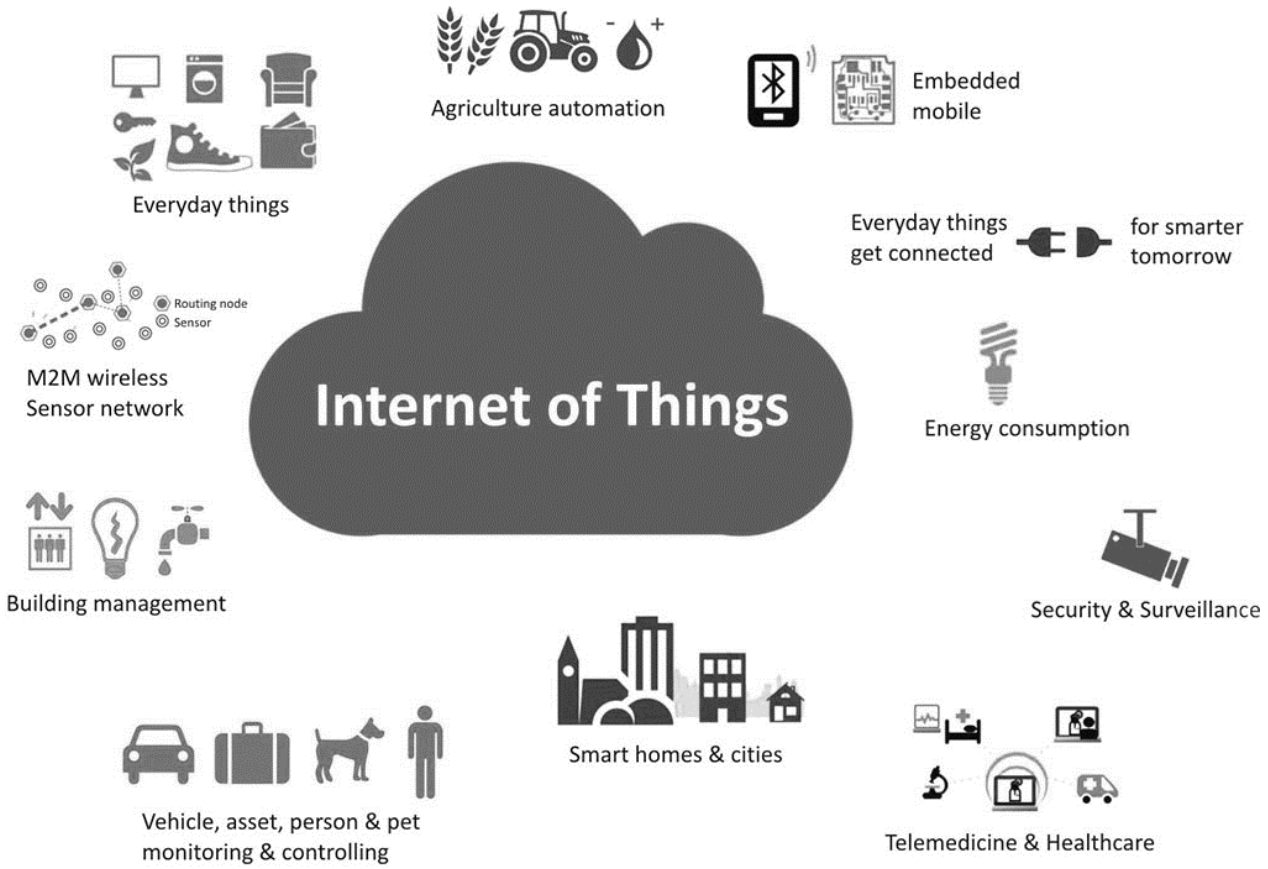

PLC &
I/O Modules
SCADA
PLC
HMI
RS485 Bus – Modbus RTU Protocol
Transducers, Encode, Stepper Motor, Digital Inputs, Digital Outputs, RTD sensors, Relays etc.

IIOT ??


ThingSpeak™
Internet
Internet
WIFI MODULE
PLC &
I/O Modules
SCADA
PLC
HMI
Mobile Phone

Application areas of IoT

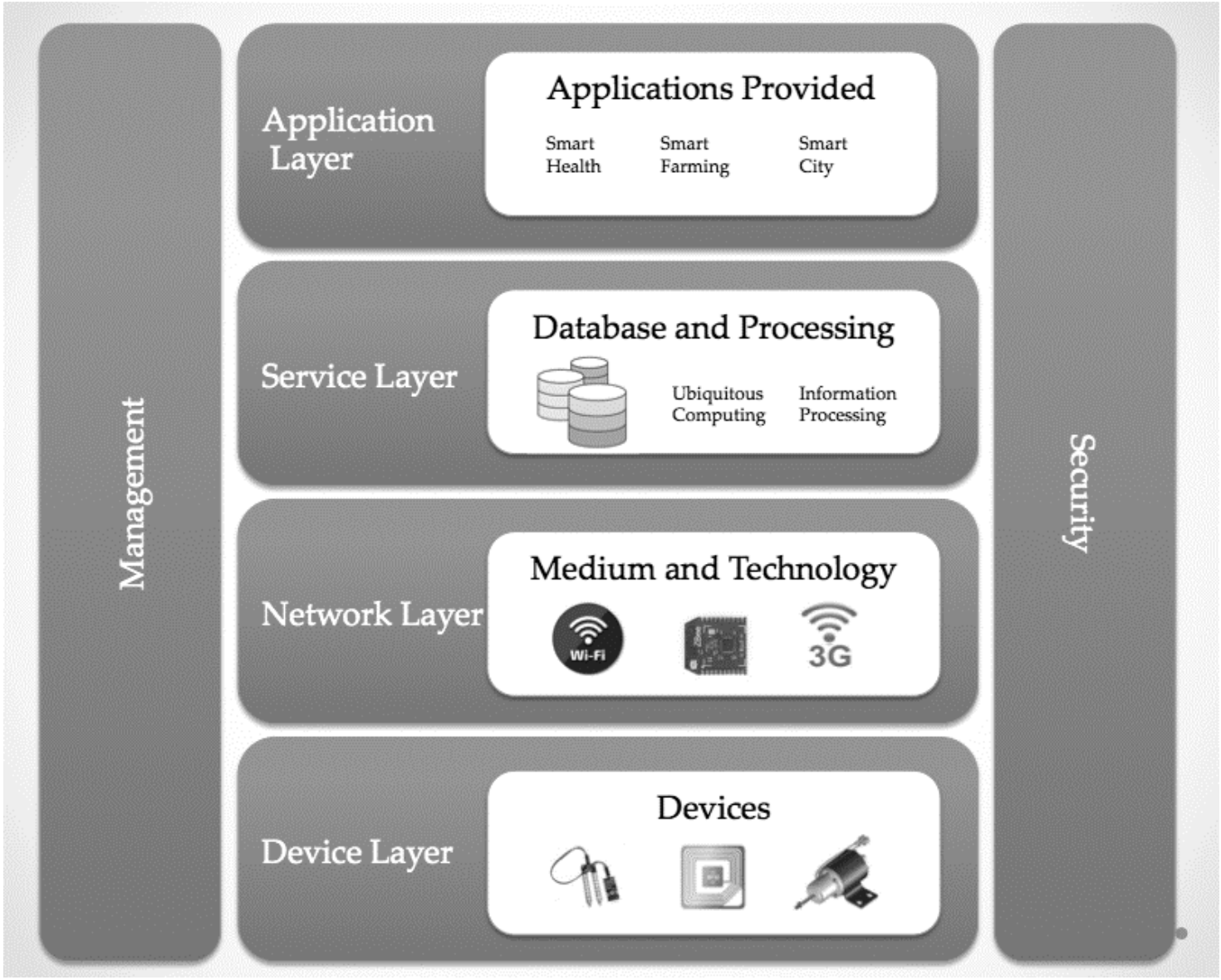
- The scope and application areas of IoT is very huge.
- IoT can be used to build applications for…



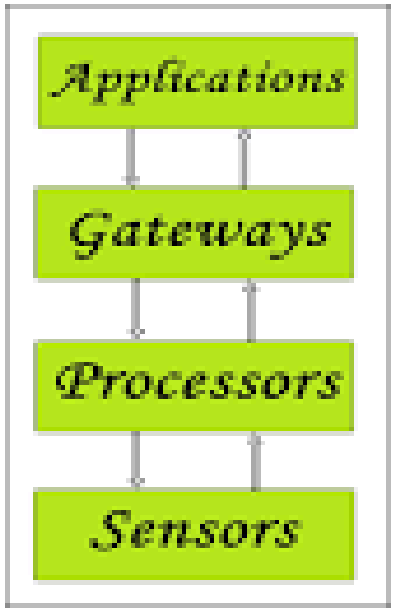
- Agriculture
- Assets Tracking
- Energy Sector
- Defense
- Embedded Applications
- Education
- Waste Management
- Healthcare Products
- Telemedicine
- Safety And Security Sector
- Smart City Applications etc.

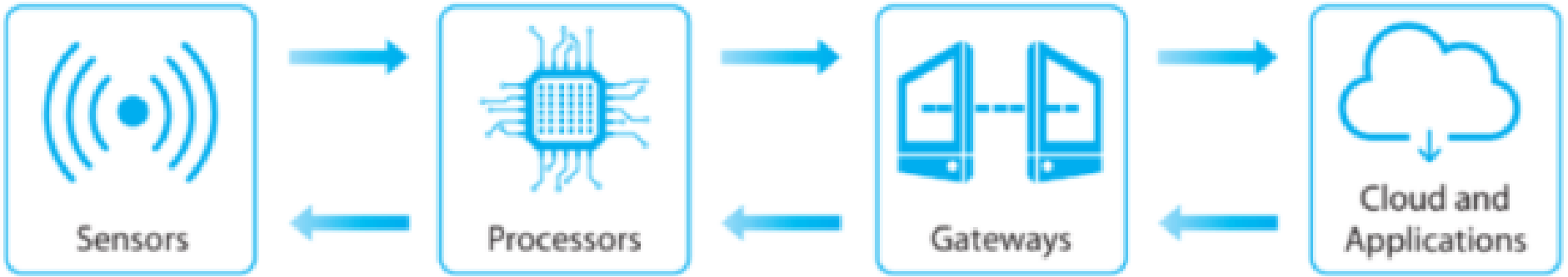
IOT Architecture

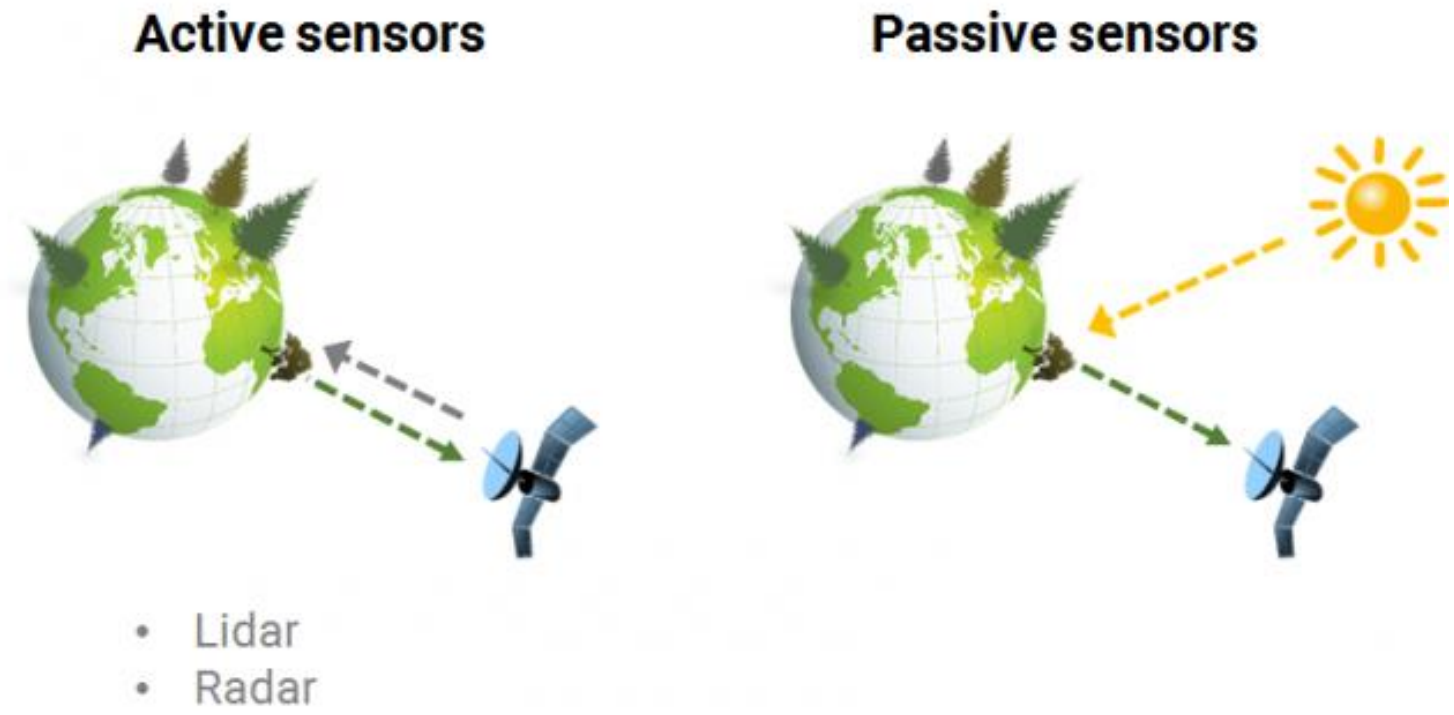
- Architecture:
  - IoT architecture is yet not uniformed and standardized.
  - It should be hybrid, supporting different manufacturer's products to function in the IoT network.



Functional Block of IOT Architecture







- **Active Sensors:**

1. **Radar**: Emits radio waves and measures the reflected signals to detect objects and determine their distance, speed, and other characteristics.
2. **Lidar (Light Detection and Ranging)**: Uses laser pulses to measure distances and create detailed 3D maps of the environment

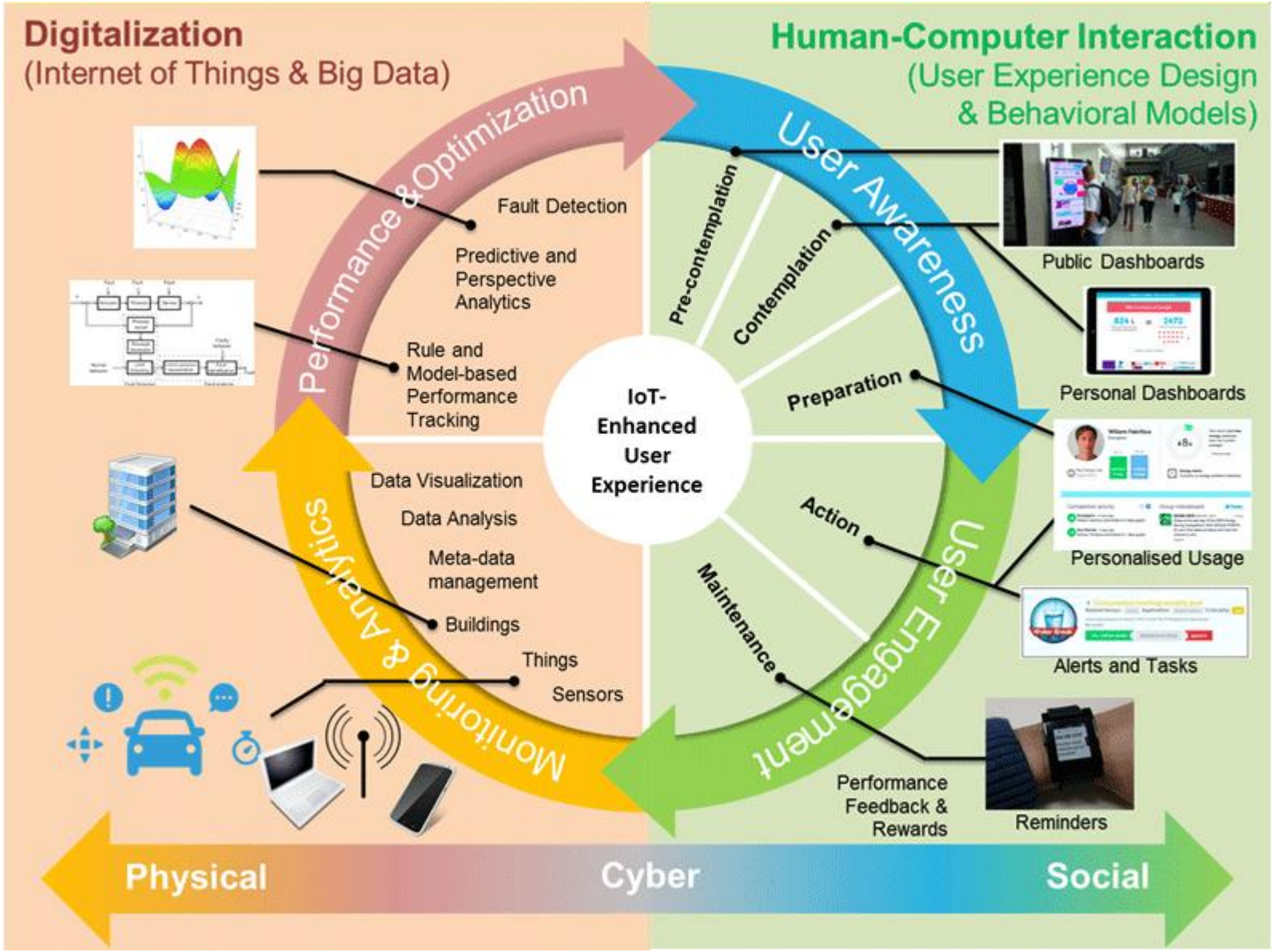
- **Passive Sensors:**

1. **Photovoltaic cells (solar cells)**: Convert light into electrical energy without needing an external power source.
2. **Thermocouples**: Generate a voltage in response to a temperature difference.
3. **Microphones**: Convert sound waves into electrical signals.
4. **Accelerometers**: Measure changes in motion or orientation by detecting the forces exerted on a mass.

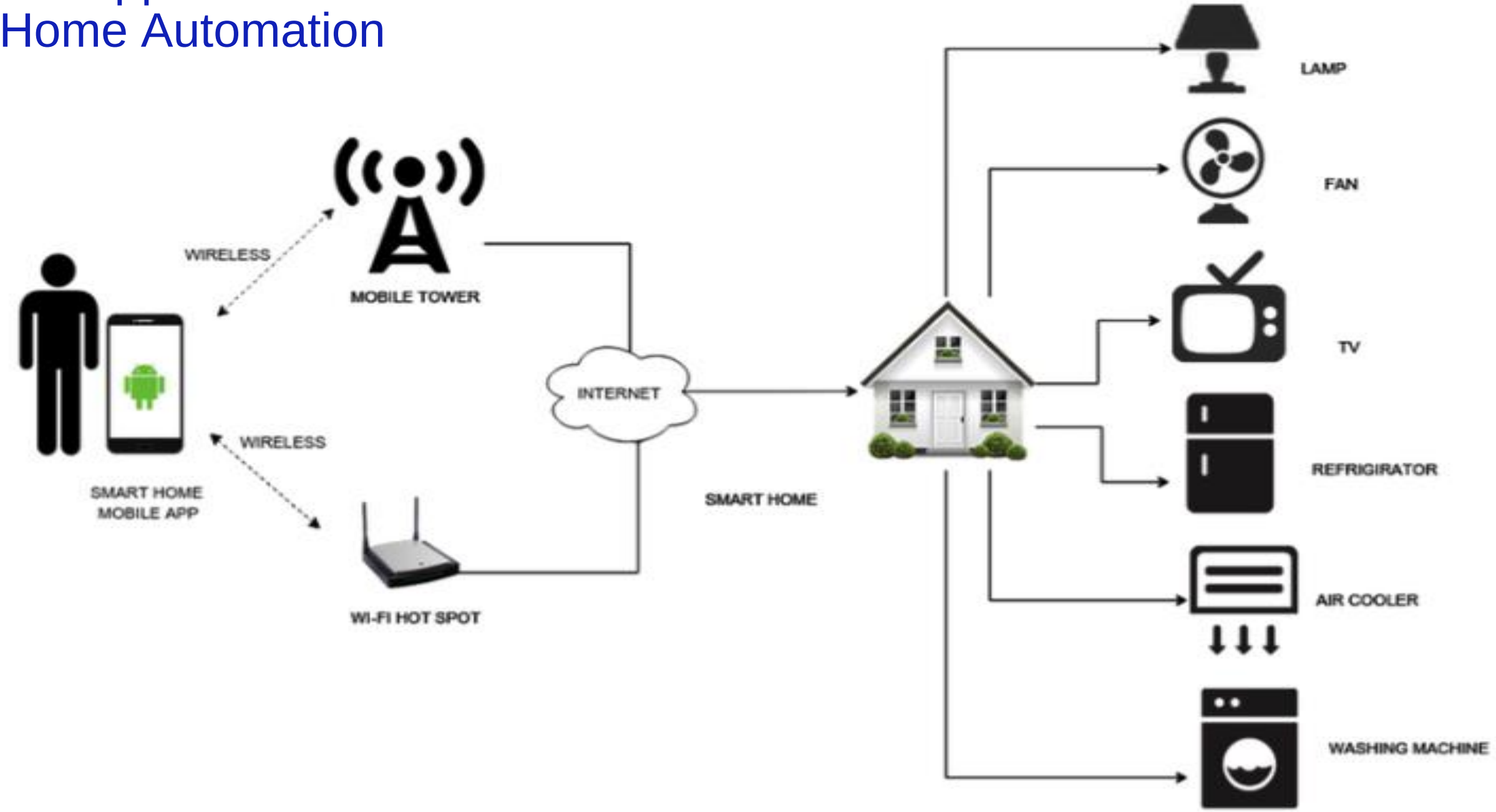
The architecture of IoT components:

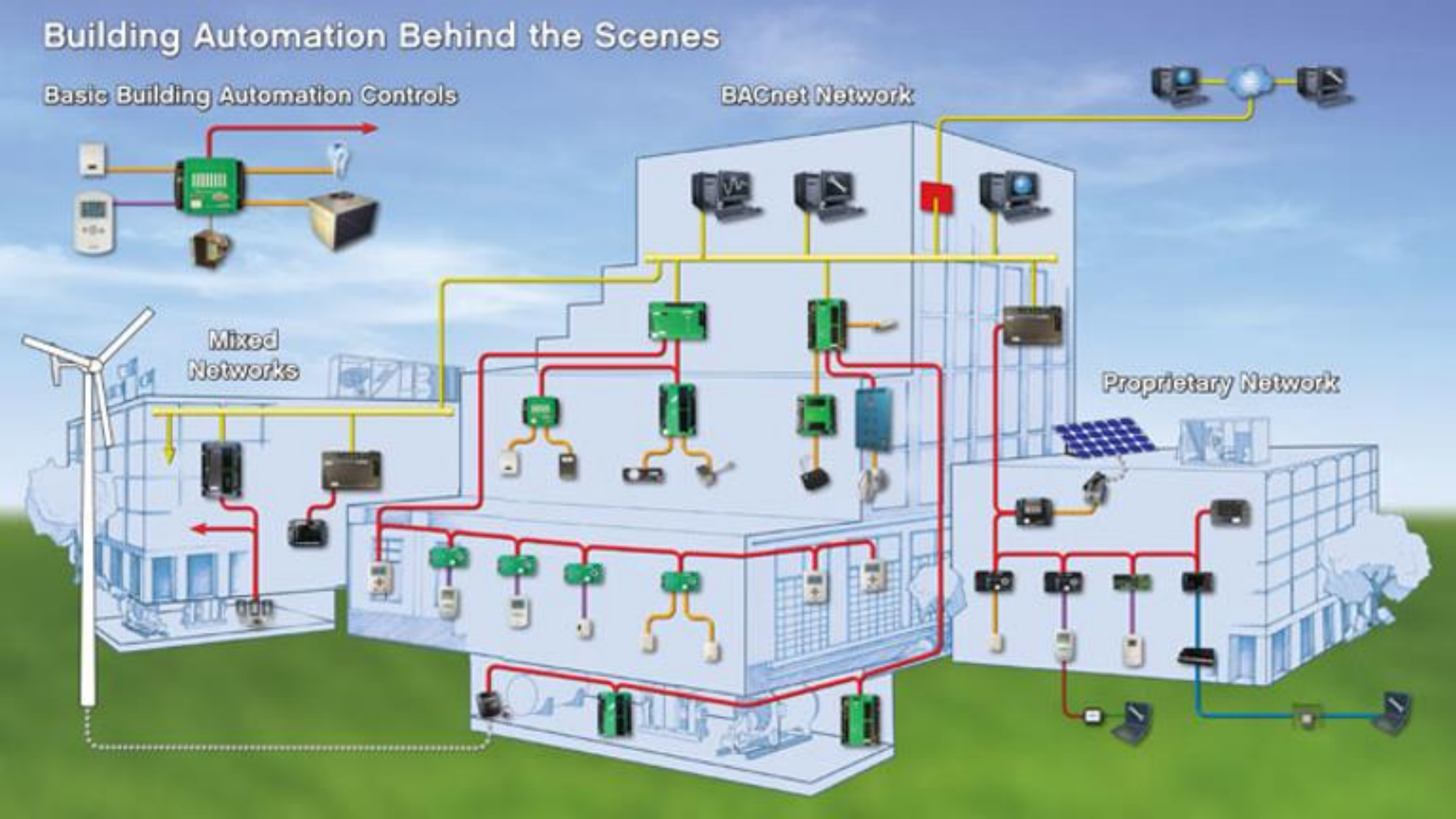
- **Sensors** convert a non-electrical input to an electrical signal.
- **Processors** are the brain, the main part of the IoT system. They process the raw data captured by the sensors and extract valuable information. Examples of processors are microcontrollers and microcomputers.
- **Gateways** are the combination of hardware and software used to connect one network to another. Gateways are responsible for bridging sensor nodes with the external Internet or World Wide Web.
- **Applications** provide a user interface and effective utilization of the data collected. The figure above illustrates some examples of IoT applications.

Application areas of IoT

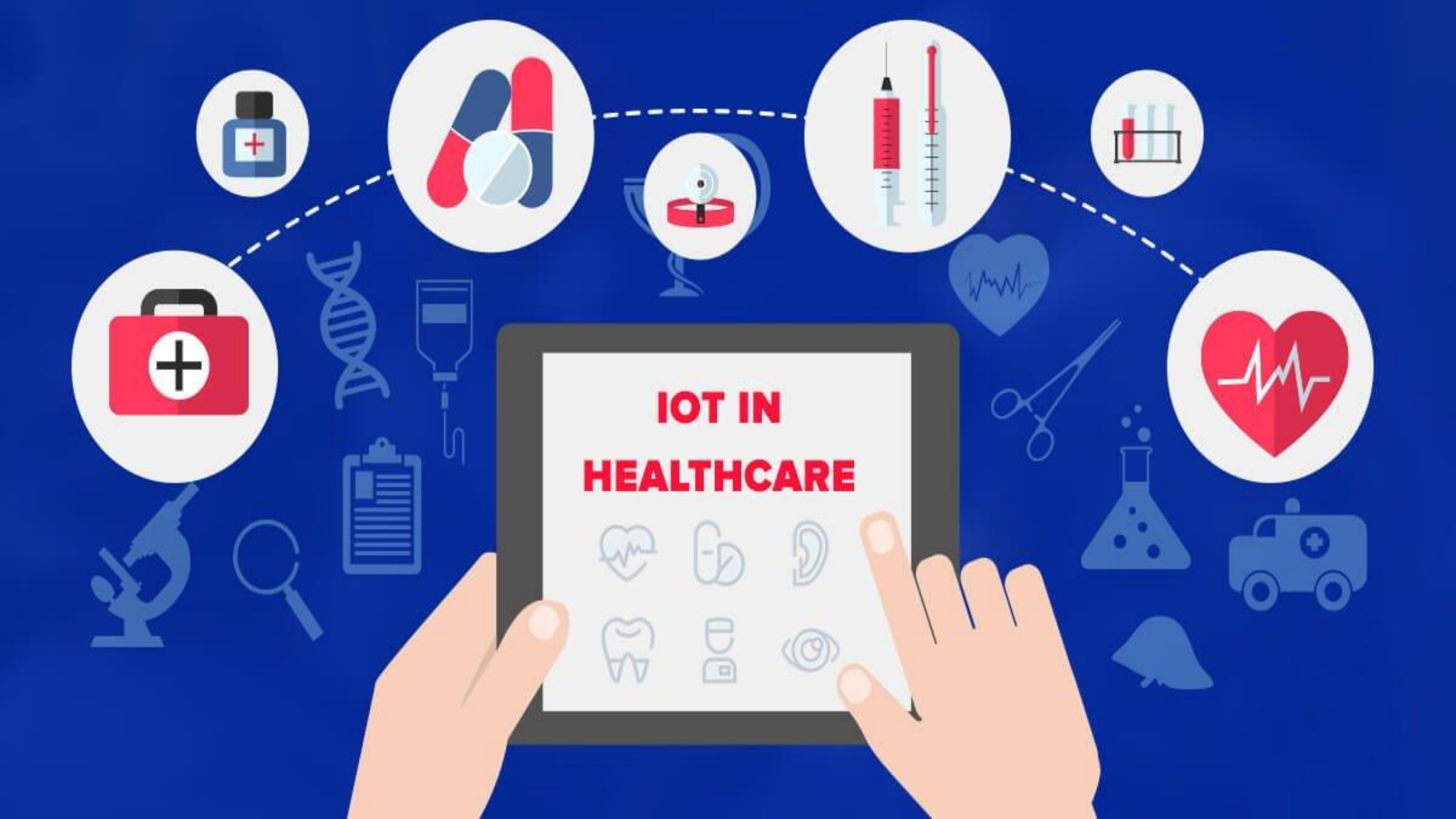


IoT Applications : Home Automation




Building Automation Behind the Scenes
Basic Building Automation Controls
BACnet Network
Mixed Networks
Proprietary Network

Industrial IoT (IIoT) Systems:


IOT IN
HEALTHCARE

Advantages of IoT in healthcare

Lower expenses

Better treatment results

Better disease control

Fewer mistakes

More trust towards doctors

Medicines control

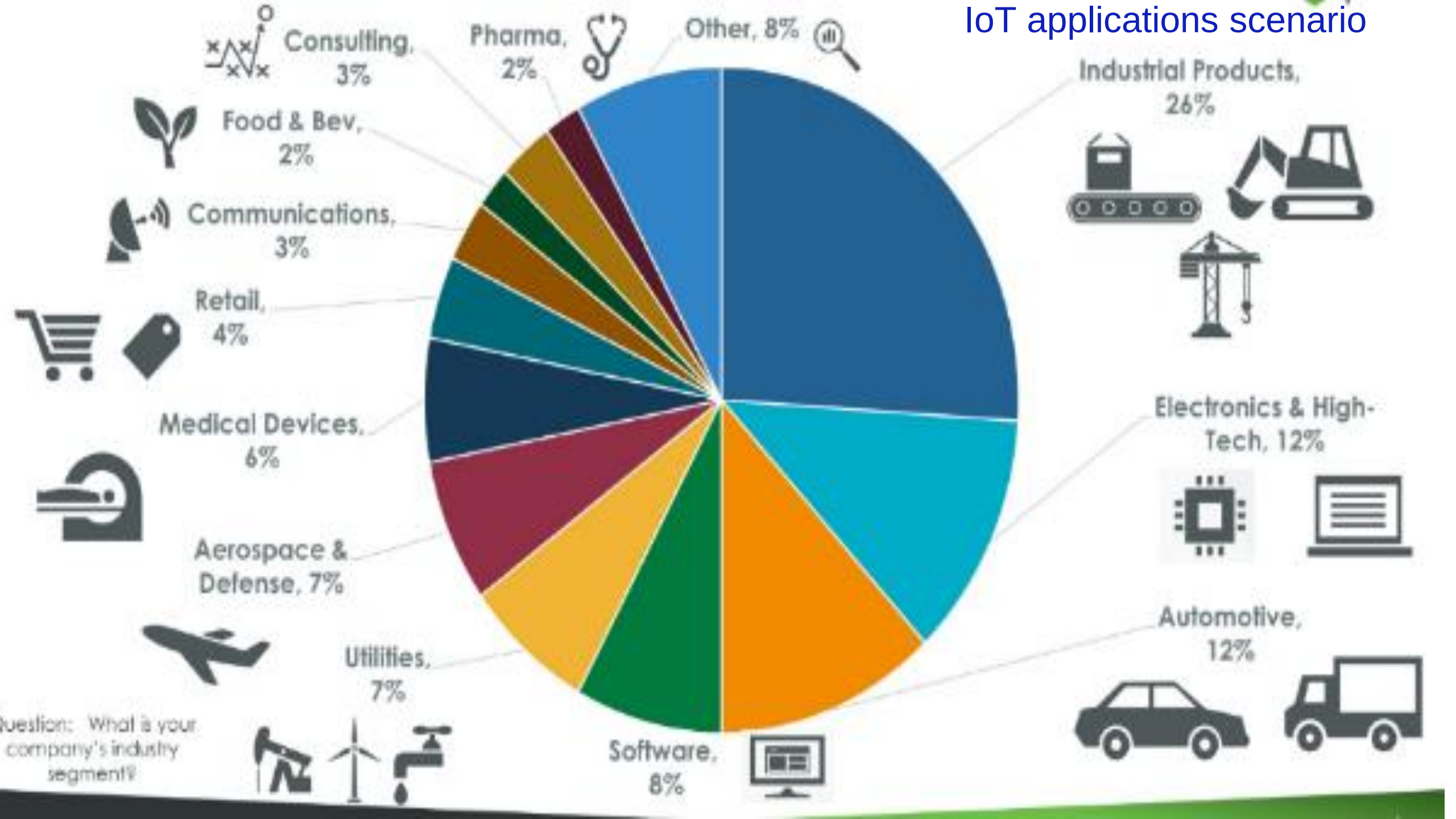
Better disease control

Maintenance of medical devices

IoT in healthcare

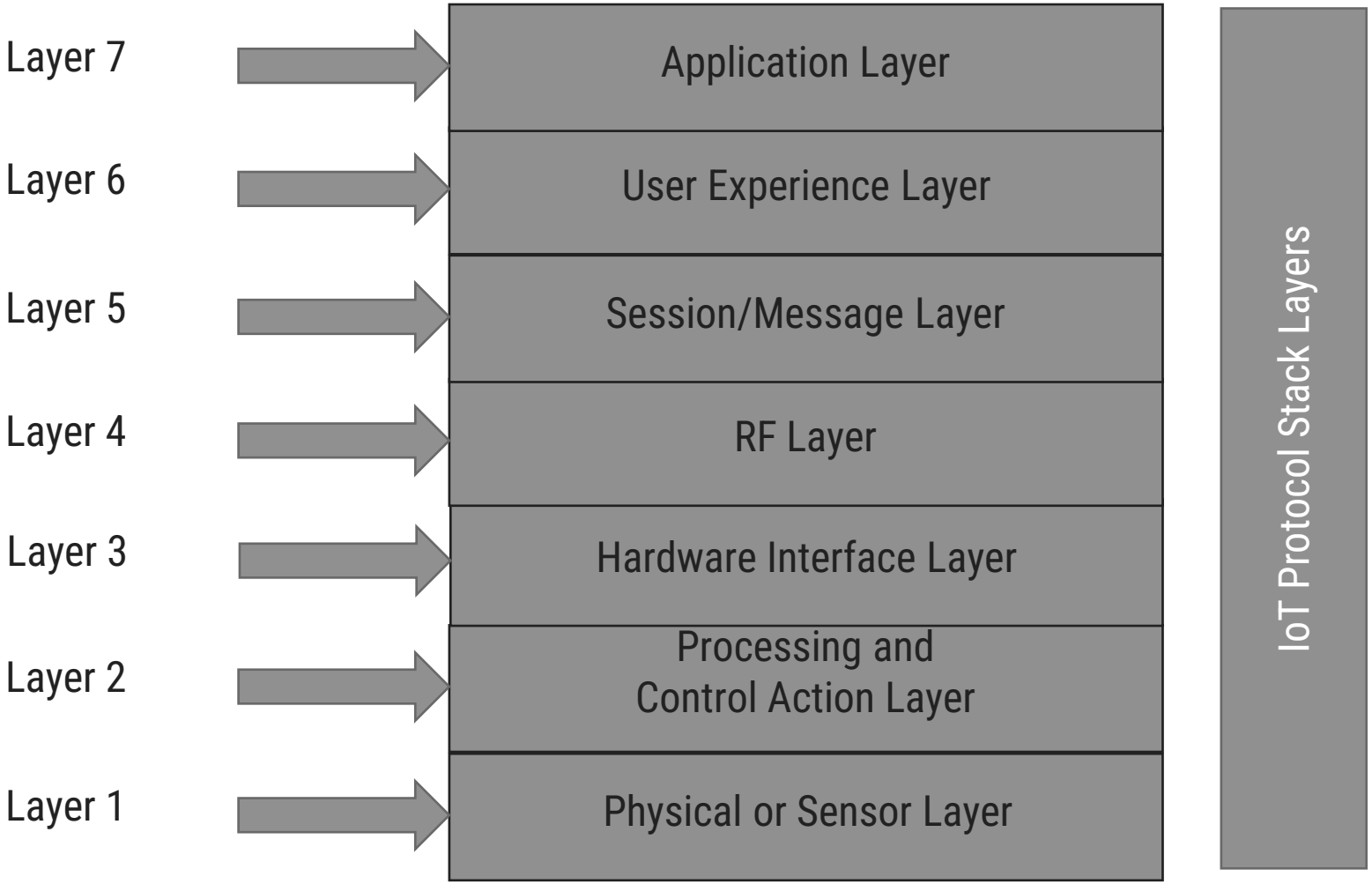
Robotic applications:

IoT applications scenario



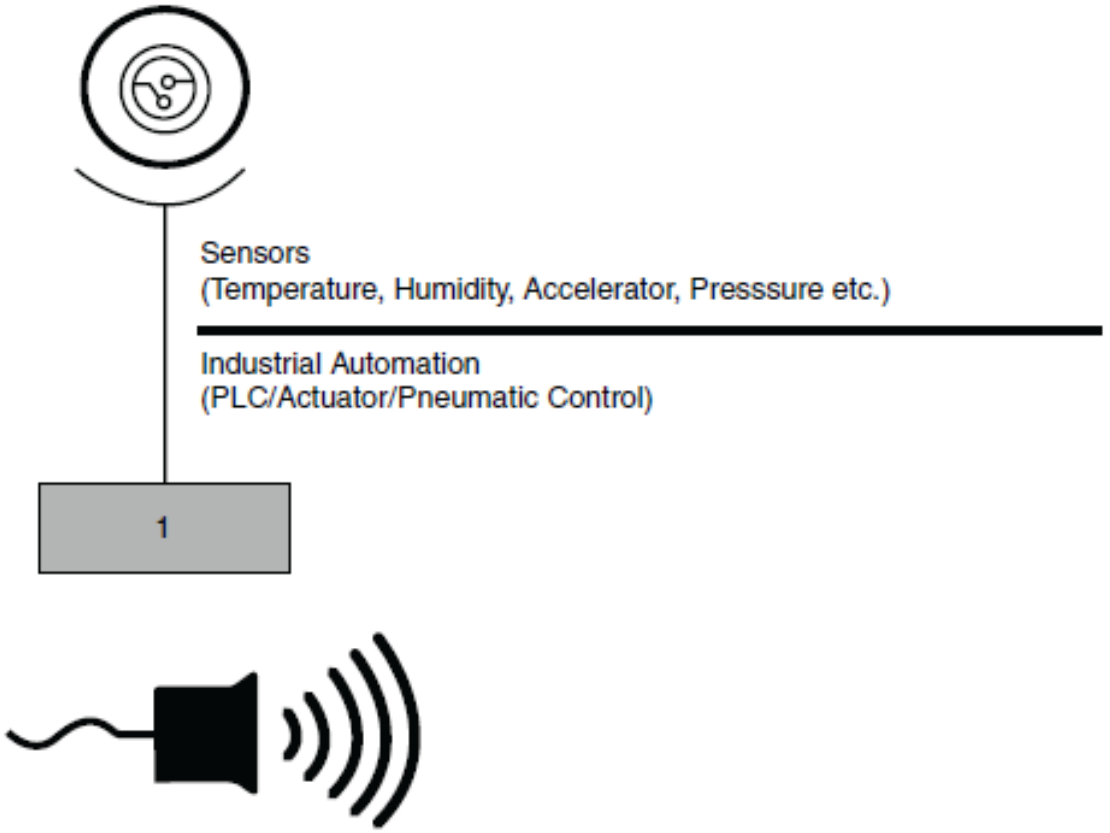
IoT Stack

- Like other digital technology IoT has stack layers.



IoT Stack - Layer 1 (Physical or Sensor Layer)

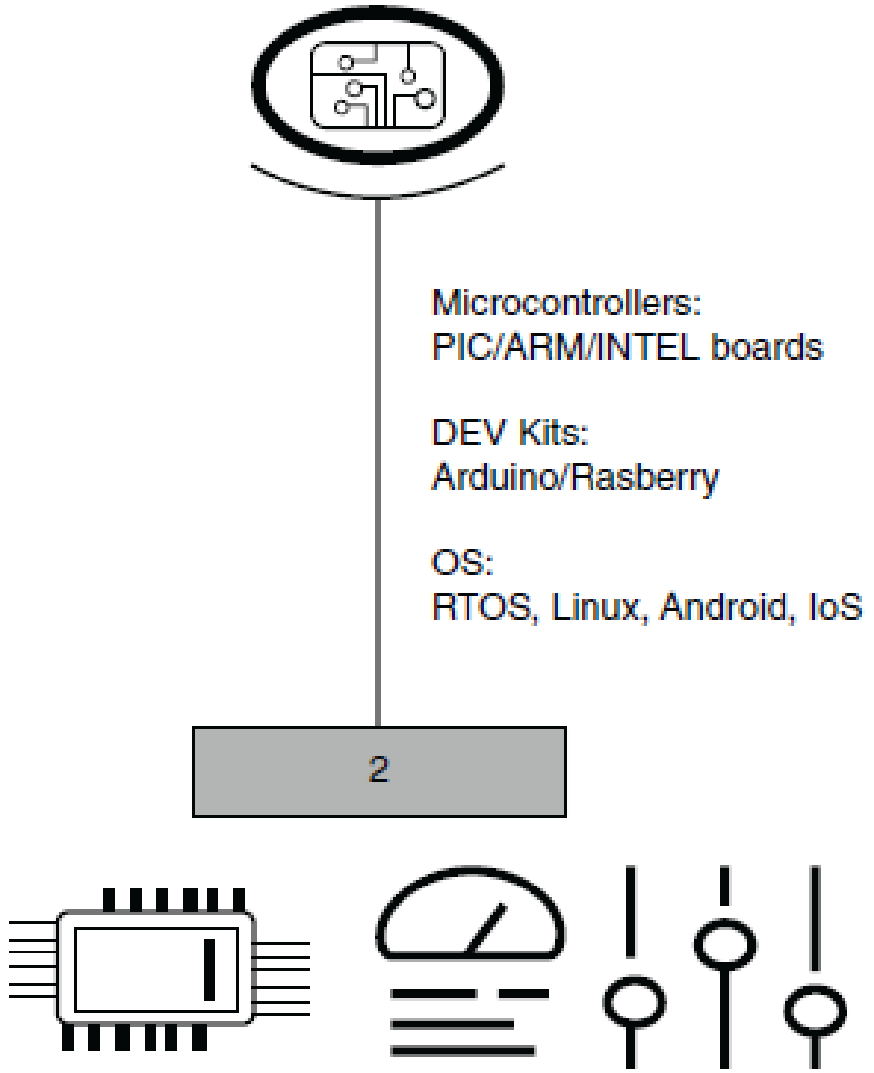
- This layer is concerned about the physical components, which mainly includes sensors.
- In this layer, the sensors are the core component.
- In industrial automation, PLC, actuator, etc. are considered as physical layer components.
- This layer is responsible for data collection and action execution.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



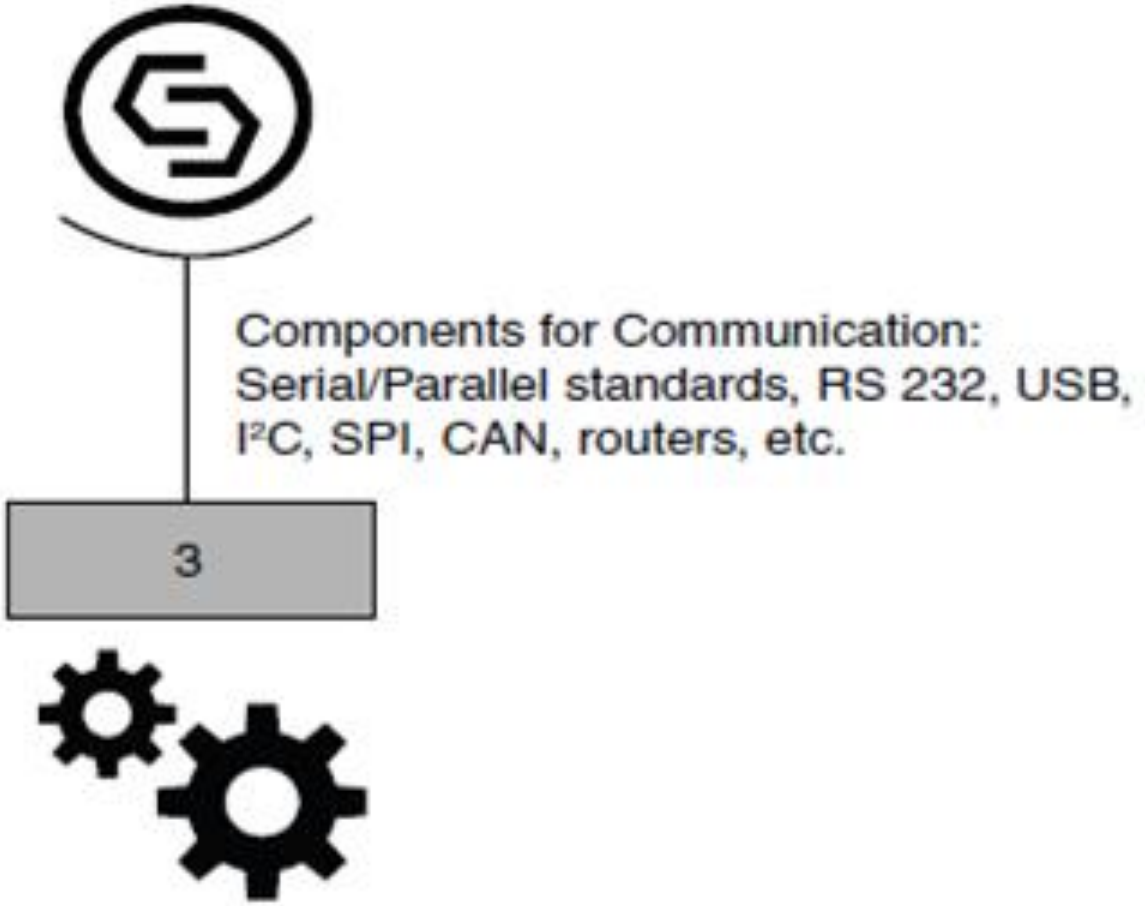
Layer 1: Sensor layer (physical layer); data collection happens here.

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.

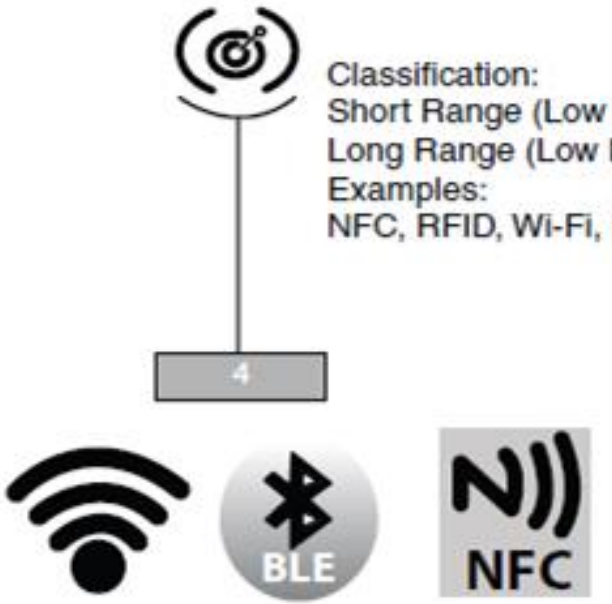


IoT Stack - Layer 3 (Hardware Interface Layer)



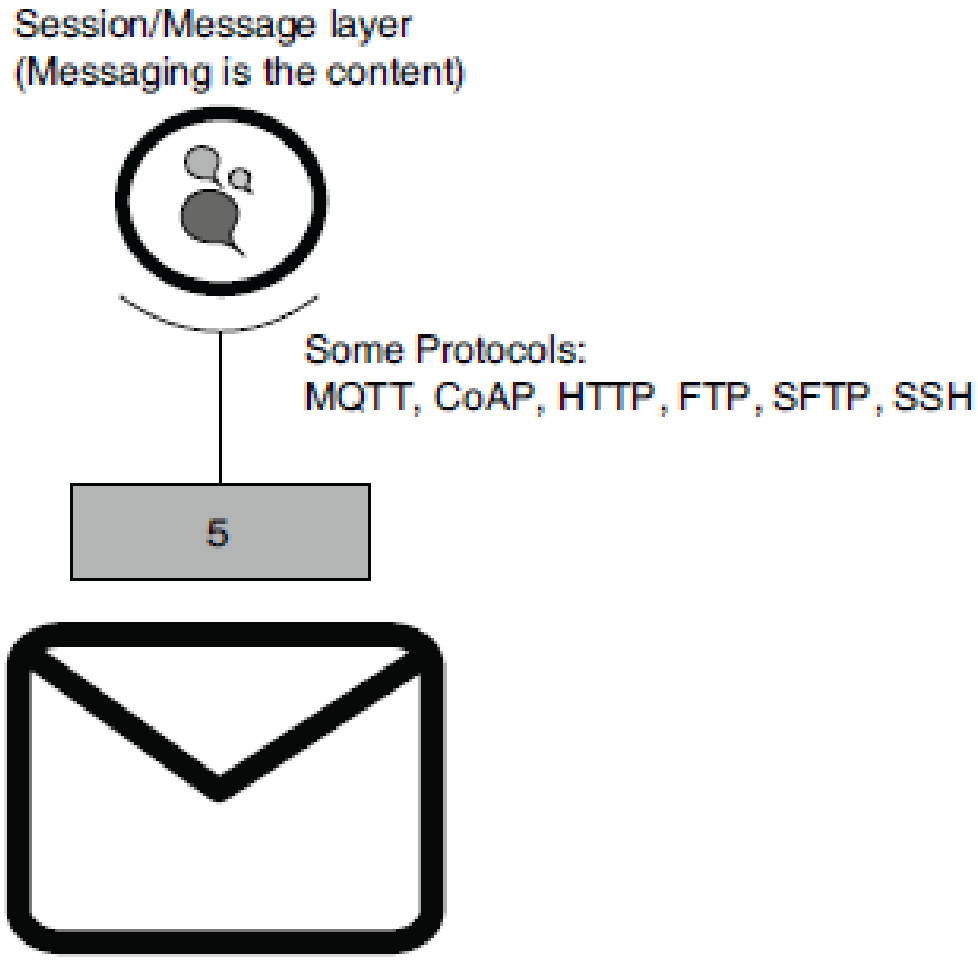
- The 3rd layer in the stack is the Hardware Interface Layer.
- Hardware components and communication standards such as RS232, CAN, SPI, SCI, I2C, etc. occupy this layer.
- All these components ensure flawless communication
- Handshake happens here.

IoT Stack - Layer 4 (RF Layer)



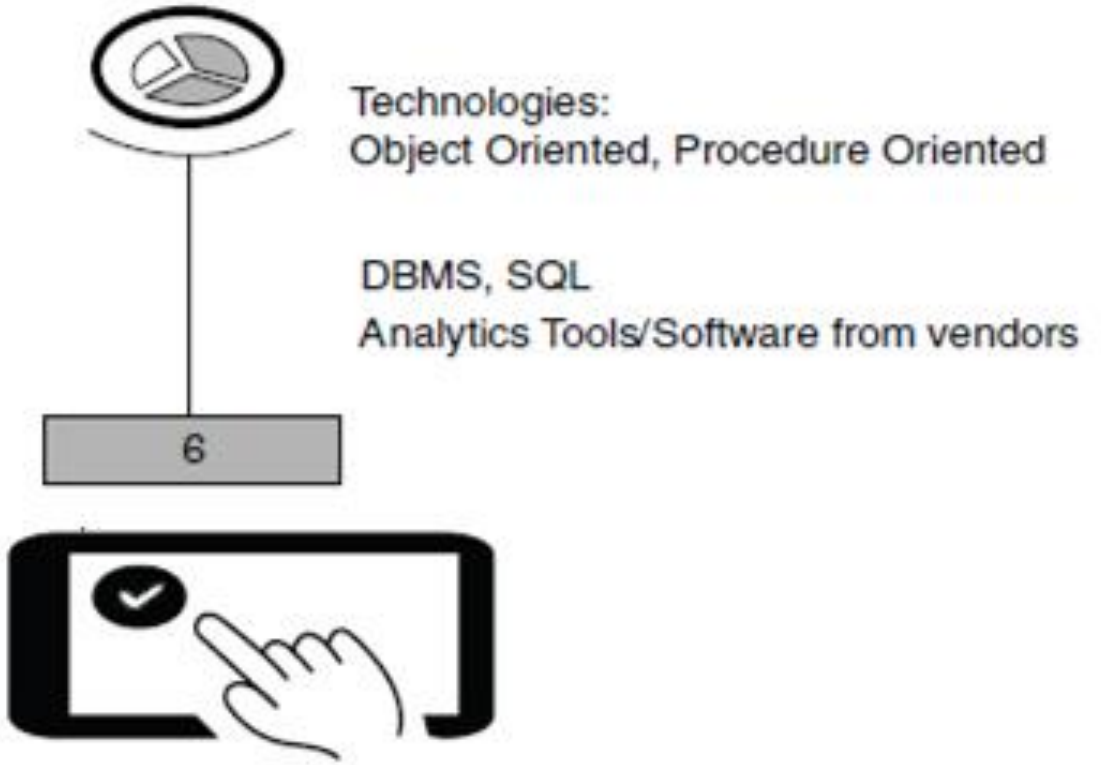
- Whenever one talks about IoT, RF is discussed and comes in picture.
- It plays a major role in the communication channel – whether it is short range or long range.
- Protocols used for communication and transport of data based on RF are listed in this layer.
- Some famous and common protocols are Wi-Fi, 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)



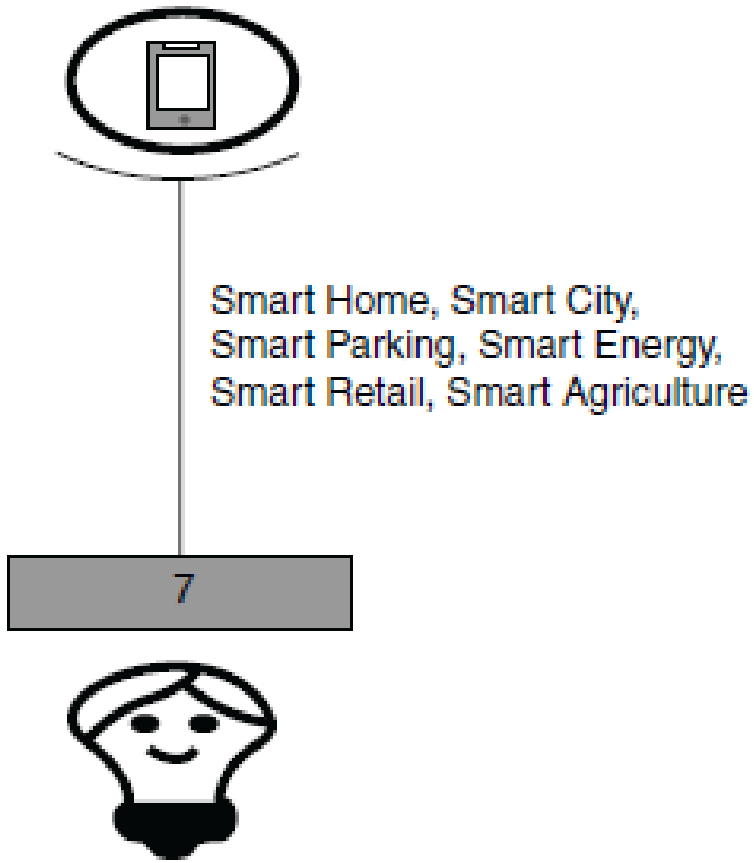
- Like computer network session management is also important in IoT.
- There are many protocols which manage how messages or data are broadcasted to the cloud.
- Layer 5 (session layer) deals with the various messaging protocols as MQTT, CoAP, etc. and also other protocols such as SSH and FTP.

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.

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

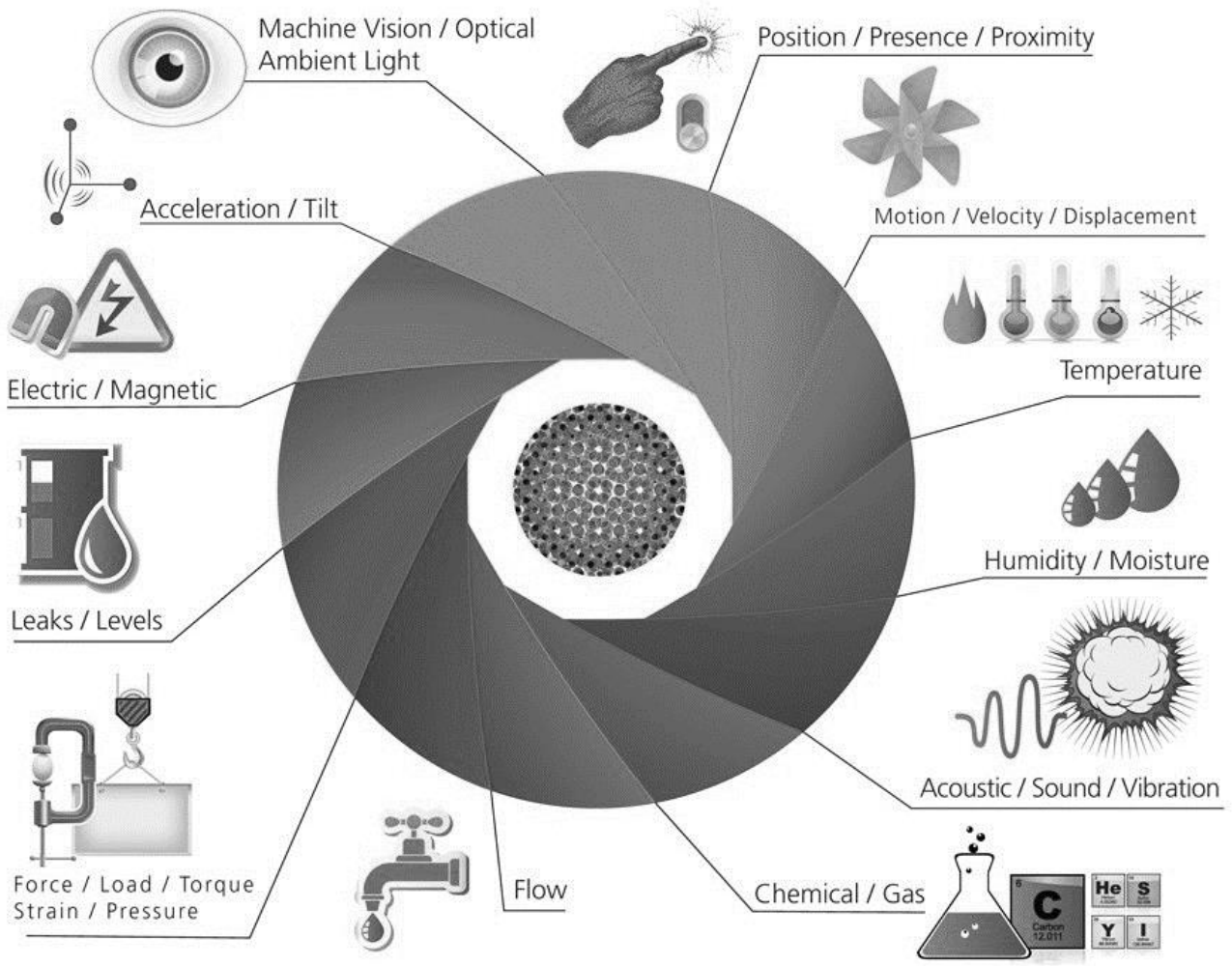
Vibration Index Sensor
Precisio 4mg
Range - 16 to 16g

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.

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.

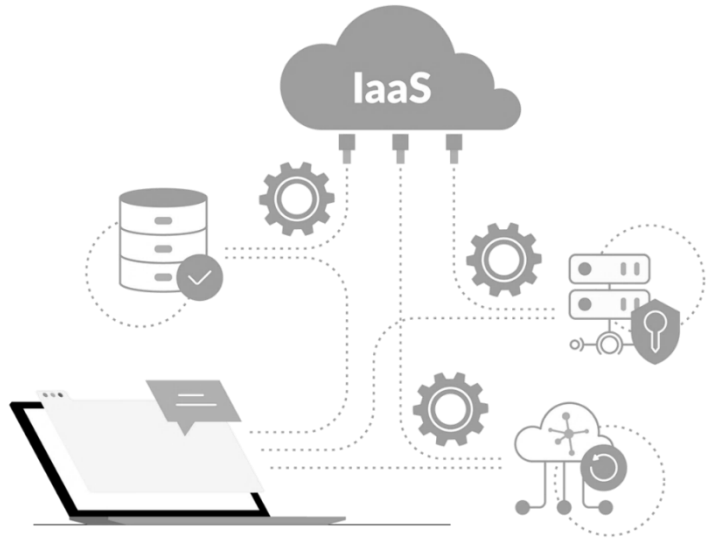


Enabling Technologies - Cloud Computing

- 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):

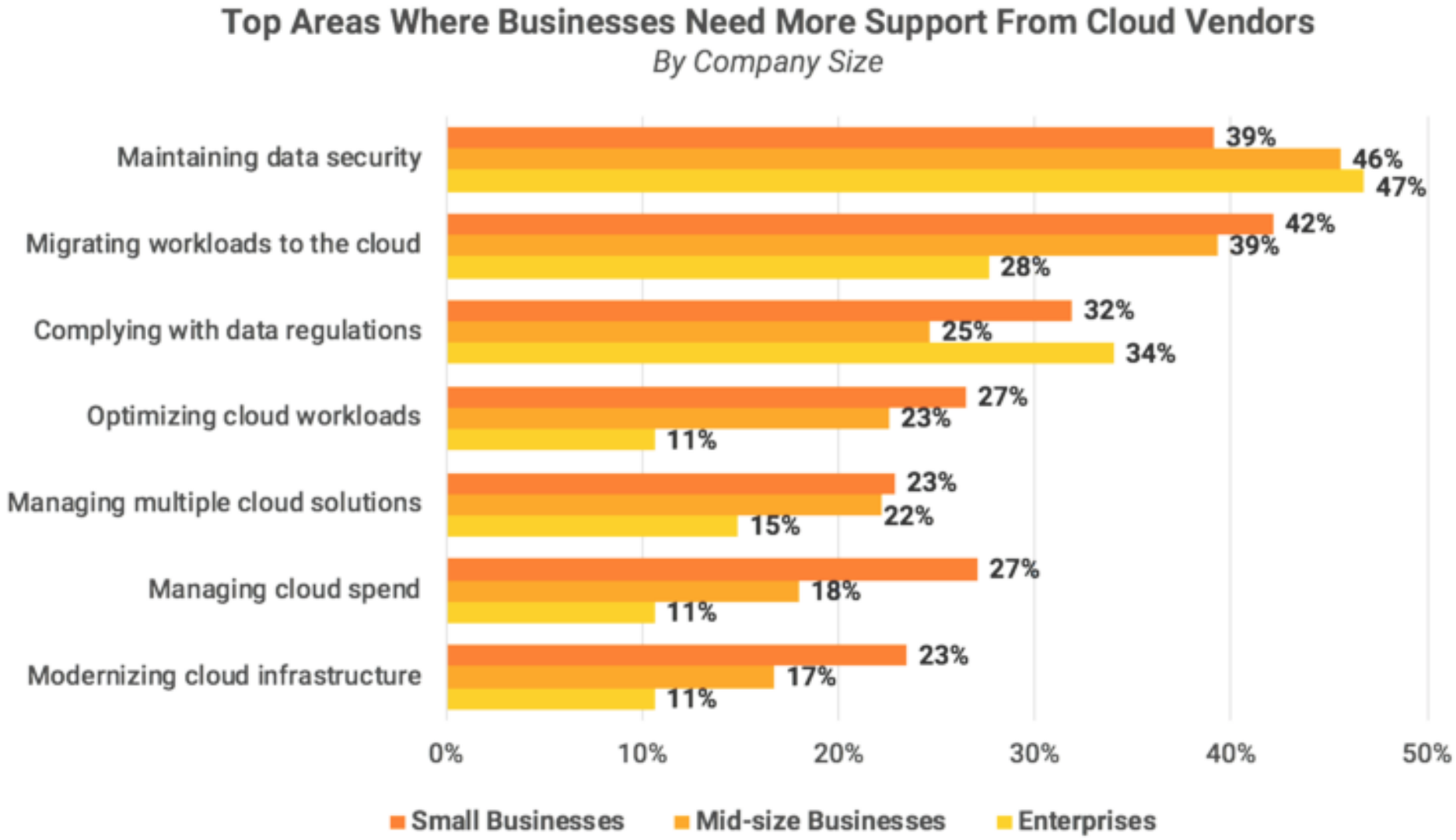
- This is a cloud computing model in which the cloud service provider delivers hardware and software tools needed for application development to users over the Internet.
- A PaaS provider hosts the hardware and software on its own infrastructure. Users have to build, manage and maintain the applications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

https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/

Enabling Technologies - Cloud Computing



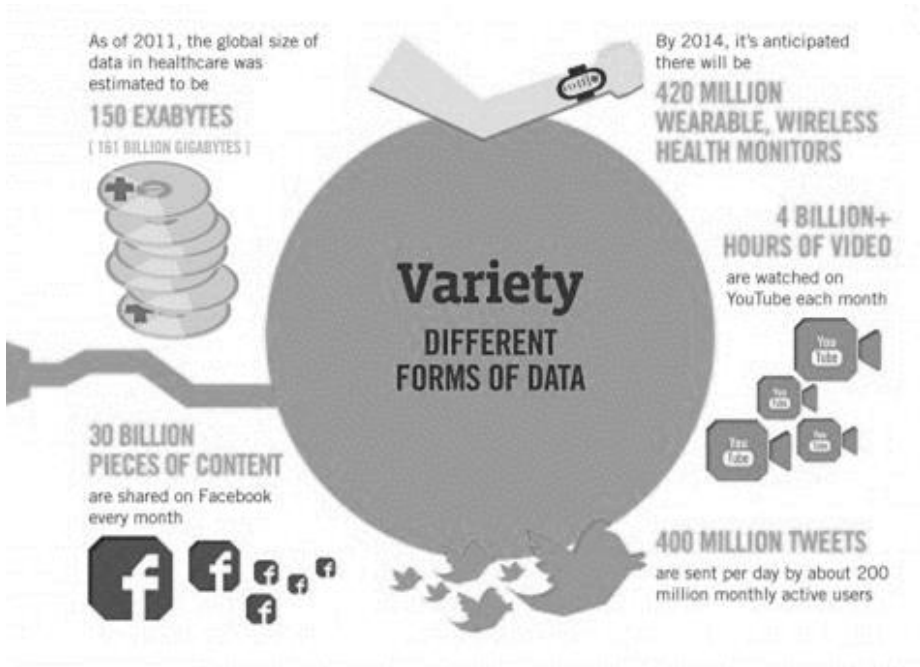
Enabling Technologies - Big Data Analytics

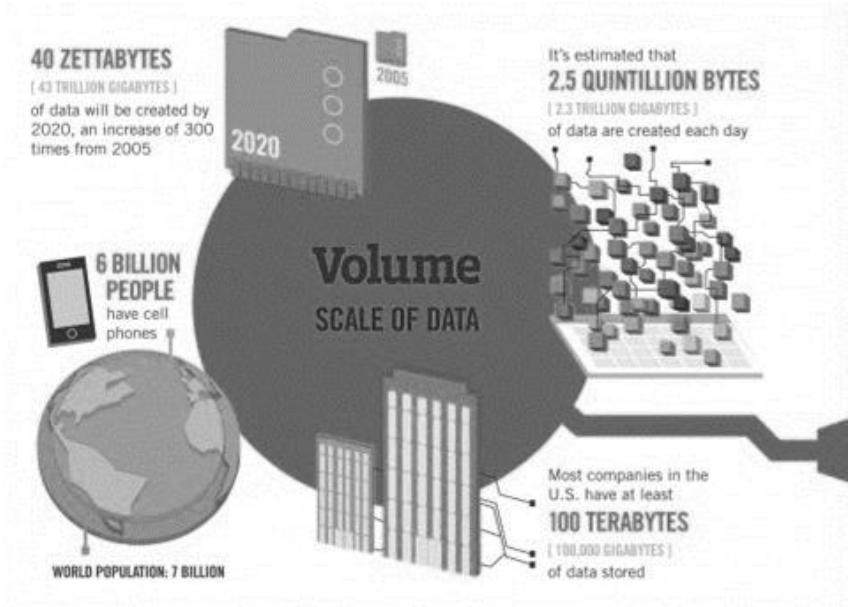
- Data is everywhere, and from every function or operation we get more data.
- IoT is all about collecting data from various sensory nodes.
- Handling the huge data is fundamental to make the application a success.
- The biggest challenge with big data is 4Vs.

https://www.datacenters.com/news/and-the-title-of-the-largest-data-center-in-the-world-and-largest-data-center-in#:~:text=But%20First%2C%20a%20Quick%20Journey,million%20square%20feet%20of%20space.

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.

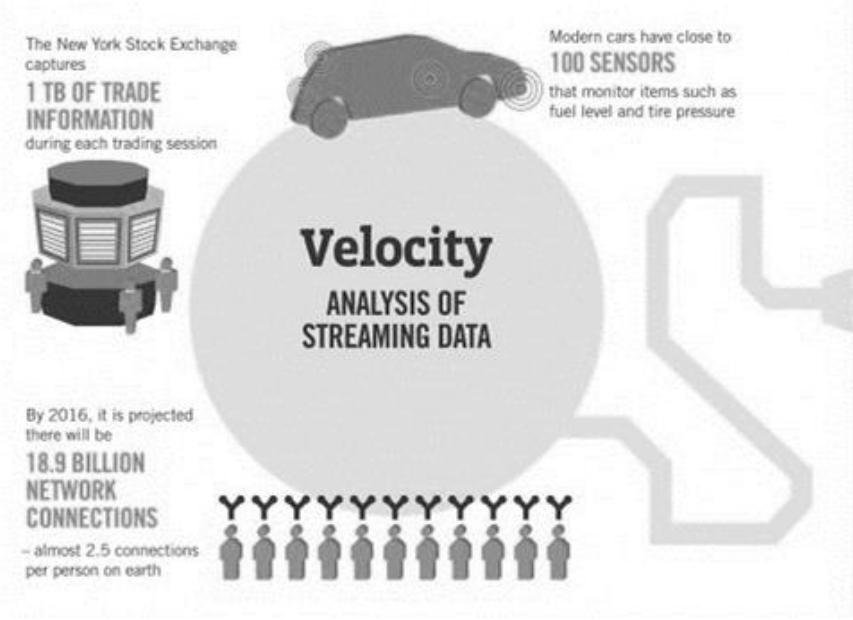


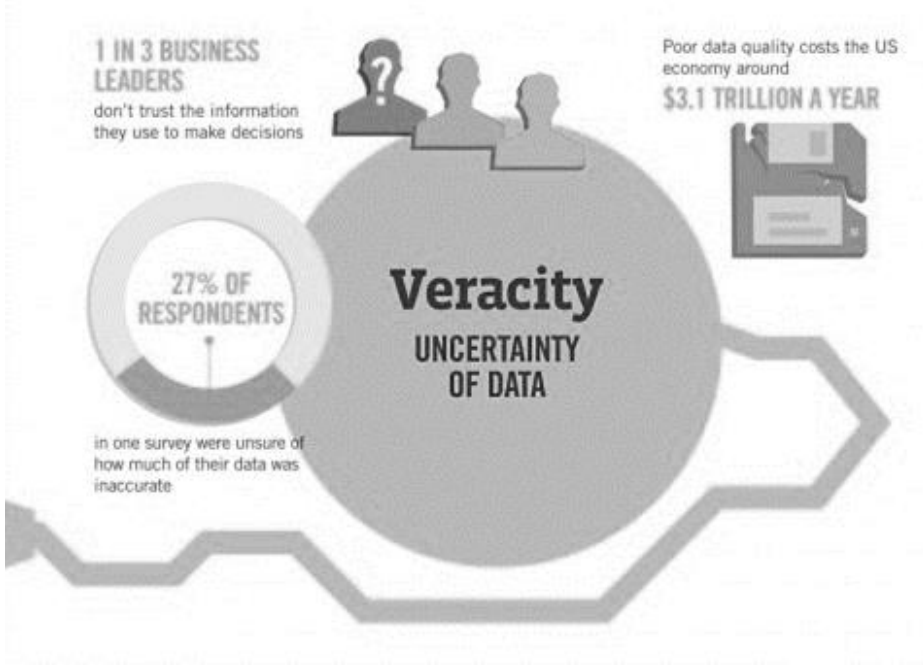


- Complexity (Variety):
  - Data no longer comes from one single source.
  - It also comes in different formats (e.g., audio, video, text and image) and has to be interpreted systematically.
  - Varieties of data becomes a huge challenge.

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.

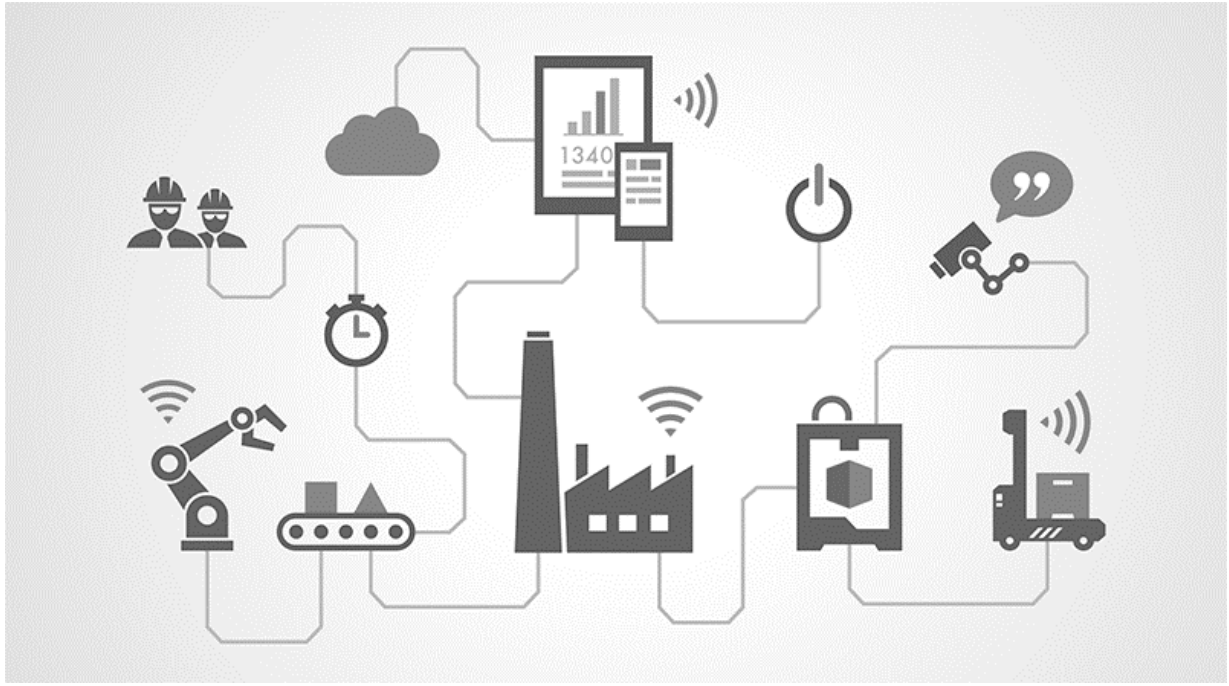




- Data in doubt (Veracity):
  - How accurate is all this data anyway?
  - Because we are now rely on it
  - The data's nature alters dynamically and uncertainty is often seen.
  - So, it would be challenging to process this unstable data.

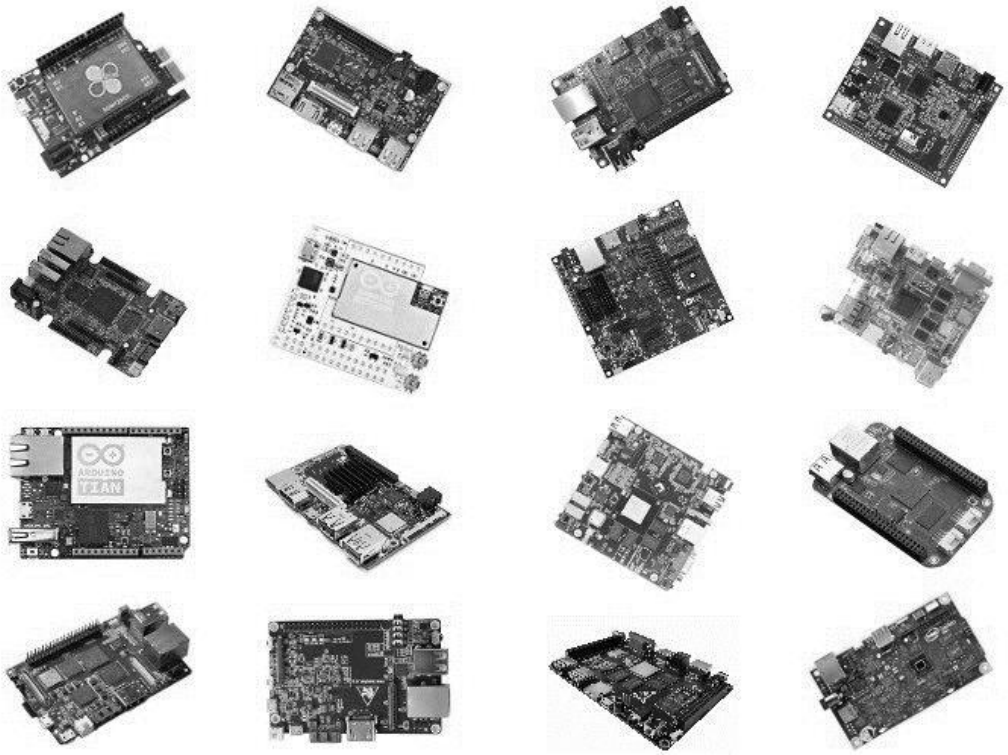
Enabling Technologies - Big Data Analytics

- 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 IoT application.



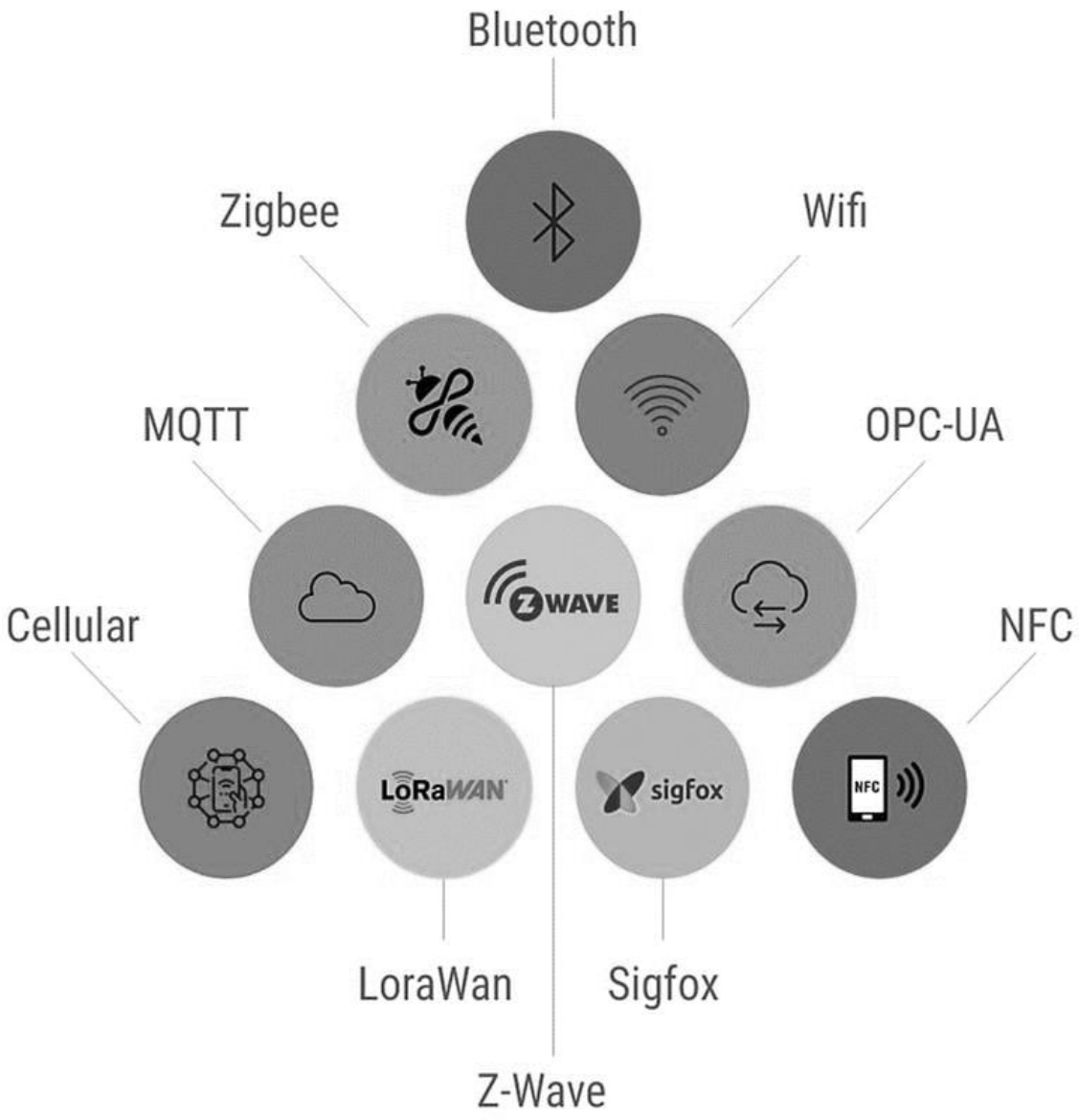
Enabling Technologies - Embedded Computing Boards

- An embedded computing board is 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.



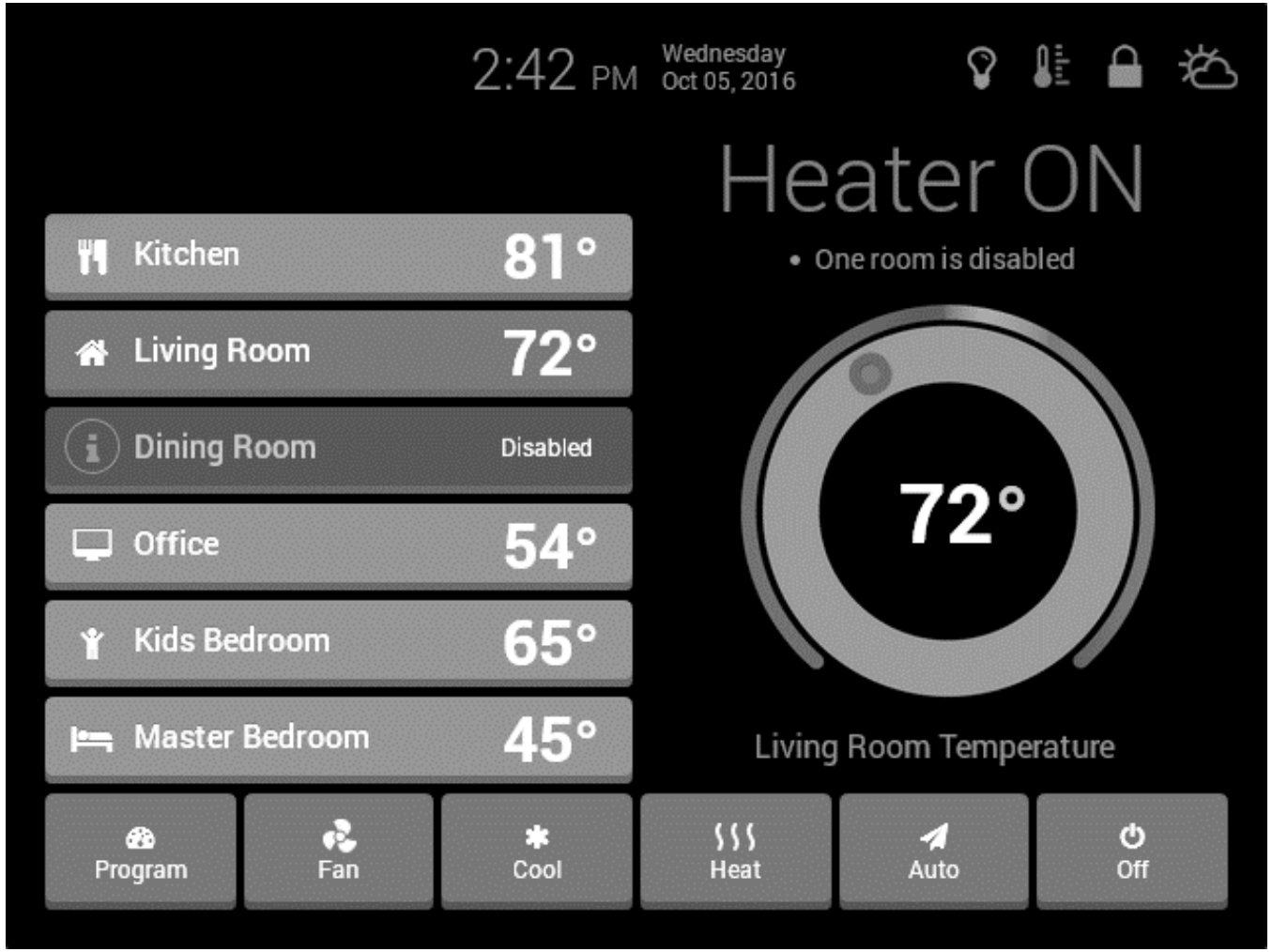
Enabling Technologies - Communication Protocols

- 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.



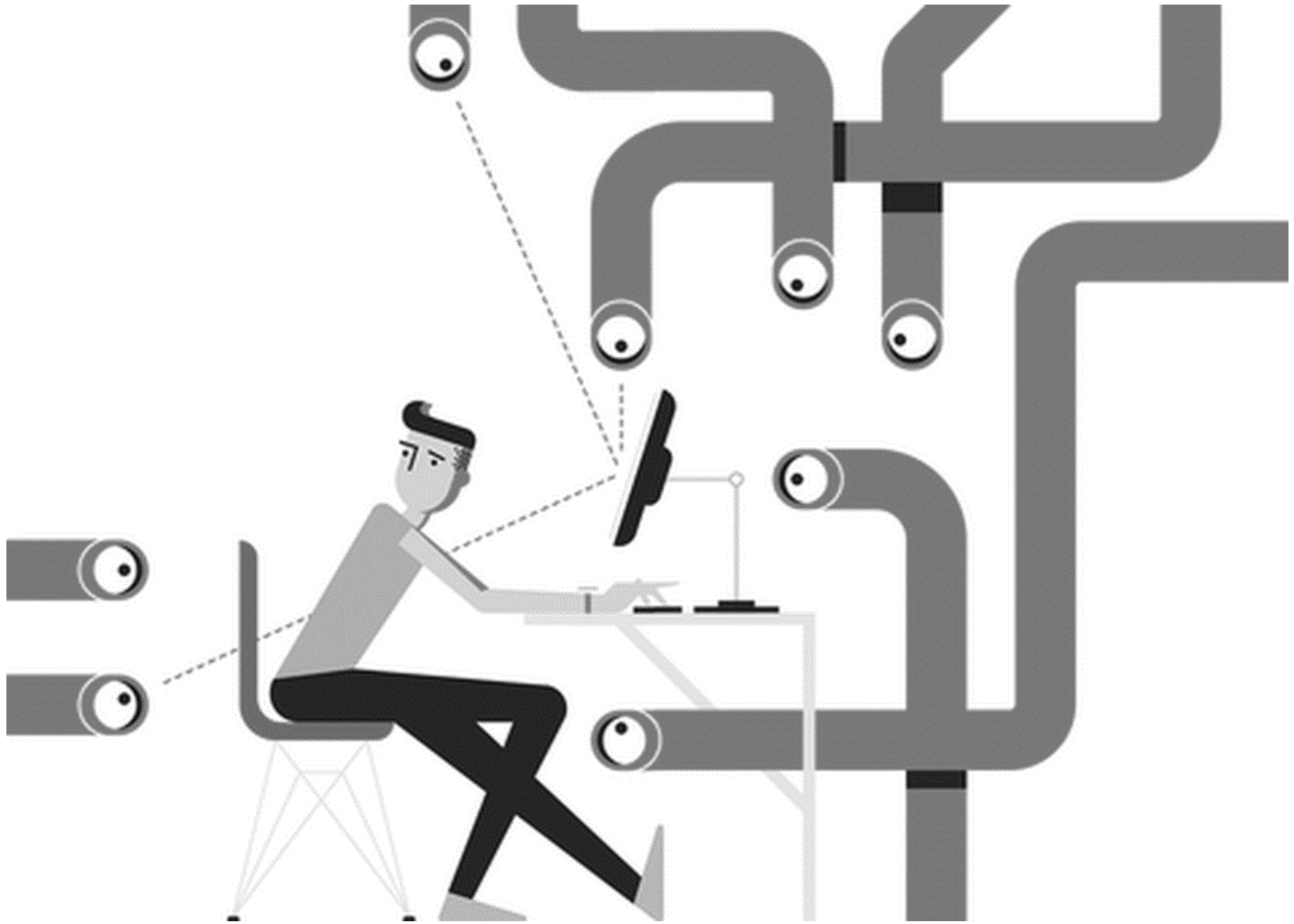
IoT Challenges

- 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.

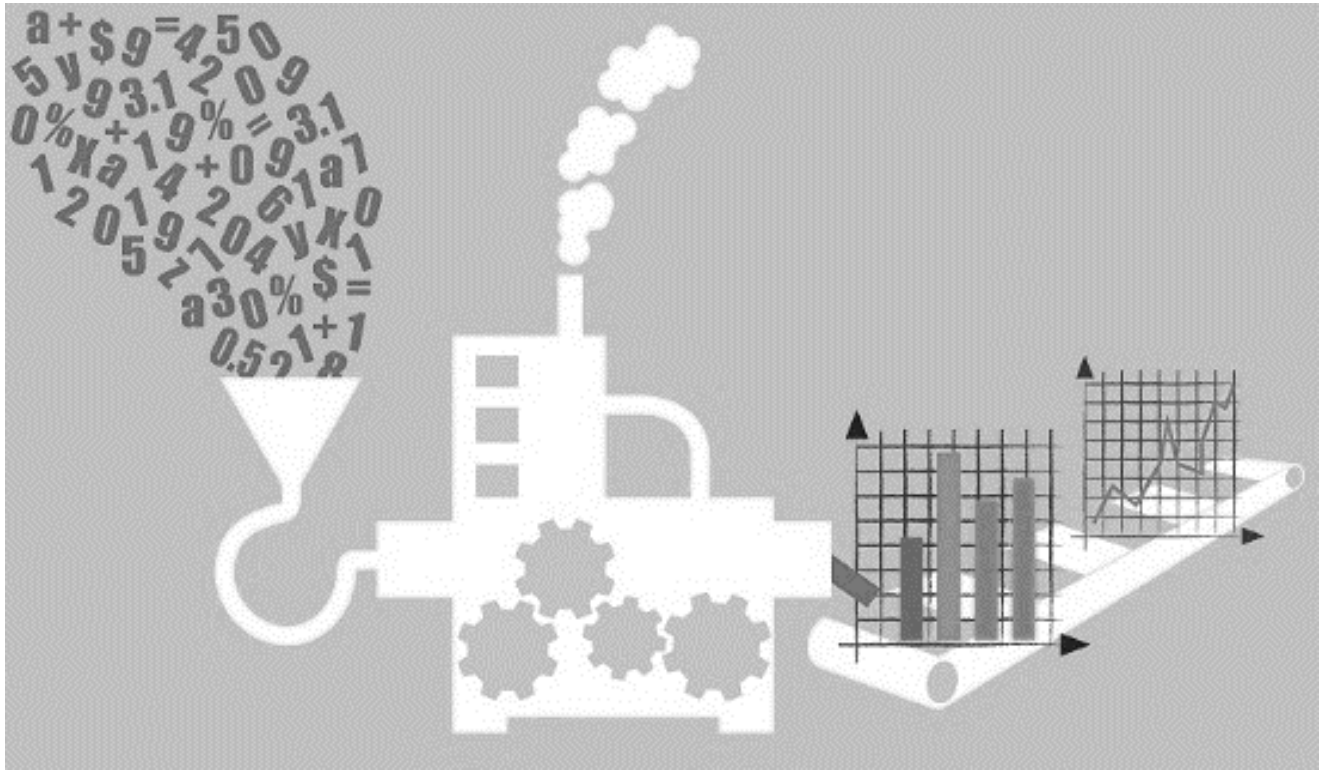
IoT Challenges

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?"



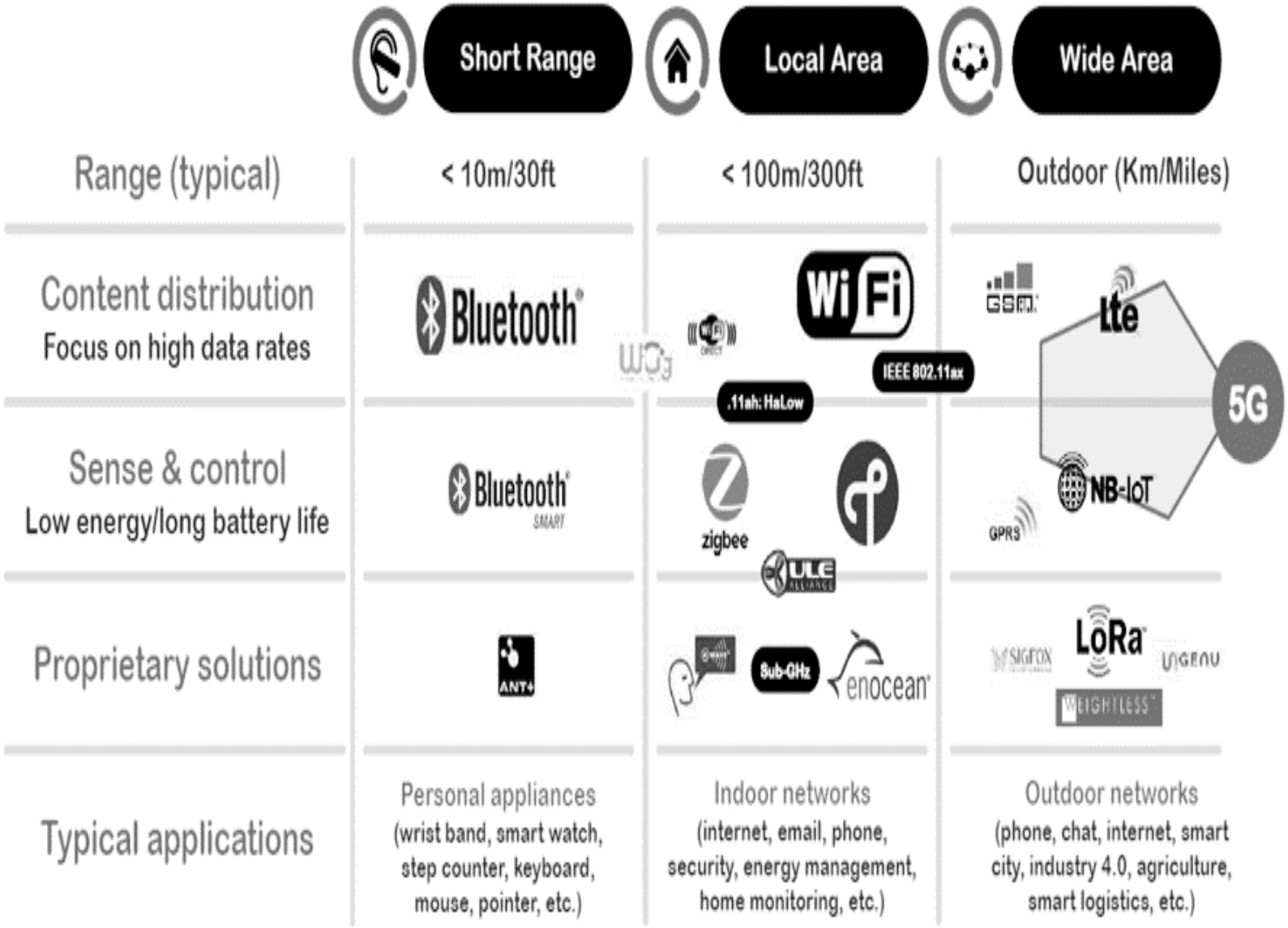
IoT Challenges

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.



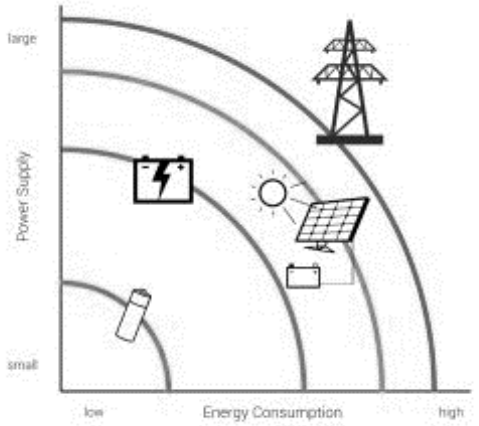
IoT Challenges

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.

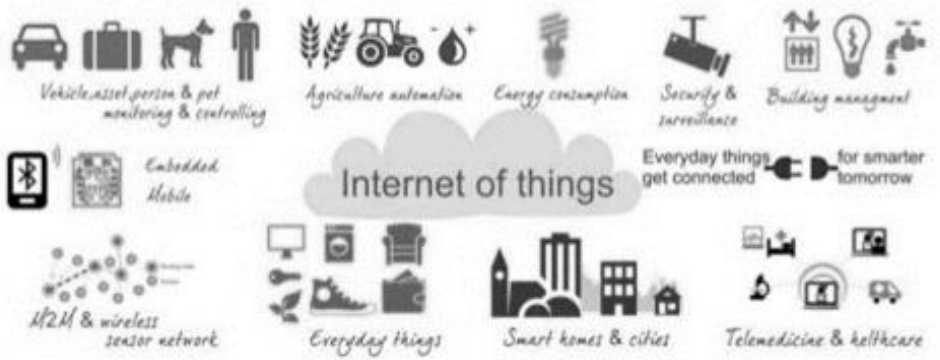


IoT Challenges

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.

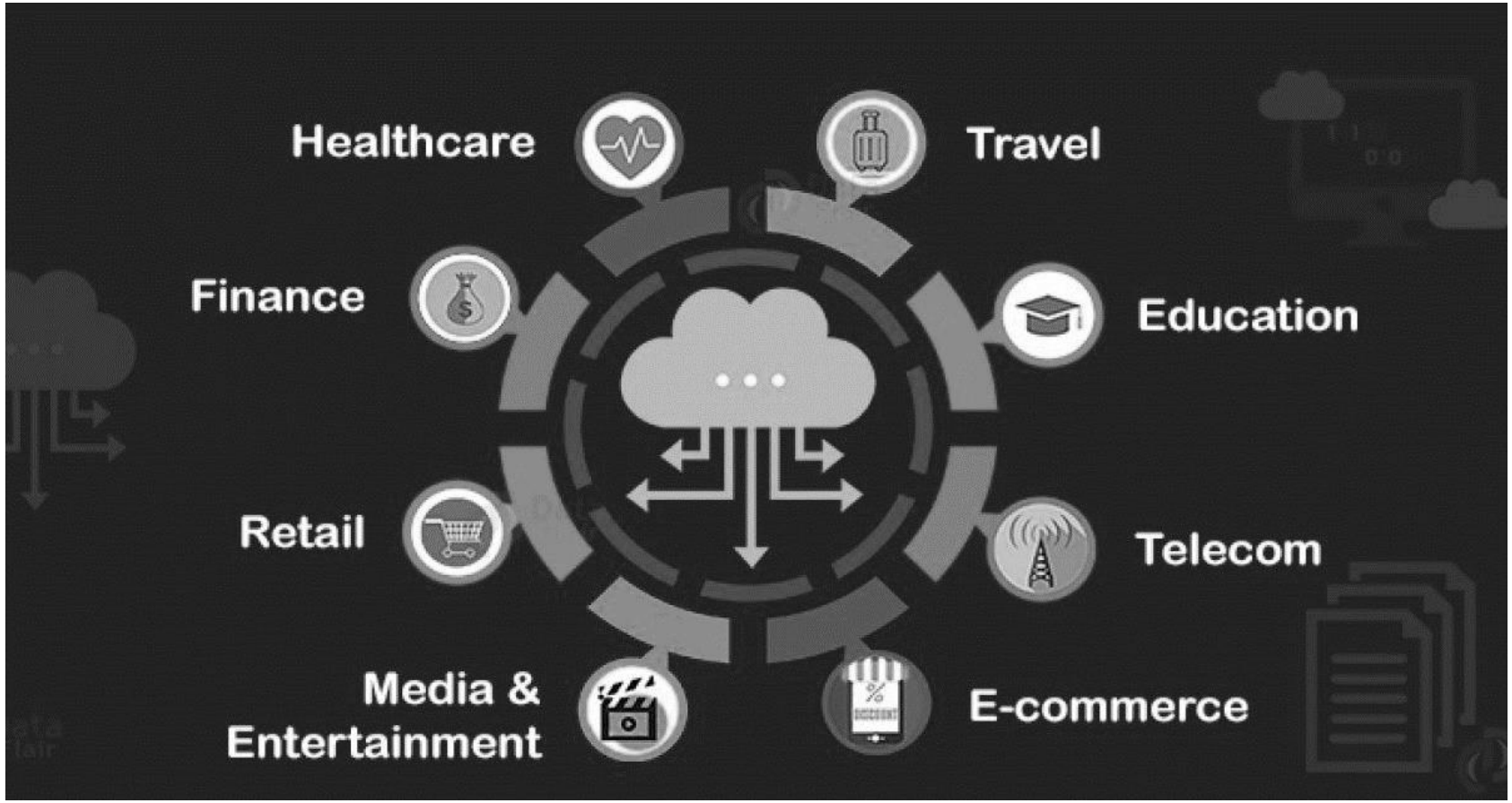


6. Complexity involved:
   - IoT is not easy. It needs a lot of different domains to integrate into a cohesive system.
   - There is very limited expertise available in the market, but the growth is very rapid.
   - The toolkits, software and hardware are not abundant and real skill is required to build an application.



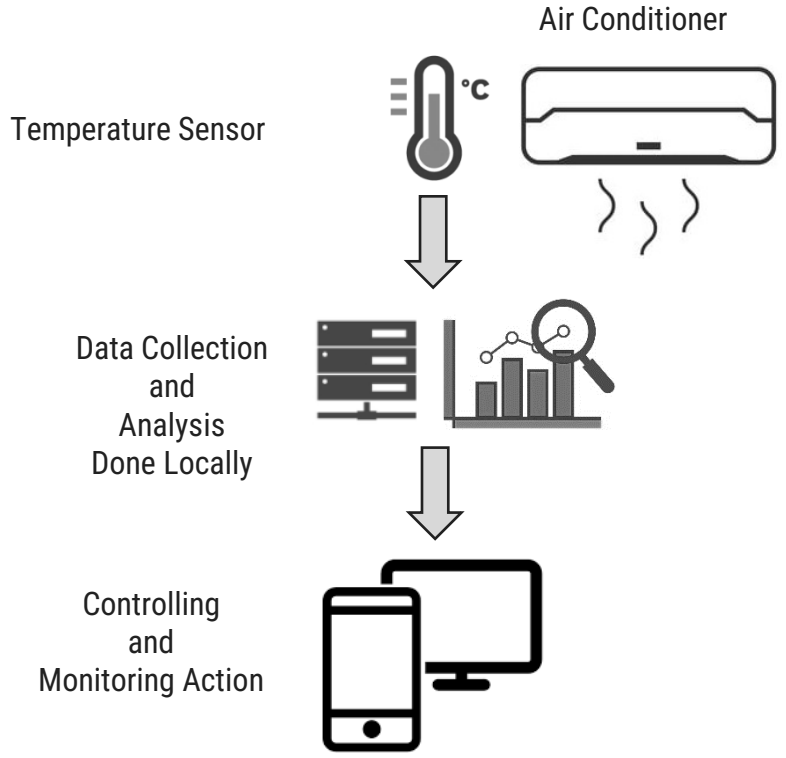
IoT Challenges

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

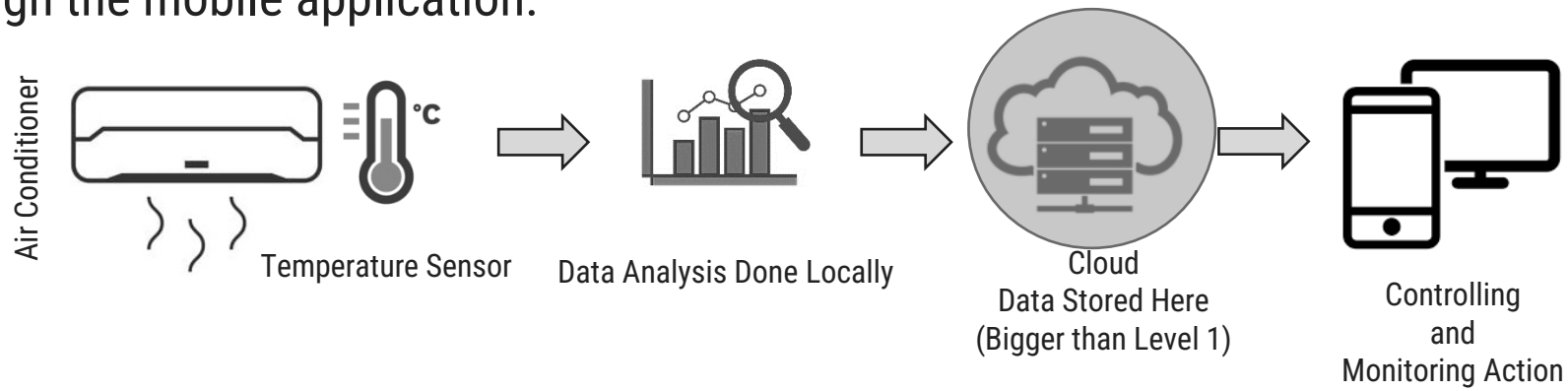
- Based on the architectural approach, IoT can be classified in five levels: Level 1 to Level 5.
- Level 1
  - It is of minimal complexity.
  - The application has one sensor (temperature sensor, pressure sensor, etc).
  - The data sensed is stored locally and the data analysis is done locally.
  - Monitoring / 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

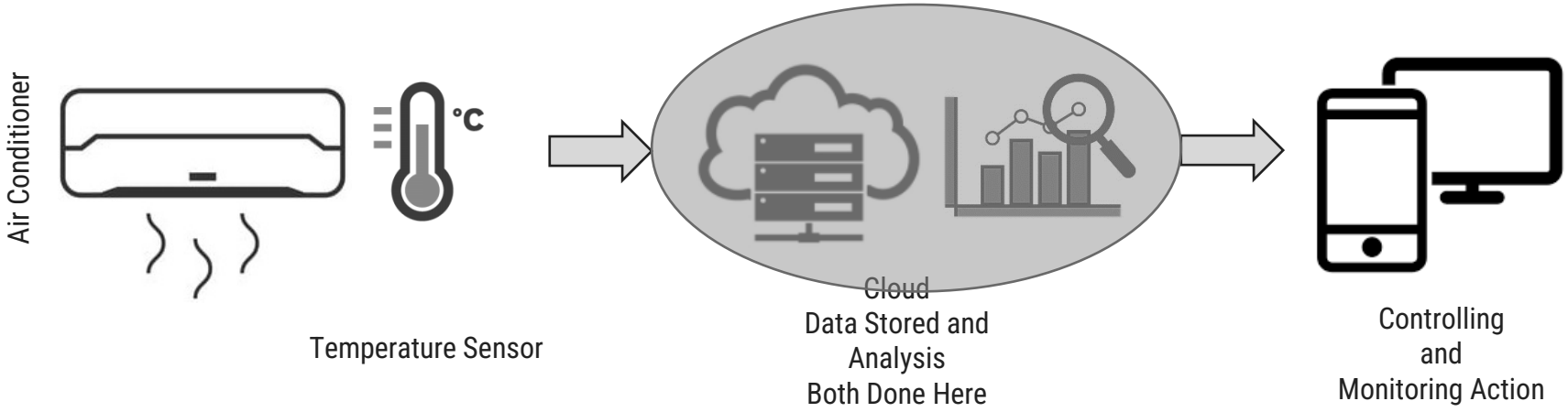
- The second level is slightly more complex than the previous level.
- The data is more voluminous and hence, cloud storage is preferred.
- The frequency of sensing done by the sensor is faster.
- The number of times sensing is done would be much more than Level 1.
- The analysis is carried out locally, 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

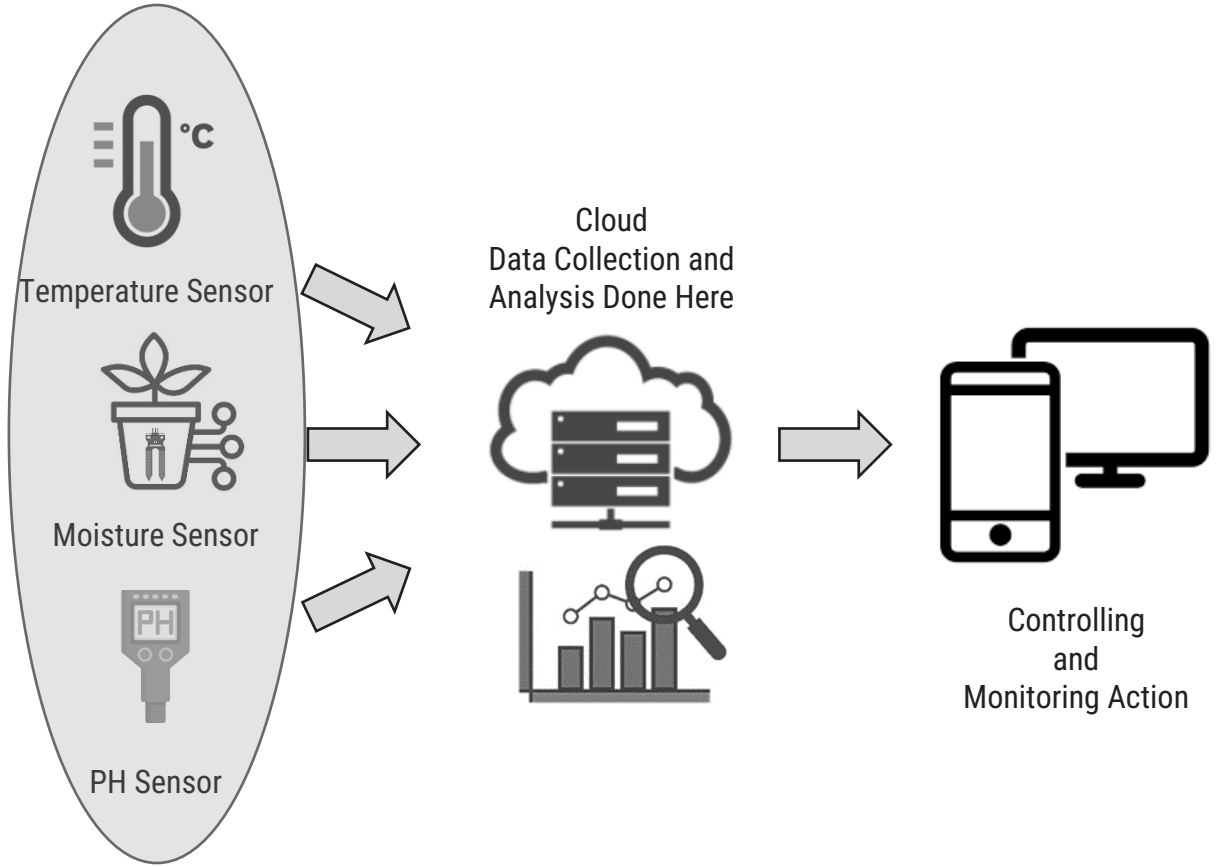
- The data is huge, frequency of sensing done by the sensor is faster and the data is stored on cloud.
- The difference is that the analysis is also carried out on cloud.
- Based on the data analysis, the control action can be triggered through the web application or mobile application.
- Some examples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



IoT Levels

Level 4

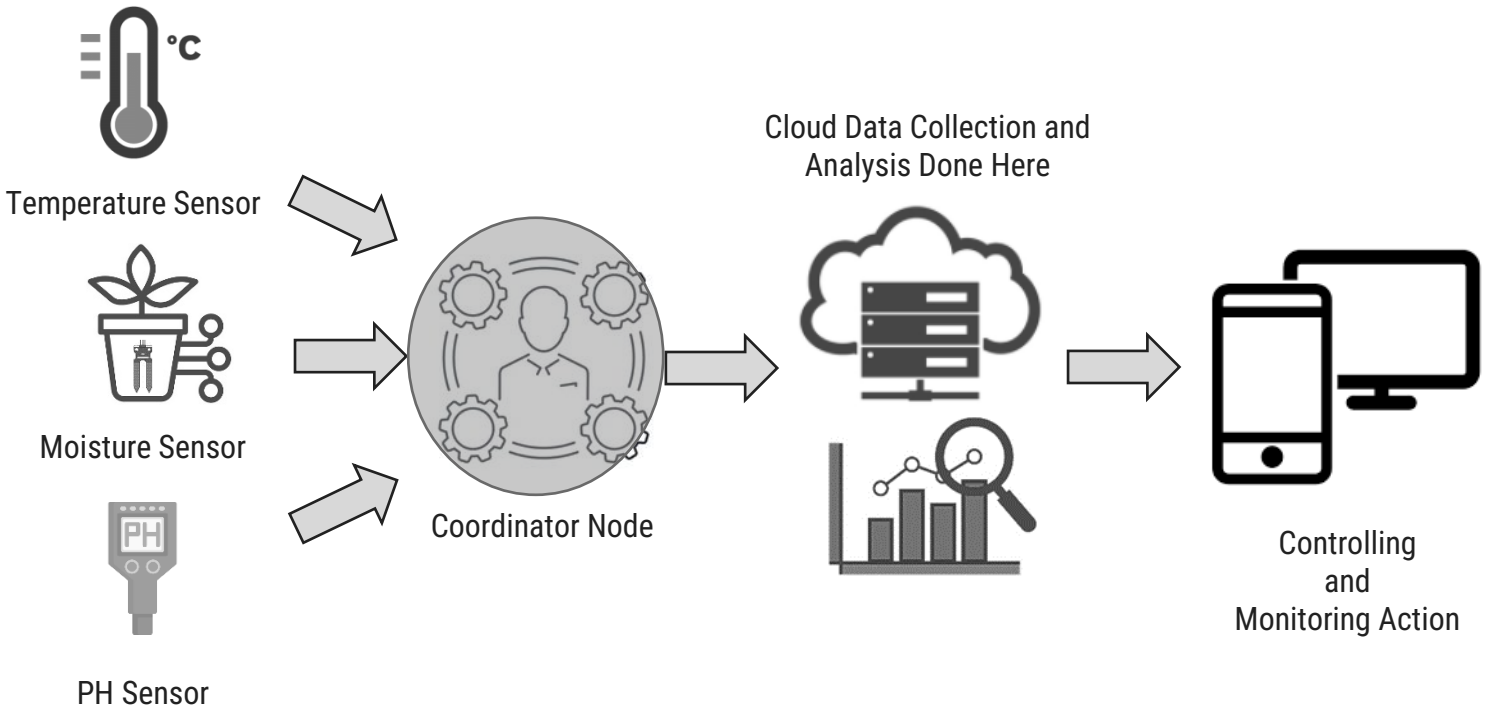
- With every passing level, the volume of data increases and hence the rate at which it is sensed also increases.
- At this level, multiple nodes are present which are independent of each other.
- These nodes upload data to the cloud.
- All the sensors upload the read sensory inputs on cloud storage.
- 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

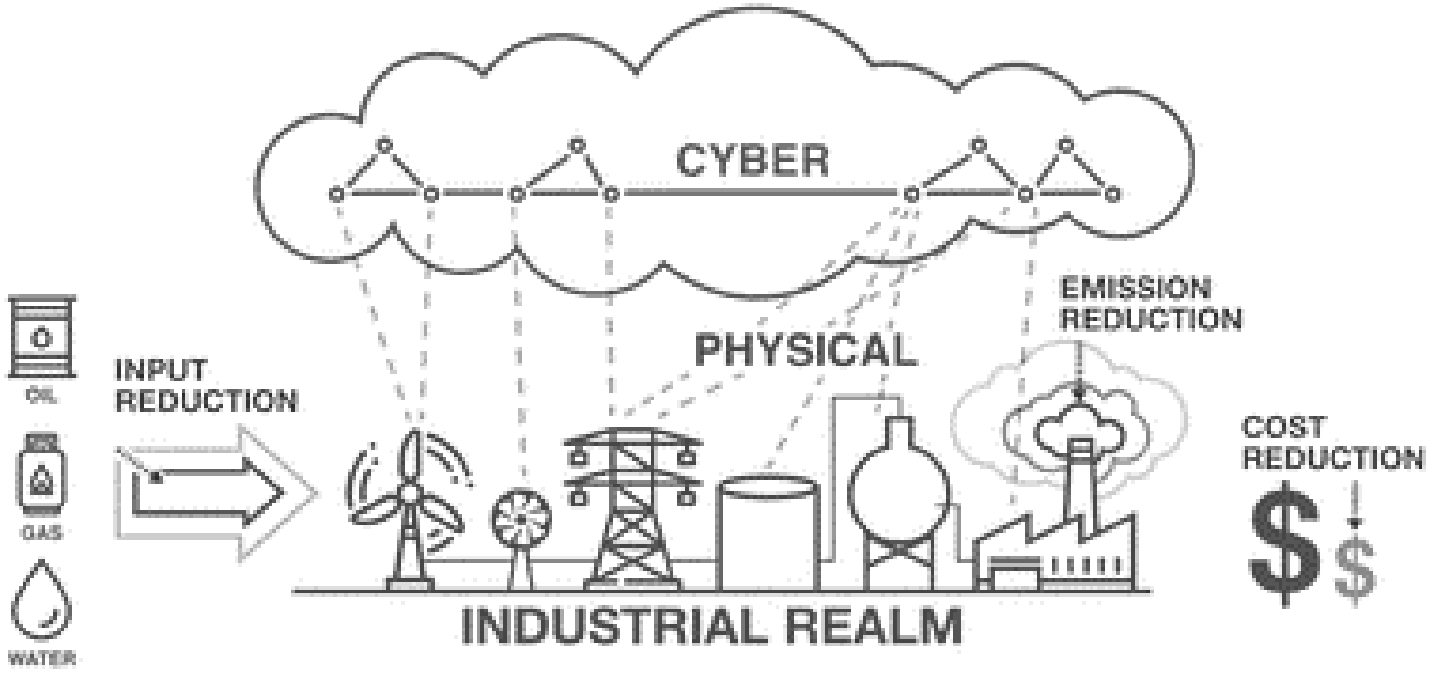
Level 5

- 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.



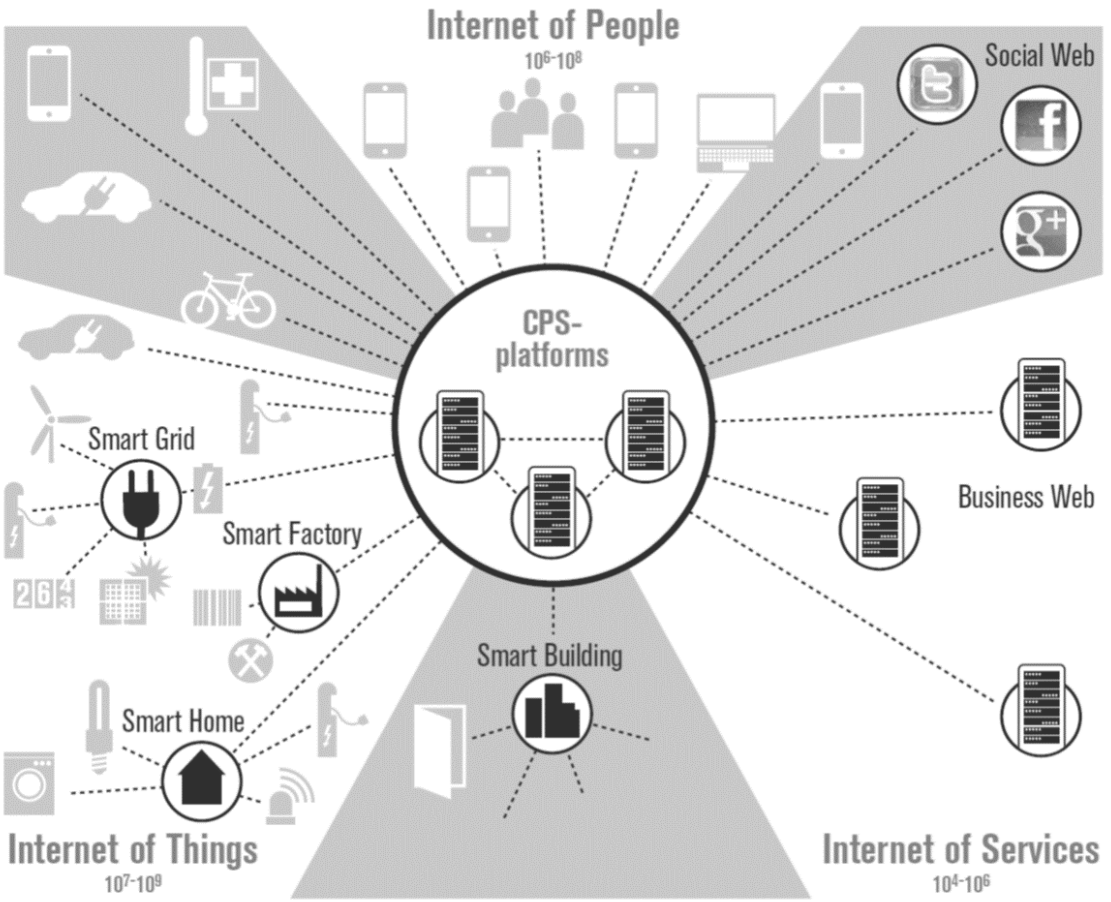
Cyber Physical System versus IoT

- 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.



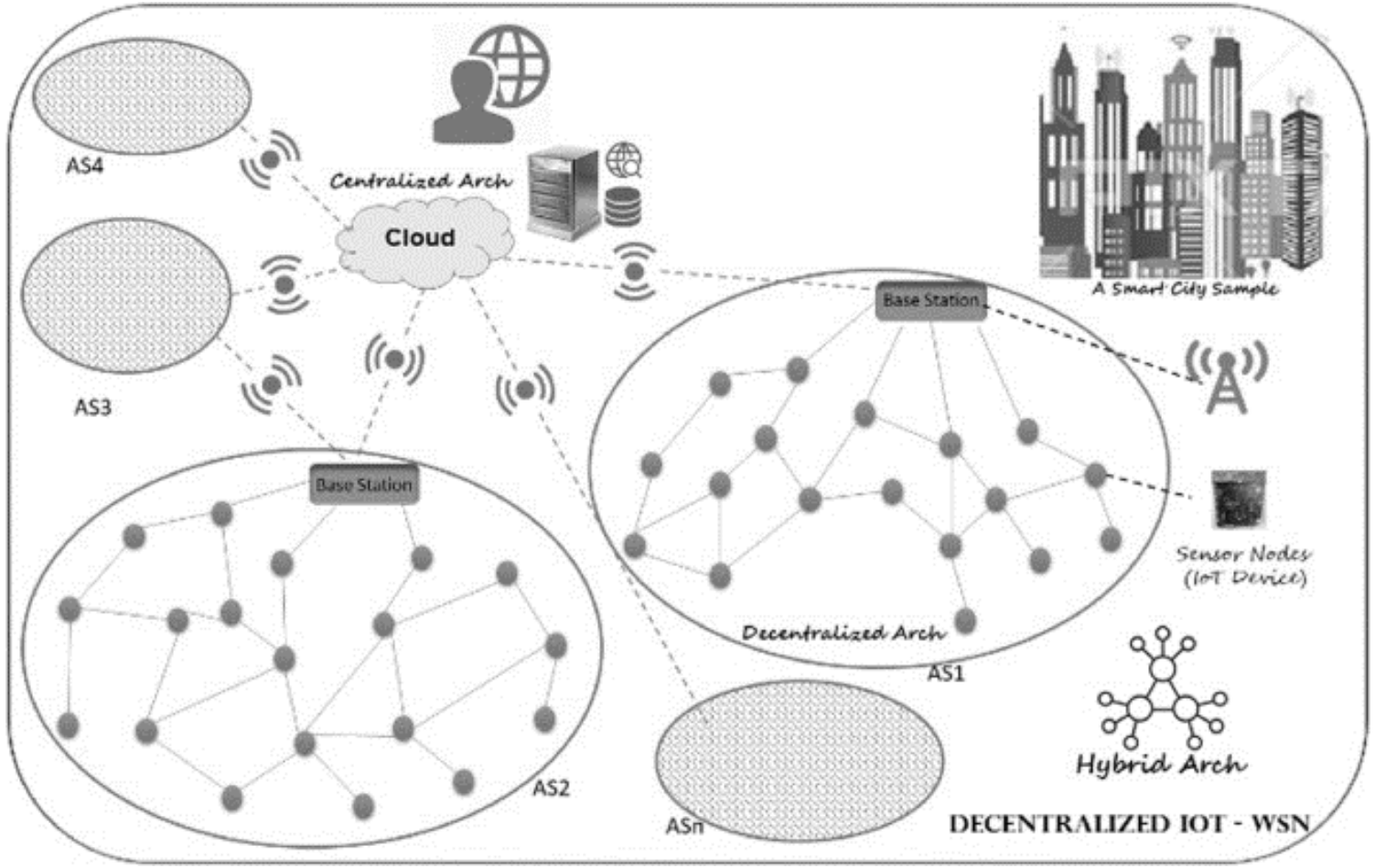
Cyber Physical System versus IoT

- 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.



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.



Physical Design of IoT

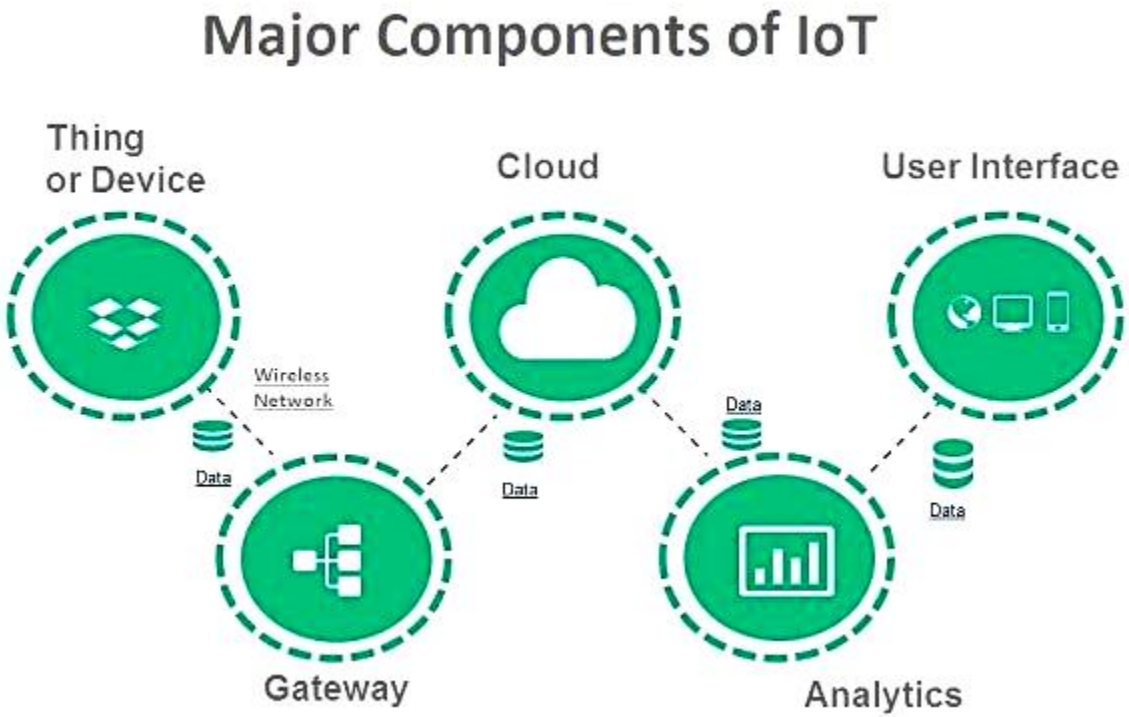
Physical design indicates importance and role of each physical component in IoT Ecosystem.

There are three IoT components which enable seamless communication:

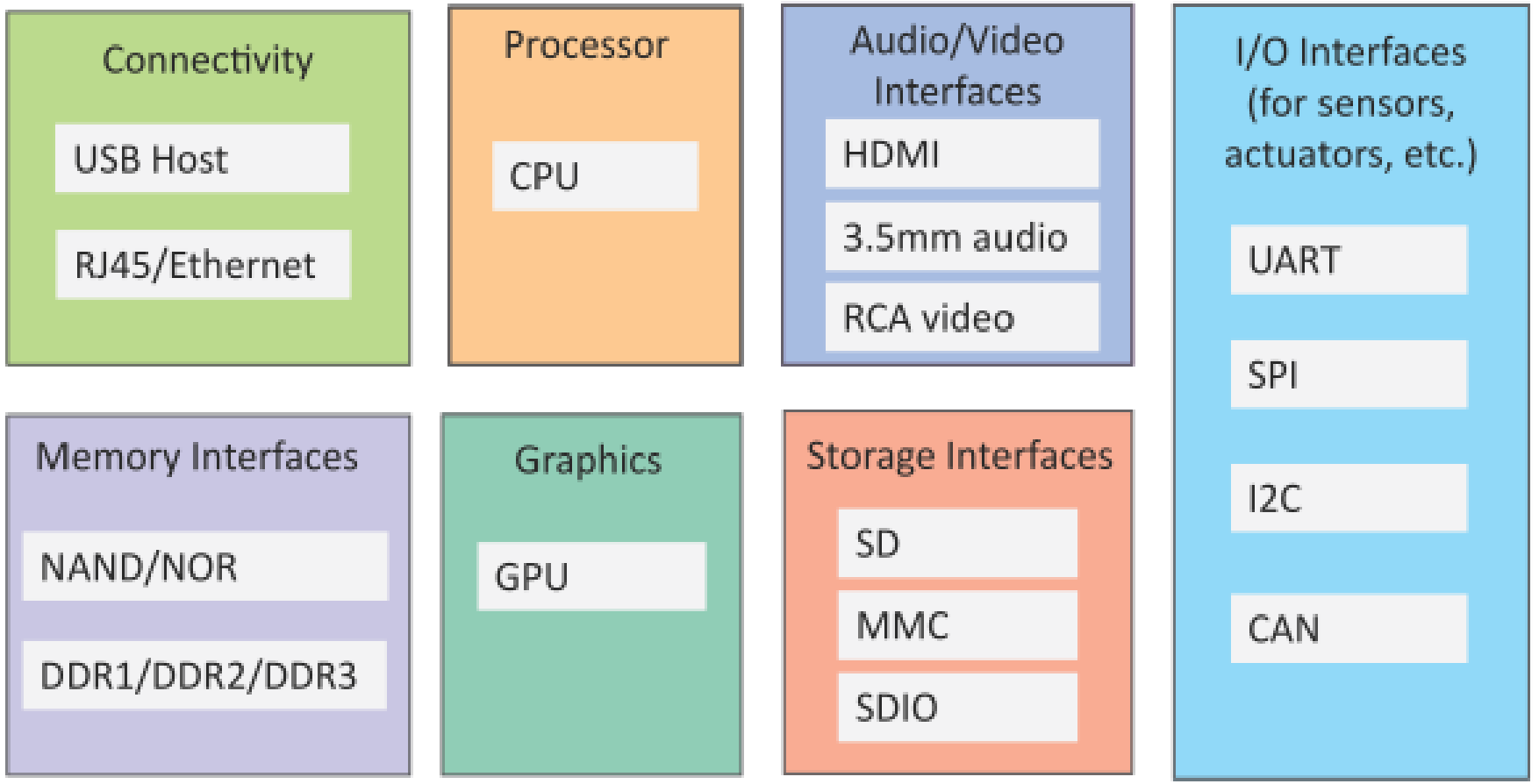
a) Hardware - made up of sensors, actuators and embedded communication hardware

b) Middleware - on demand storage and computing tools for data analytics

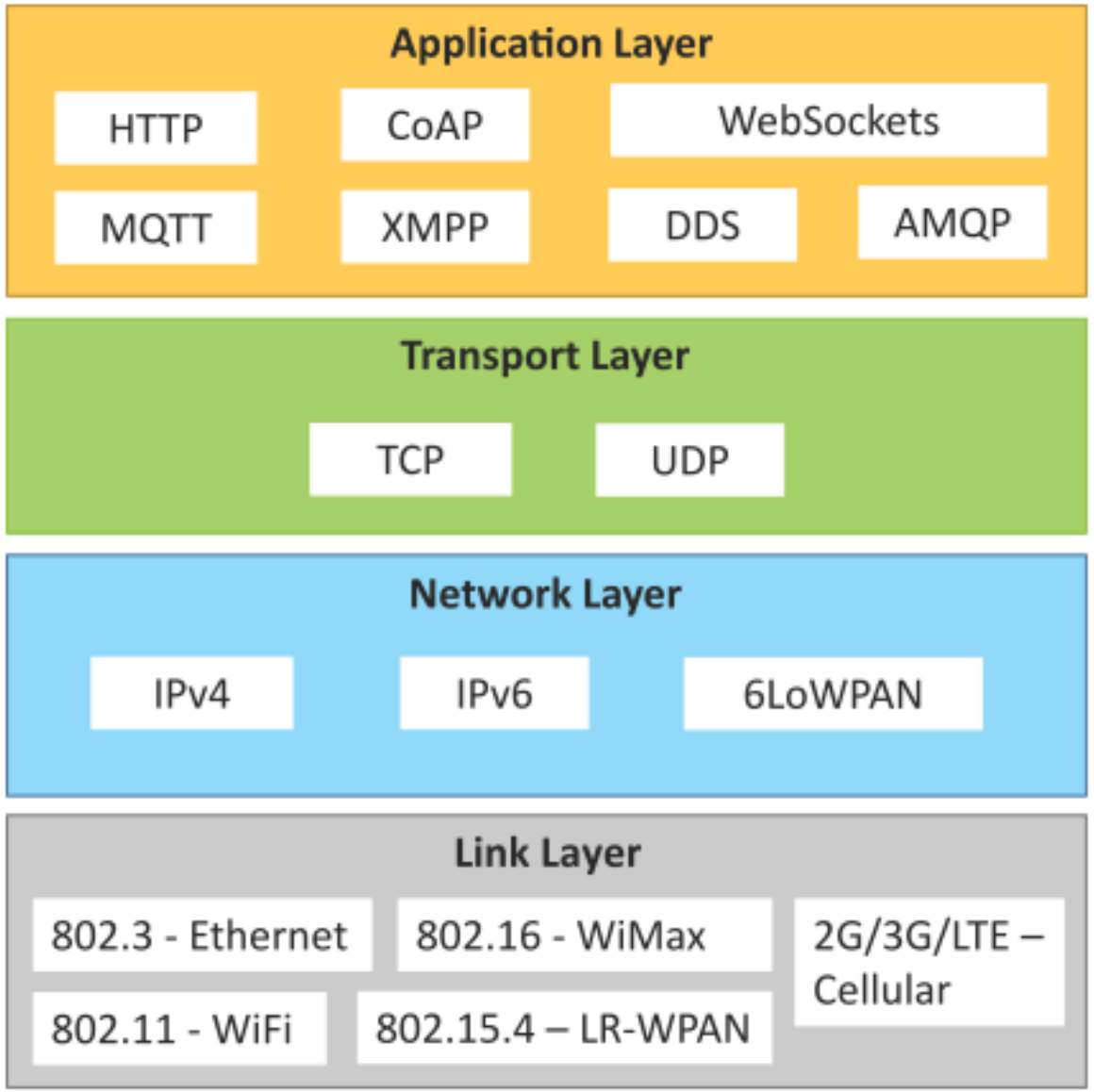
c) Presentation - novel easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications.



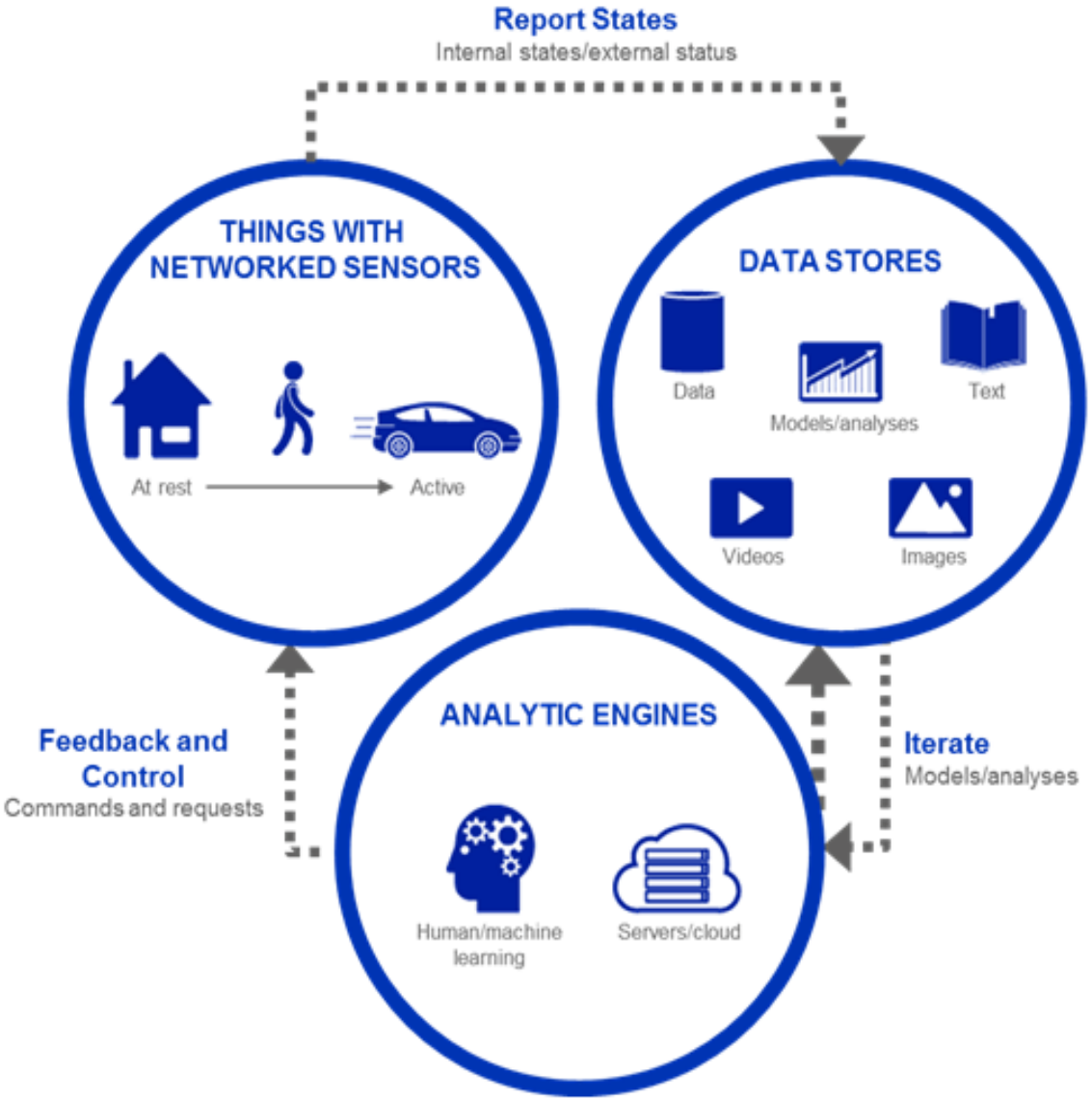
- An IoT device may consist of several interfaces for connections to other devices, both wired and wireless.
- I/O interfaces for sensors
- Interfaces for internet connectivity
- Memory and storage interfaces
- Audio/video interfaces



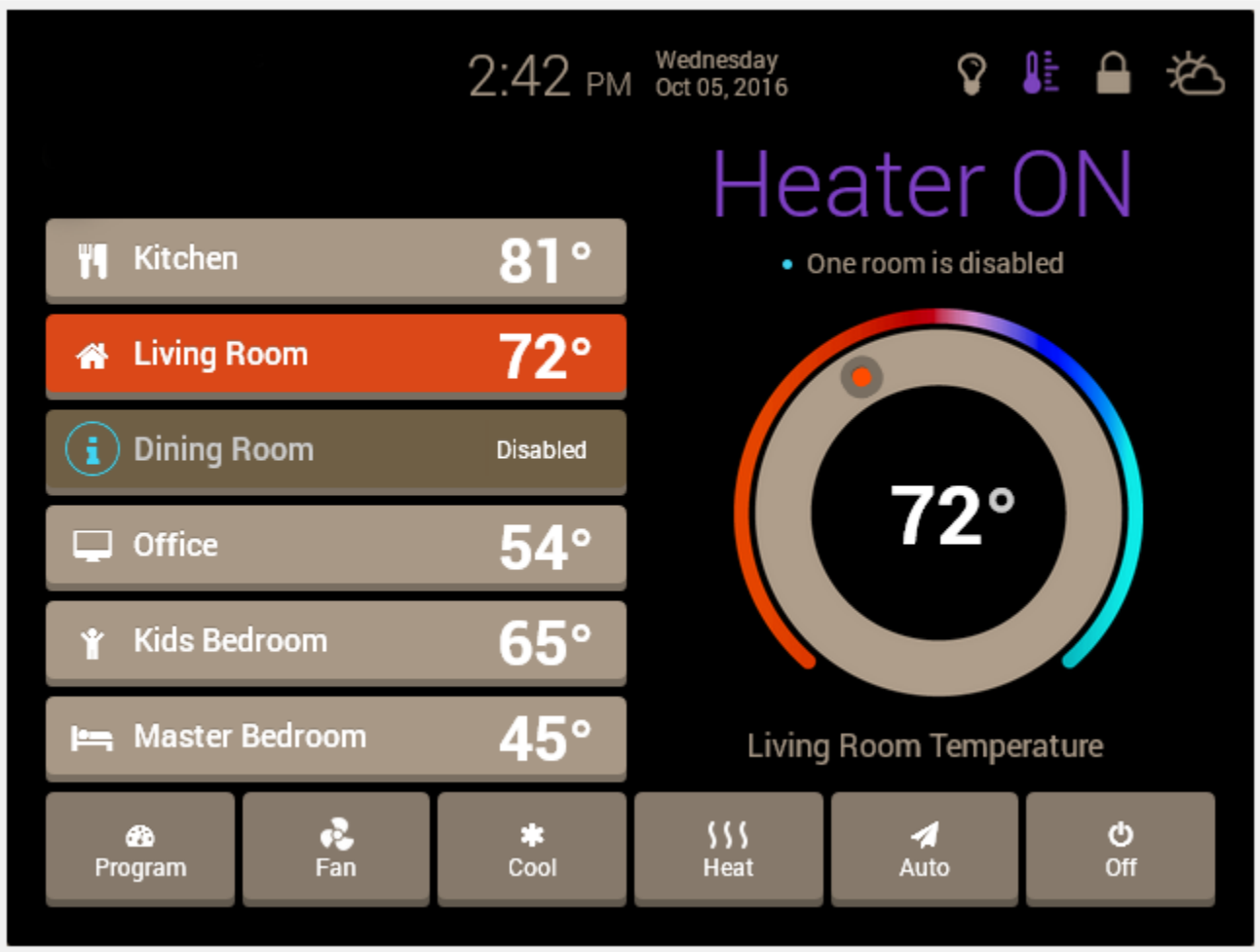
- Link Layer
  - 802.3 – Ethernet
  - 802.11 – WiFi
  - 802.16 – WiMax
  - 802.15.4 – LR-WPAN
  - 2G/3G/4G
- Network Layer
  - IPv4
  - IPv6
  - 6LoWPAN
- Transport Layer
  - TCP
  - UDP
- Application Layer
  - HTTP
  - CoAP
  - WebSocket
  - MQTT
  - XMPP
  - DDS
  - AMQP



- Once the data is collected and it gets to the cloud, the software performs processing on the acquired data.
- This can range from something very simple, such as checking that the temperature reading on devices such as AC or heaters is within an acceptable range.
- It can sometimes also be very complex, such as identifying objects (such as intruders in your house) using computer vision on video.
- But there might be a situation when a user interaction is required, example- what if when the temperature is too high or if there is an intruder in your house? That's where the user comes into the picture.

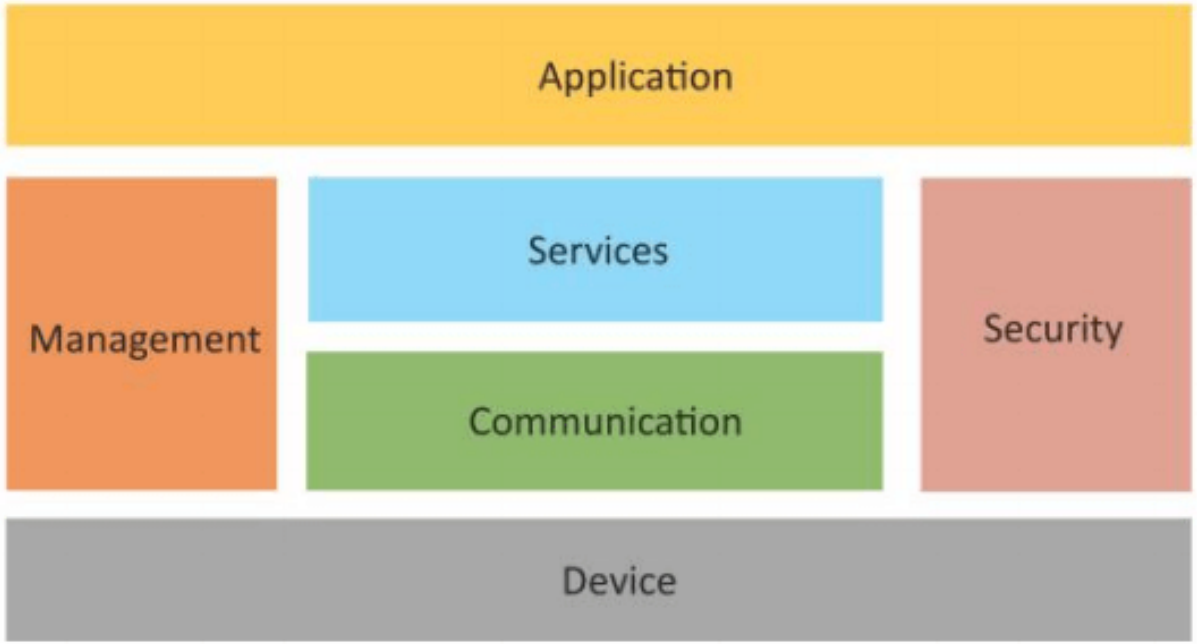


- Next, the information made available to the end-user in some way. This can achieve by triggering alarms on their phones or notifying through texts or emails.
- Also, a user sometimes might also have an interface through which they can actively check in on their IoT system. For example, a user has a camera installed in his house, he might want to check the video recordings and all the feeds through a web server.
- User interface provides large visibility of IoT ecosystem.



Logical Design of IoT:

- Logical design presents logical data flow between source and destination of data.
- Logical design of an IoT system refers to an abstract representation of the entities and processes without going into the low-level specifics of the implementation.
- An IoT system comprises of a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication, and management.
- Depending on logical communication between source and destination of data, there are different kinds of logical communication model, which are:

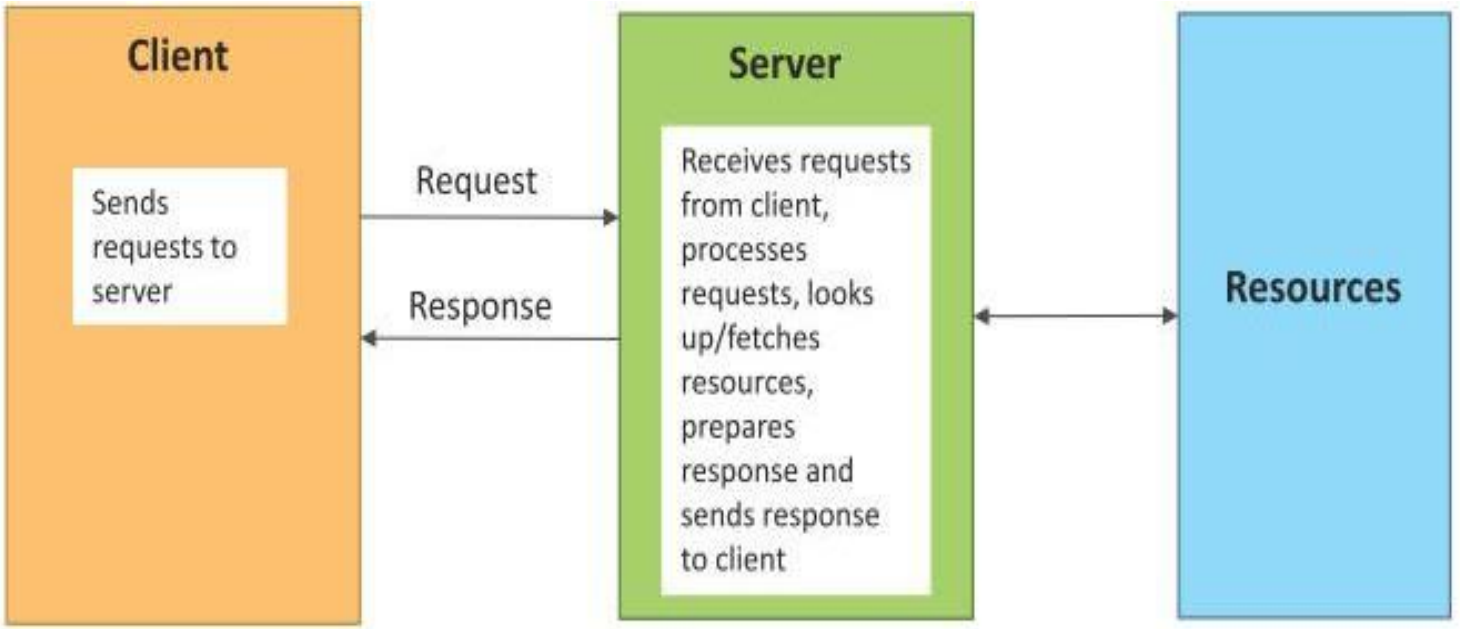


logical communication model

1. Request-Response communication model
2. Publish-Subscribe communication model
3. Push-Pull communication model
4. Exclusive Pair communication model
5. REST-based Communication APIs
6. WebSocket-based Communication APIs

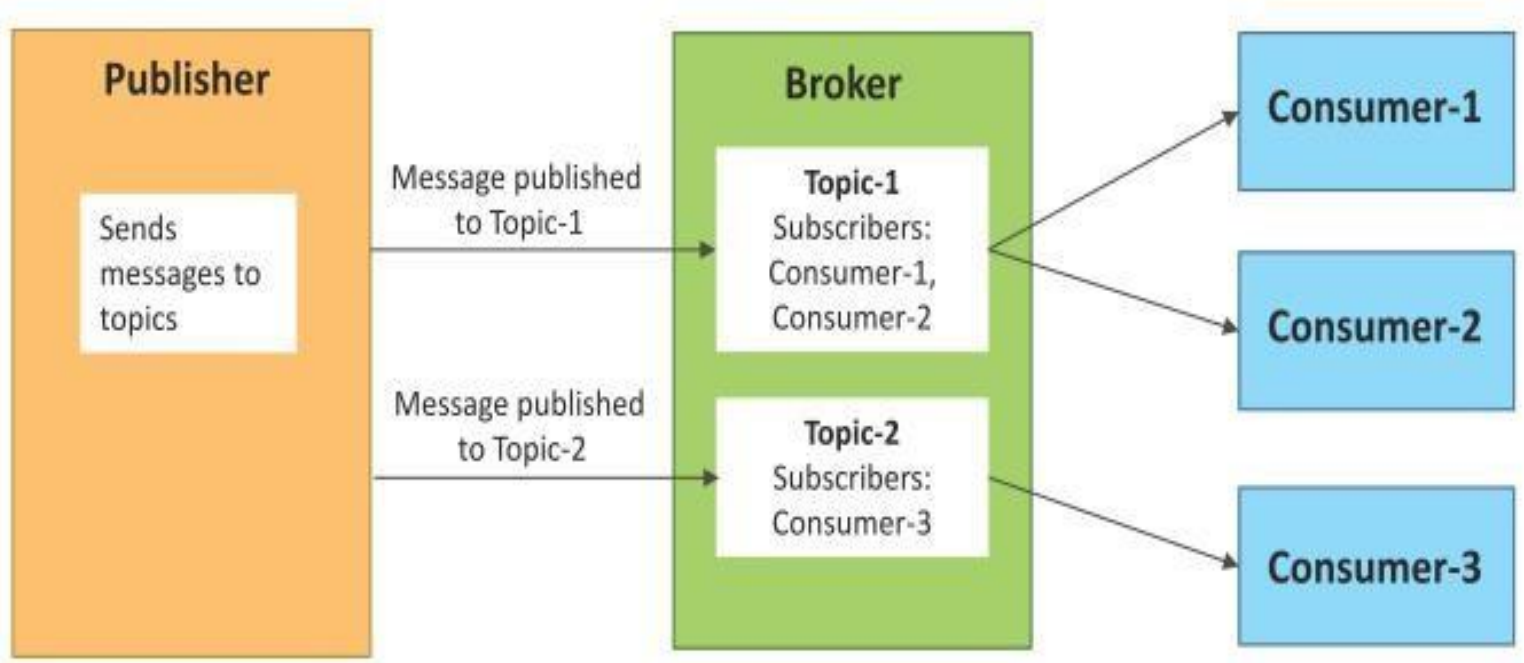
Logical Design of IoT: Request-Response communication model

- Request-Response is a communication model in which the client sends requests to the server and the server responds to the requests.
- When the server receives a request, it decides how to respond, fetches the data, retrieves resource representations, prepares the response, and then sends the response to the client.



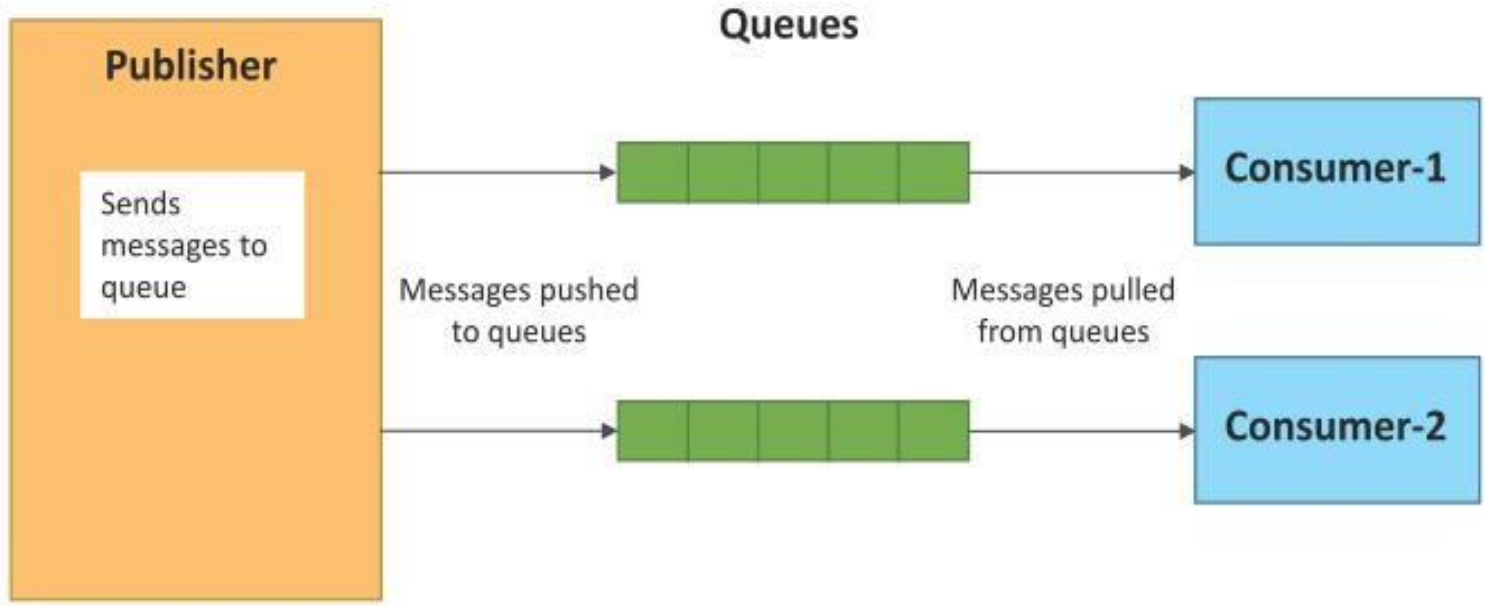
Logical Design of IoT: Publish-Subscribe communication model

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



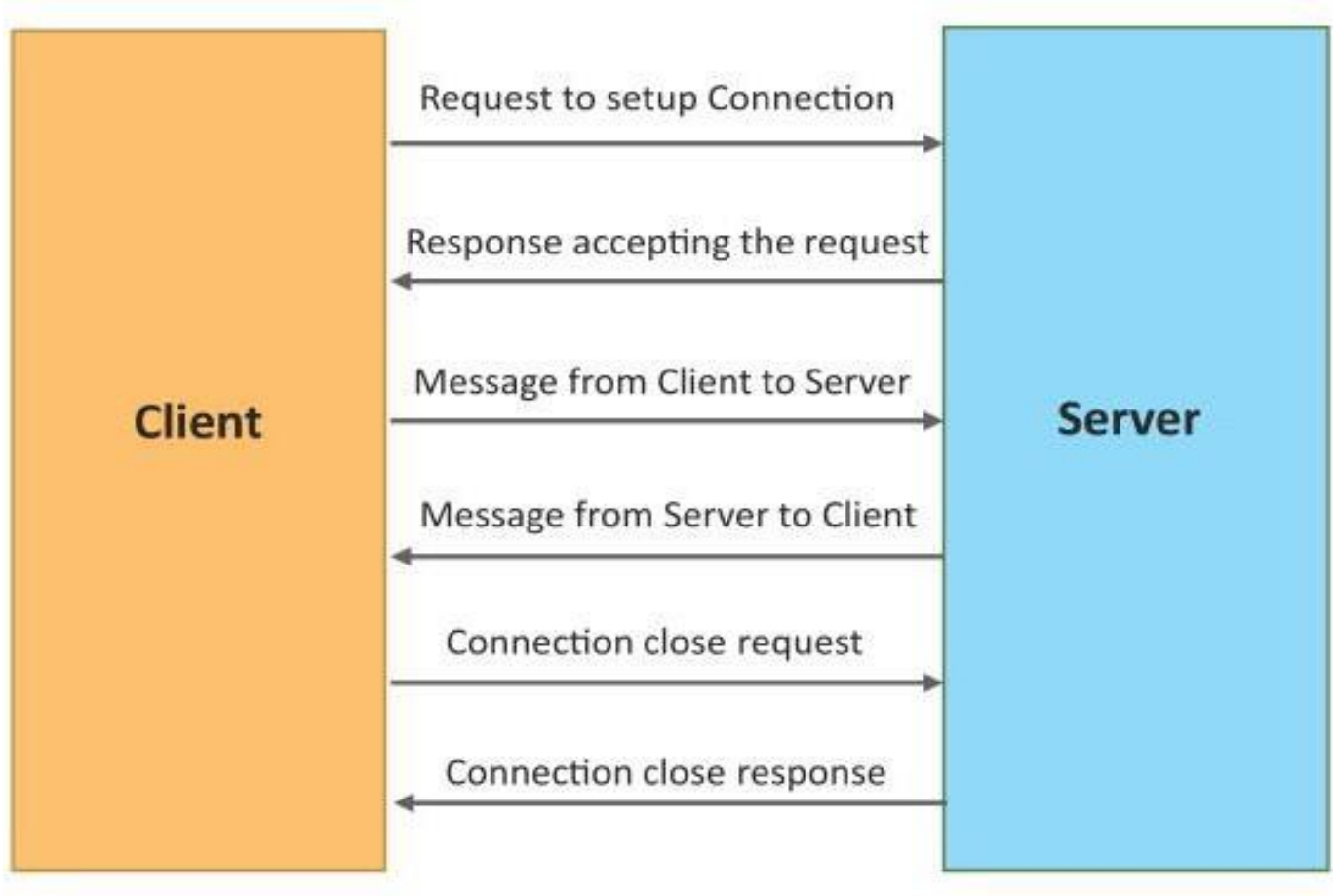
Logical Design of IoT: Push-Pull communication model

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



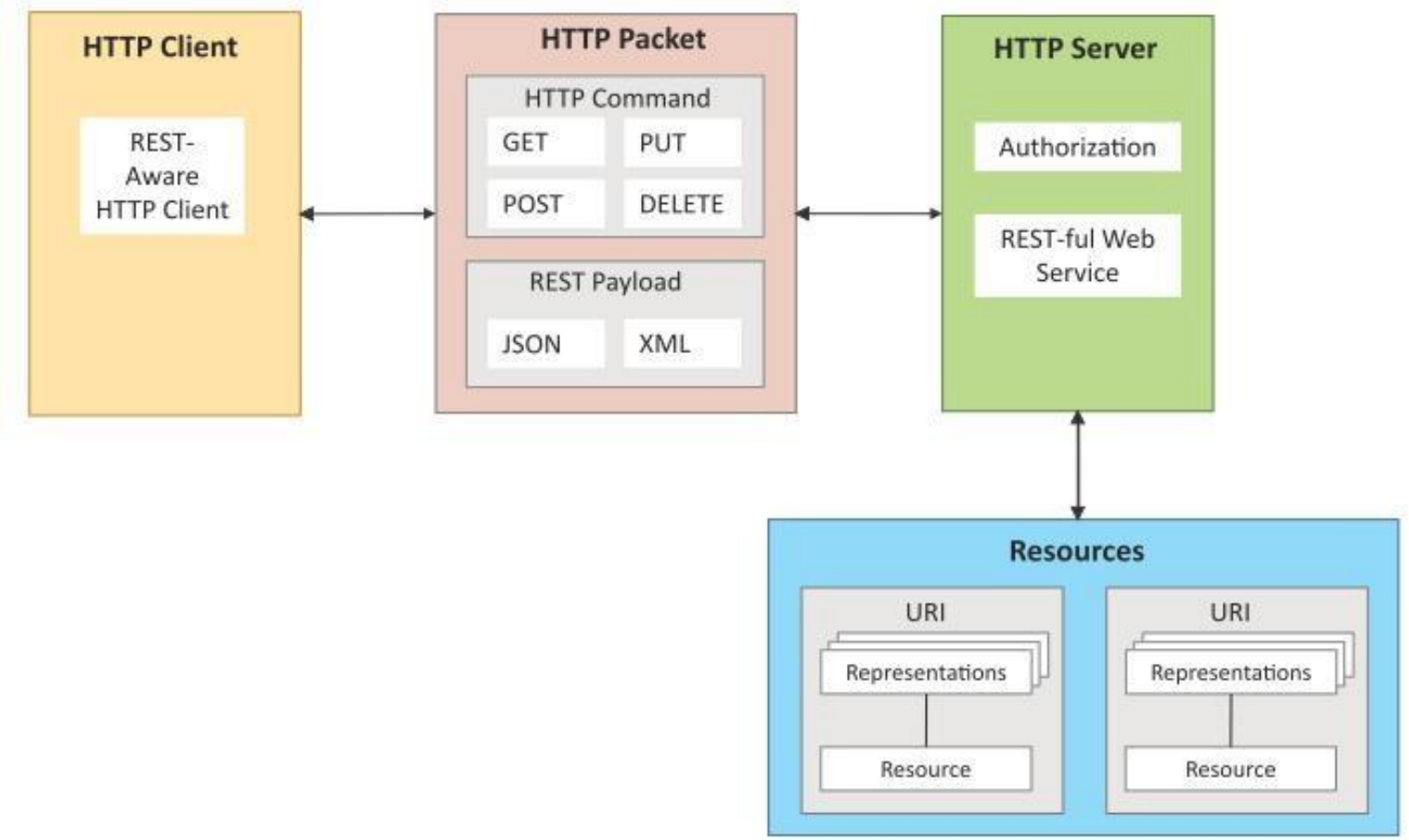
Logical Design of IoT: Exclusive Pair communication model

- Exclusive Pair is a bidirectional, fully duplex communication model that uses a persistent connection between the client and server.
- Once the connection is setup it remains open until the client sends a request to close the connection.
- Client and server can send messages to each other after connection setup.



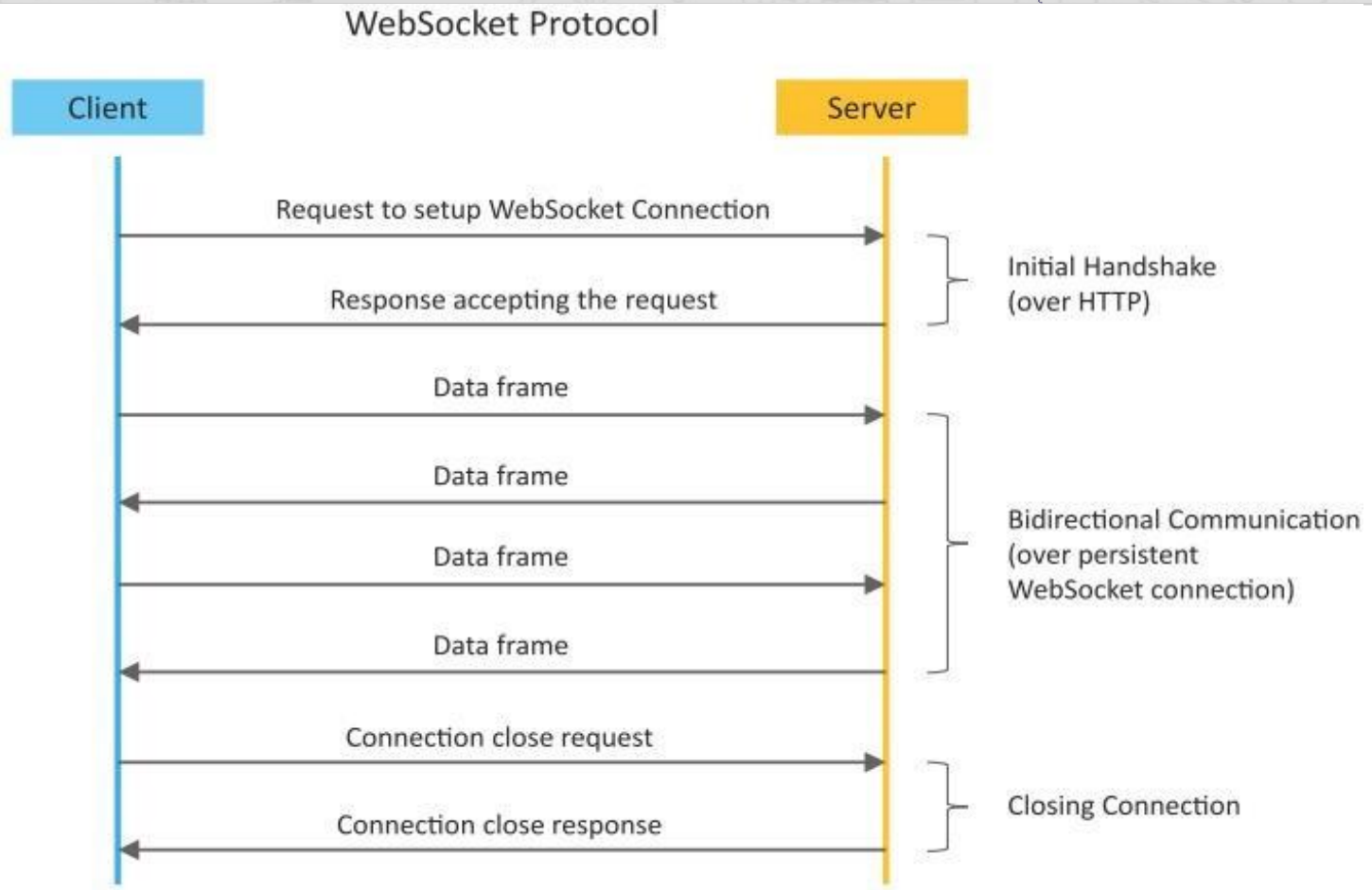
Logical Design of IoT: REST-based Communication APIs

- Representational State Transfer (REST) is a set of architectural principles by which you can design web services and web APIs that focus on a system's resources and how resource states are addressed and transferred.
- REST APIs follow the request-response communication model.
- The REST architectural constraints apply to the components, connectors, and data elements, within a distributed hypermedia system.



Logical Design of IoT: WebSocket-based Communication APIs

- WebSocket APIs allow bi-directional, full duplex communication between clients and servers.
- WebSocket APIs follow the exclusive pair communication model between client and server.



Summary of Key Protocols:

Sr.No.	Protocol	Type	Range	Power Consumption	Use Cases
1	MQTT	TCP/IP	Medium	Low	Industrial, smart homes, real-time monitoring
2	CoAP	UDP	Medium	Low	Smart energy, environmental monitoring
3	Zigbee	Mesh	Short	Very Low	Home automation, health monitoring
4	LoRaWAN	LPWAN	Long	Very Low	Agriculture, smart cities
5	BLE	Short Range	Short	Low	Wearables, medical monitoring
6	Wi-Fi	WLAN	Short/Medium	High	Smart homes, video streaming

Fixed & Short Range

- RFID
- Bluetooth
- WiFi

Paper Tag

EPC Tag

Inlay Tag

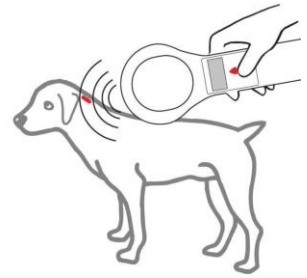
Button Tag

Metal Tag

Glue Tag

Key Tag

Glass Tube Tag

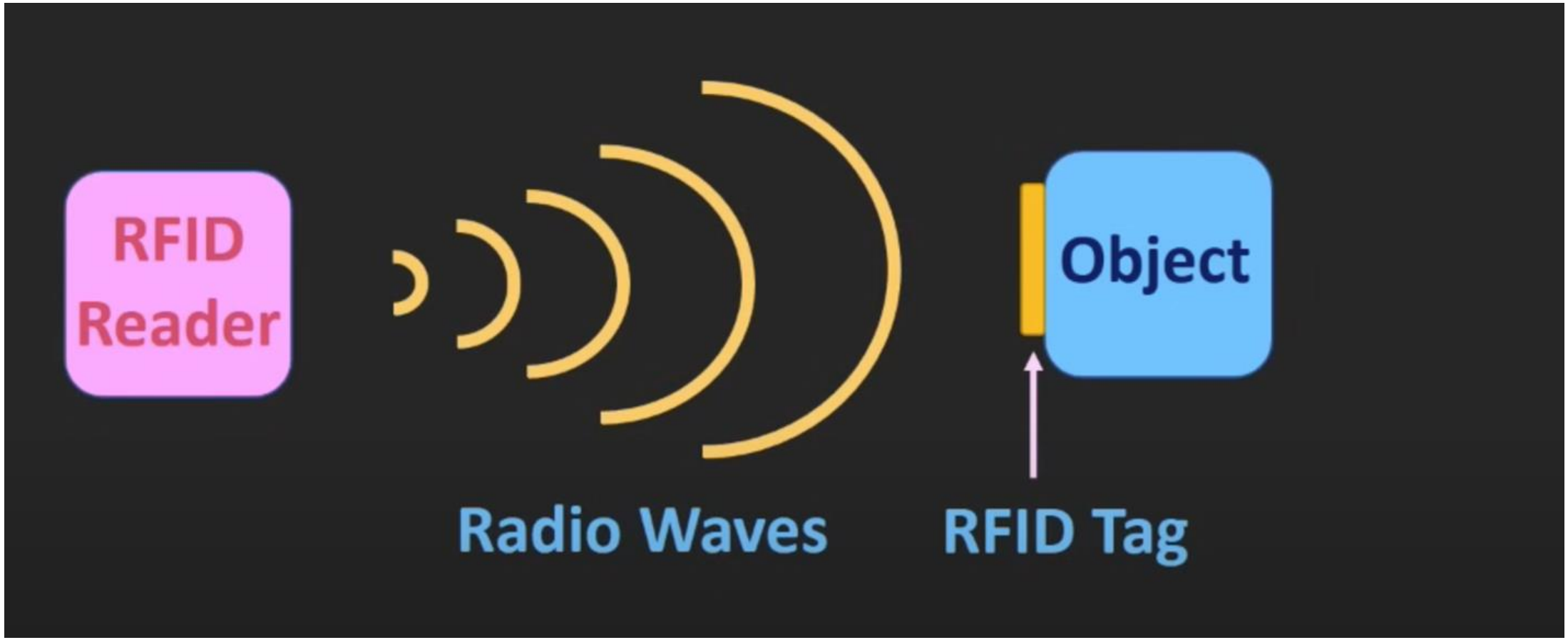


Ear Tag

Ceramic Tag

Disc Tag

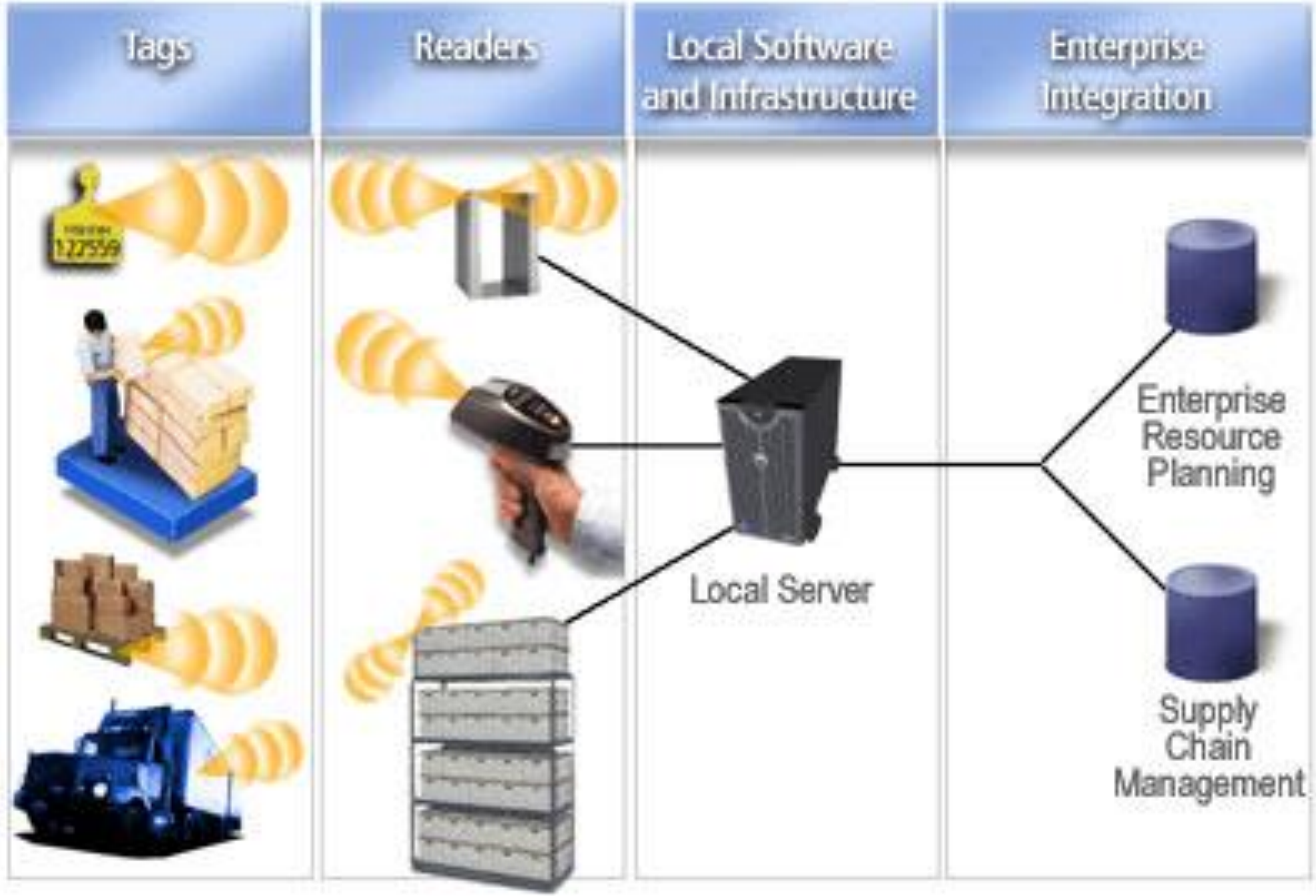
Pocket Tag


RFID
Reader
Object
Radio Waves
RFID Tag

Process

The RFID tracking process is pretty straightforward, irrespective of how you deploy your RFID system. Generally, the RFID tracking process consists of the following four steps.

1. The RFID tag stores the data.
2. The antenna then recognises the nearby RFID tag's signal.
3. The RFID reader, connected wirelessly to the antenna, receives the data stored on the RFID tag.
4. The reader then sends the data to a tracking database which stores and evaluates it.


Tags
Readers
Local Software and Infrastructure
Enterprise Integration
Local Server
Enterprise Resource Planning
Supply Chain Management

Types of RFID Tags

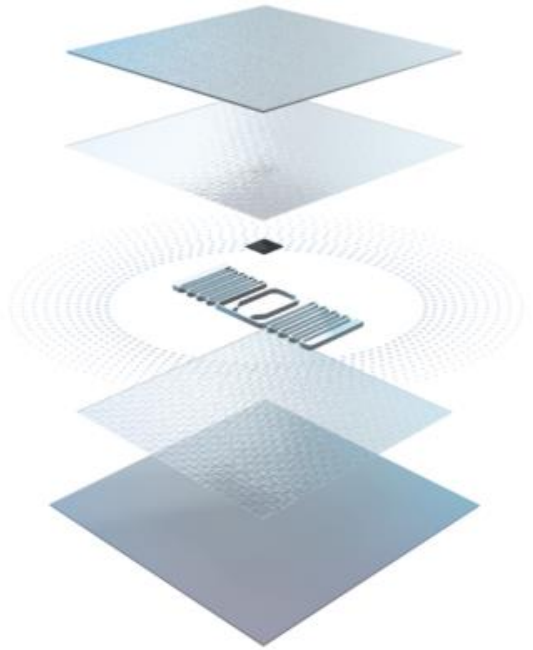
Generally, there are three main classifications of RFID tags. These are:

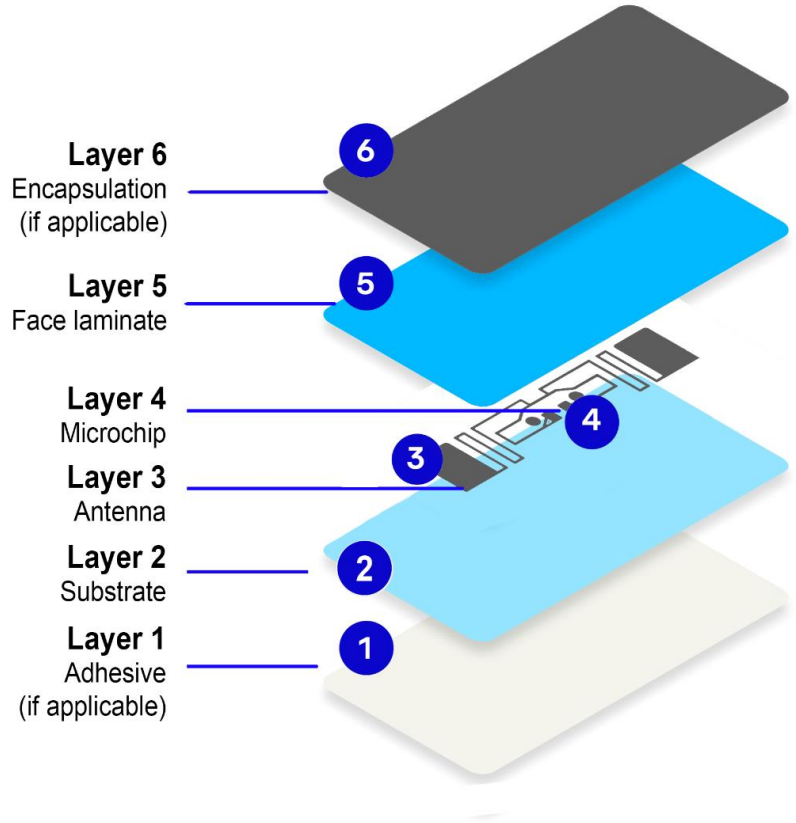
1. Active tags
2. Passive tags
3. Semi-passive (or battery-assisted) tags

Transmitter / Receiver	Antenna	Radio Signal	RFID Tag	Passive RFID
Receiver	Antenna	Radio Signal	RFID Tag	Active RFID

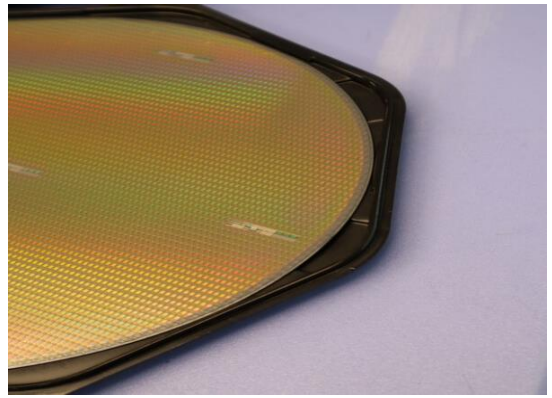
what’s inside an RFID label?

The following three RFID components come together to form what we'd call an 'RFID inlay,' a super slim piece of technology that can be inserted into garments, stickers, or labels.





Microchip



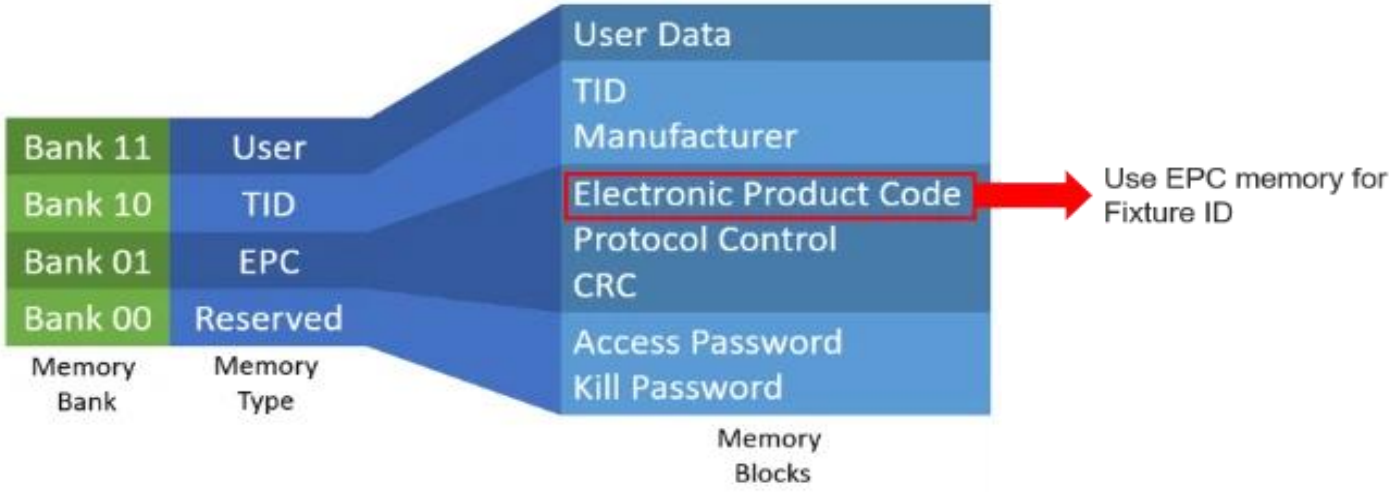
RFID chips are tiny electronic devices usually made of silicon.

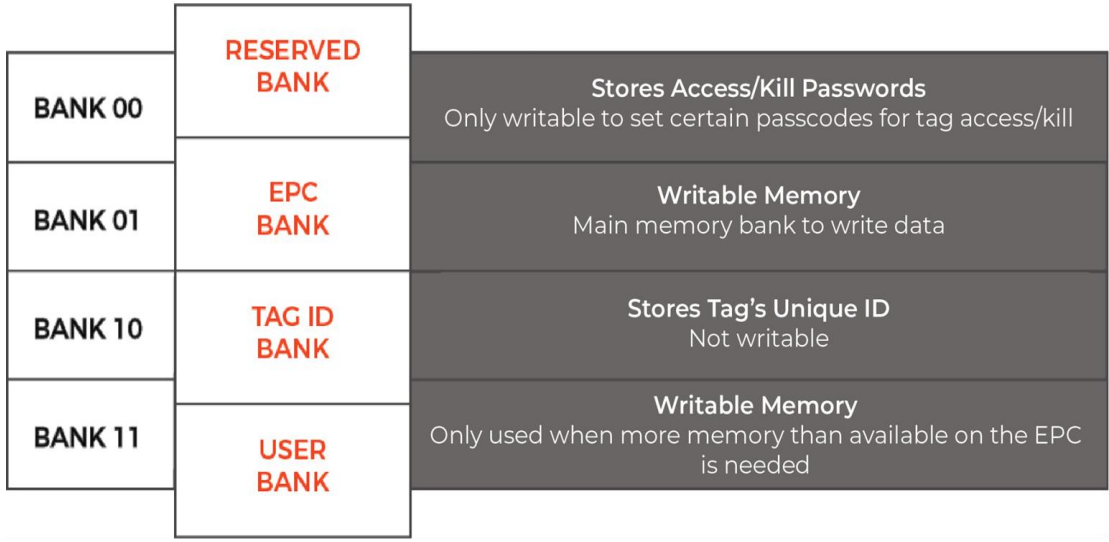
- They have a small amount of memory, which is used to encode the chip with unique product information. The chip's memory also stores information like purchase history and the product's movements through the supply chain.

- The most common RFID chips are 'passive,' which means they don't have a power source. They activate when scanned by a 'reader' (like a handheld scanner) which sends a small amount of energy through the chip via the antenna.

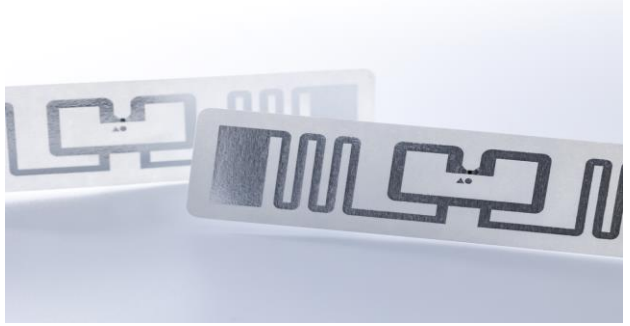
An Integrated Circuit (IC)/ RFID Chip.

This is the part of the tag that stores data. Each IC has four memory banks – **User, EPC, TID, and Reserved**.





Antenna



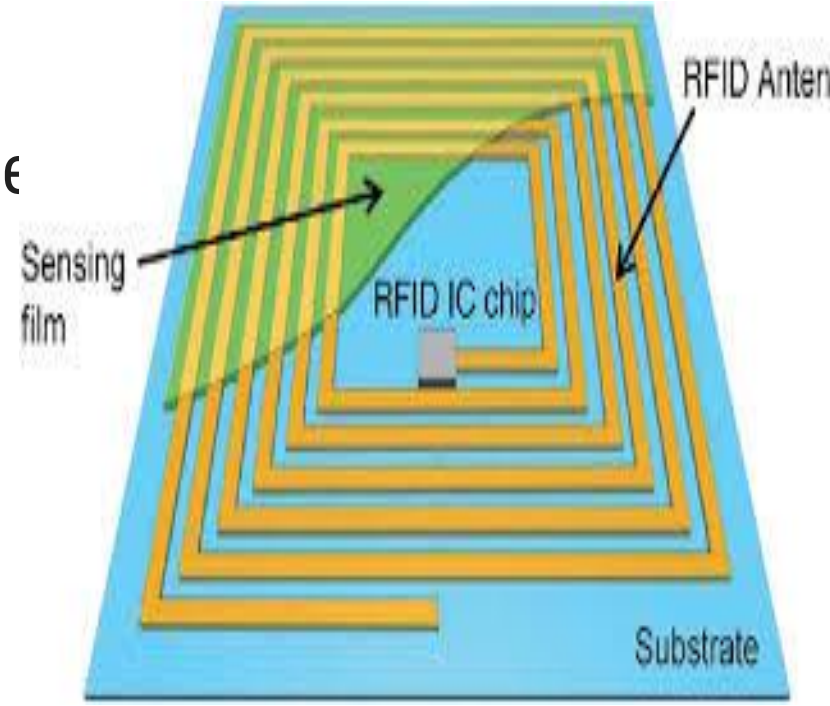
RFID antennas are the distinctive coiled or looped section of the inlay.

- Antennas are usually made of conductive materials like copper or aluminum. They can also be printed onto your labe or inlay using conductive ink.

- Radio waves activate the antenna from a reader (AKA scanner). It responds by pinging the chip's info back to the reader.

- Without the antenna, the RFID chip has no power, and its stored info can’t be accessed or updated.

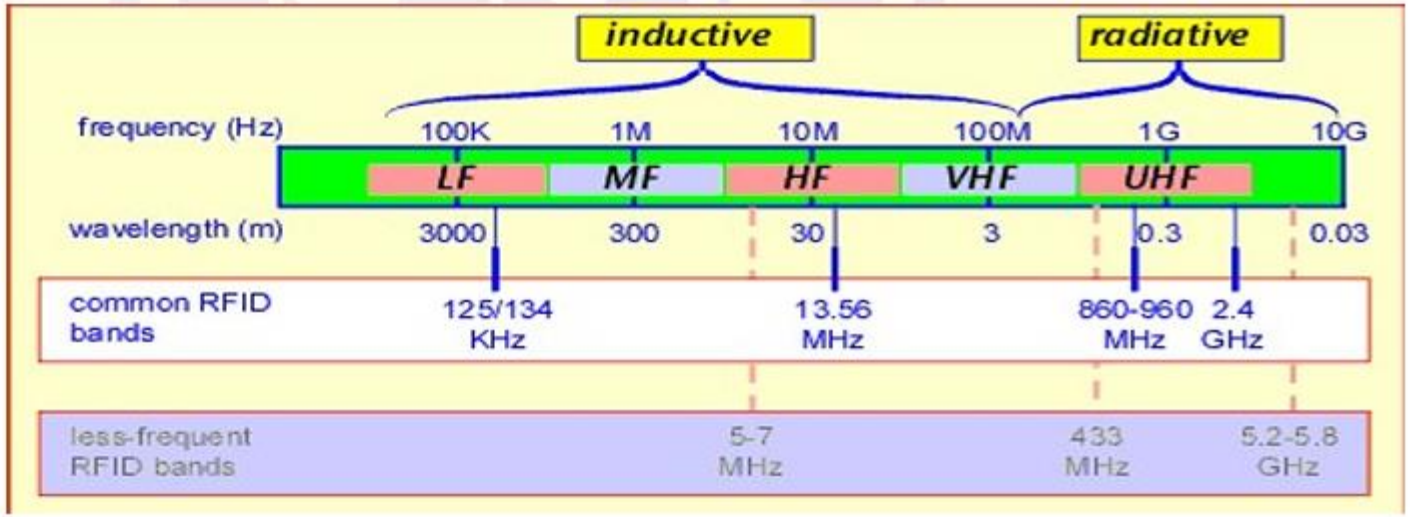
RFID antennas are responsible for converting the signals released by an interrogator into waves later picked by RFID tags.



RFID (Radio Frequency Identification)

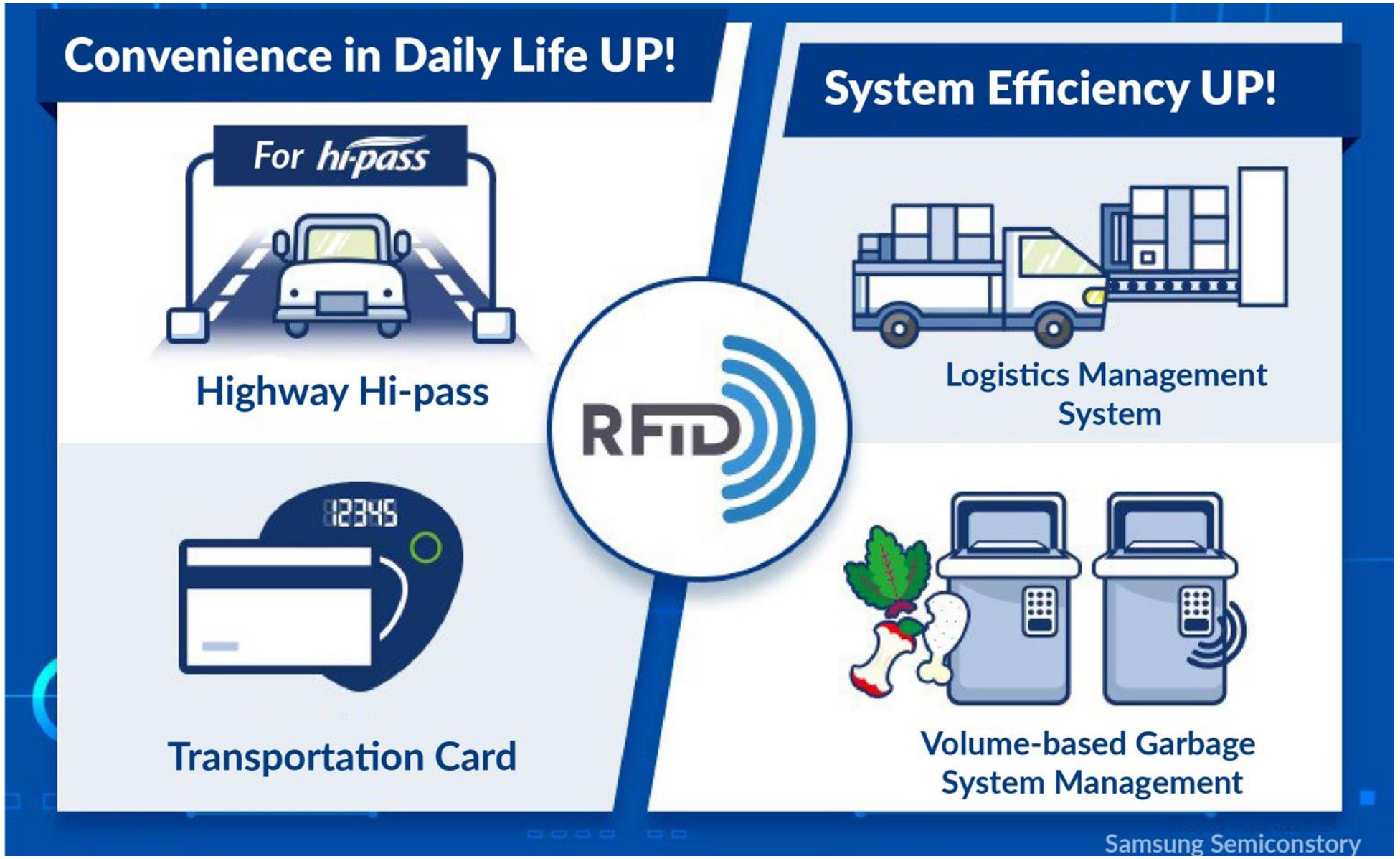
- Appeared first in 1945
- *Features*: Identify objects, record metadata or control individual target
- More complex devices (e.g., readers, interrogators, beacons) usually connected to a host computer or network
- Radio frequencies from 100 kHz to 10 GHz
- *Operating*: reading device called a reader, and one or more tags

RFID Frequencies



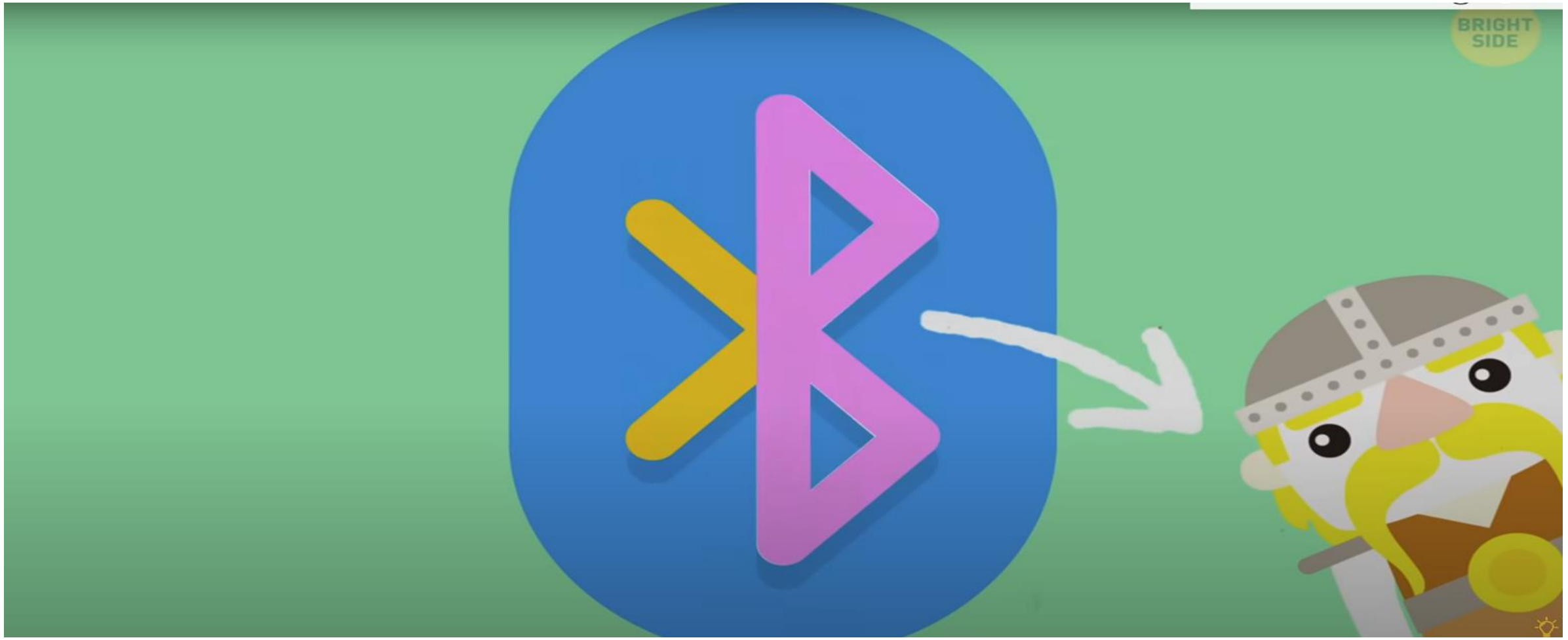
Frequency	Reading Range	Data speed	Common uses
Low Frequency	1-10 cm	Low	Animal tracking, automobile inventory
High Frequency	10 cm—1 m	Low to moderate	Contactless payment, shelf inventories
Ultra-high Frequency	Up to 12 m	Moderate	Supply chain management, defence applications

Application of RFID



Who invented bluetooth ?

Jaap Haartsen led the invention of Bluetooth® wireless technology. Used worldwide, Bluetooth allows a seemingly endless array of devices to wirelessly connect and communicate over short distances.



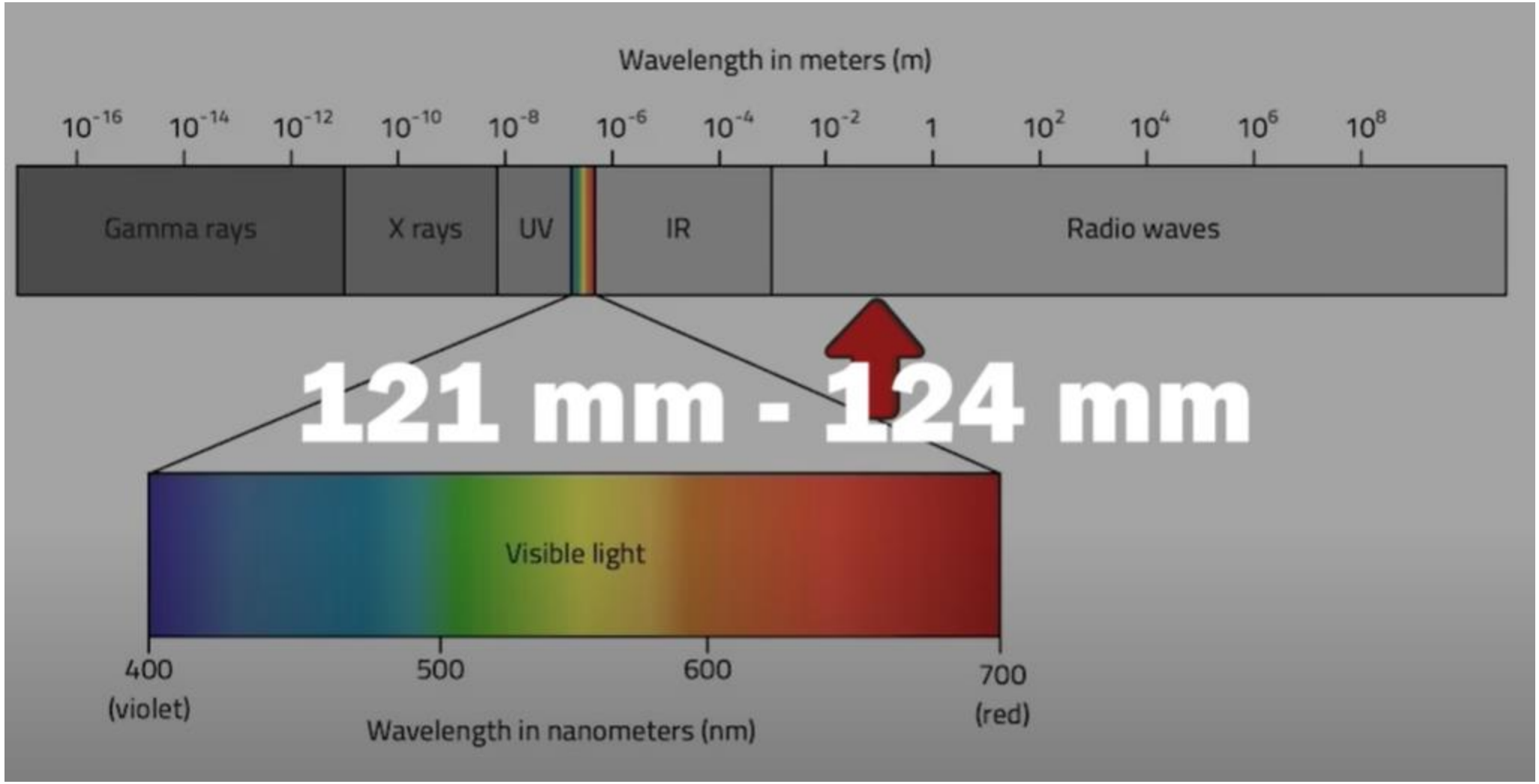
The Bluetooth logo is a combination of two Scandinavian runes that represent the initials of King Harald Bluetooth, who ruled Denmark in the 10th century:

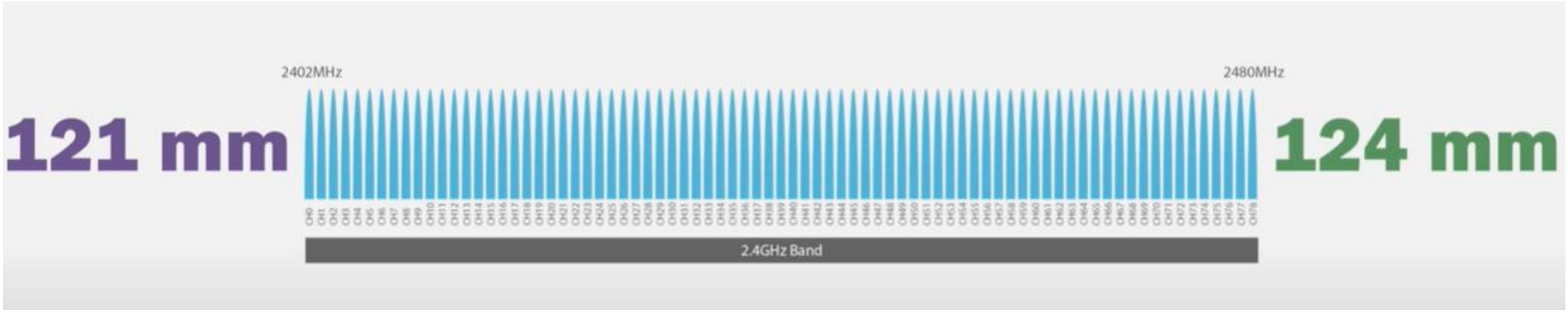
- **Hagal**: (ᚼ) represents the letter "H"
- **Bjarkan**: (ᛒ) represents the letter "B

What is bluetooth Technology ?

Bluetooth is a wireless technology that allows devices to communicate with each other without cables or wires. It uses short-range radio frequency to exchange data between devices that are close to each other

Ad-hoc networks


Wavelength in meters (m)
10^{-16} 10^{-14} 10^{-12} 10^{-10} 10^{-8} 10^{-6} 10^{-4} 10^{-2} 1 10^{2} 10^{4} 10^{6} 10^{8}
Gamma rays
X rays
UV
IR
Radio waves
121 mm - 124 mm
Visible light
400 (violet)
500
600
700 (red)
Wavelength in nanometers (nm)


2402MHz
2480MHz
121 mm
124 mm
2.4GHz Band

1600 hoping rate

Bluetooth uses FHSS (Frequency Hopping Spread Spectrum).

BLUETOOTH

- **Low Power** wireless technology
- **Short range** radio frequency at **2.4 GHz** ISM Band
- Wireless *alternative* to wires
- Creating **PANs** (*Personal area networks*)
- Support Data Rate of 1 Mb/s (data traffic, video traffic)
- Uses frequency-hopping spread spectrum

Class	Maximum Power	Range
1	100 mW (20 dBm)	~100 m
2	2,5 mW (4 dBm)	~10 m
3	1 mW (0 dBm)	~1 m

Piconet

Piconet is a type of Bluetooth network that contains one primary node called the master node and seven active secondary nodes called slave nodes.

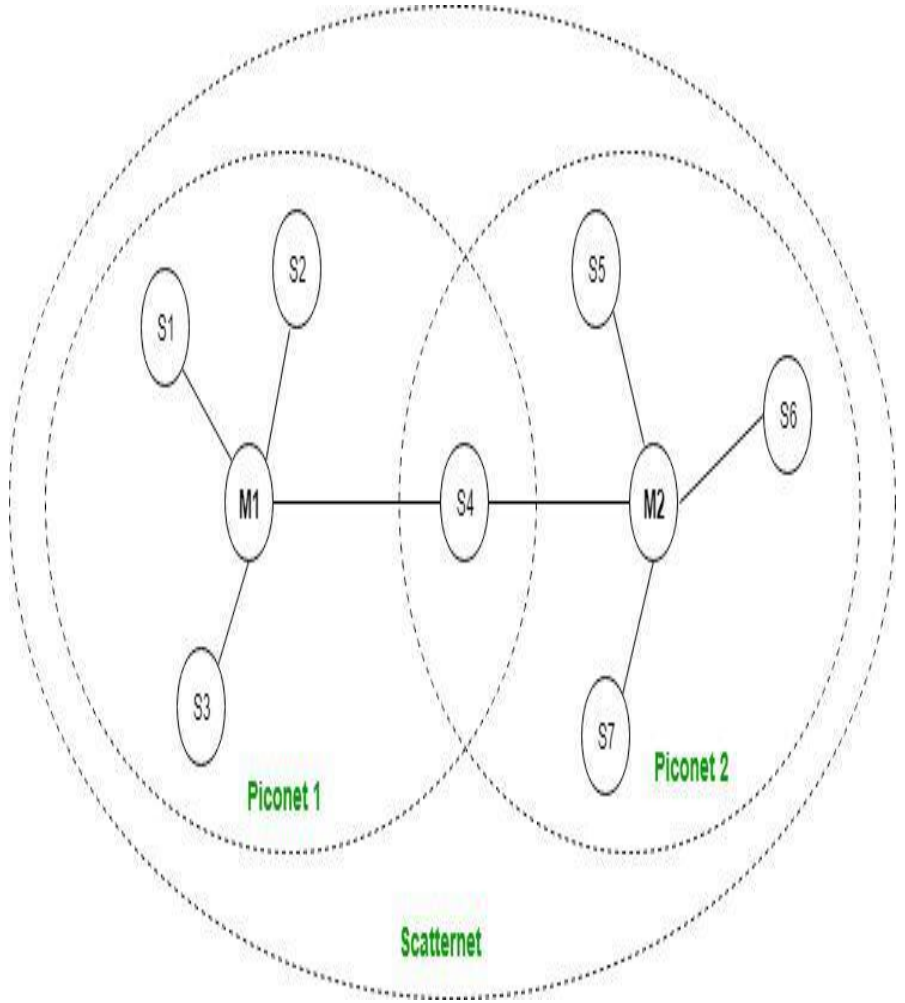
Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters.

The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. I

t also has 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

Scatternet

- It is formed by using various piconets.
- A slave that is present in one piconet can act as master or we can say primary in another piconet.
- This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master.
- This type of node is referred to as a bridge node.
- A station cannot be mastered in two piconets.



Architecture of Bluetooth

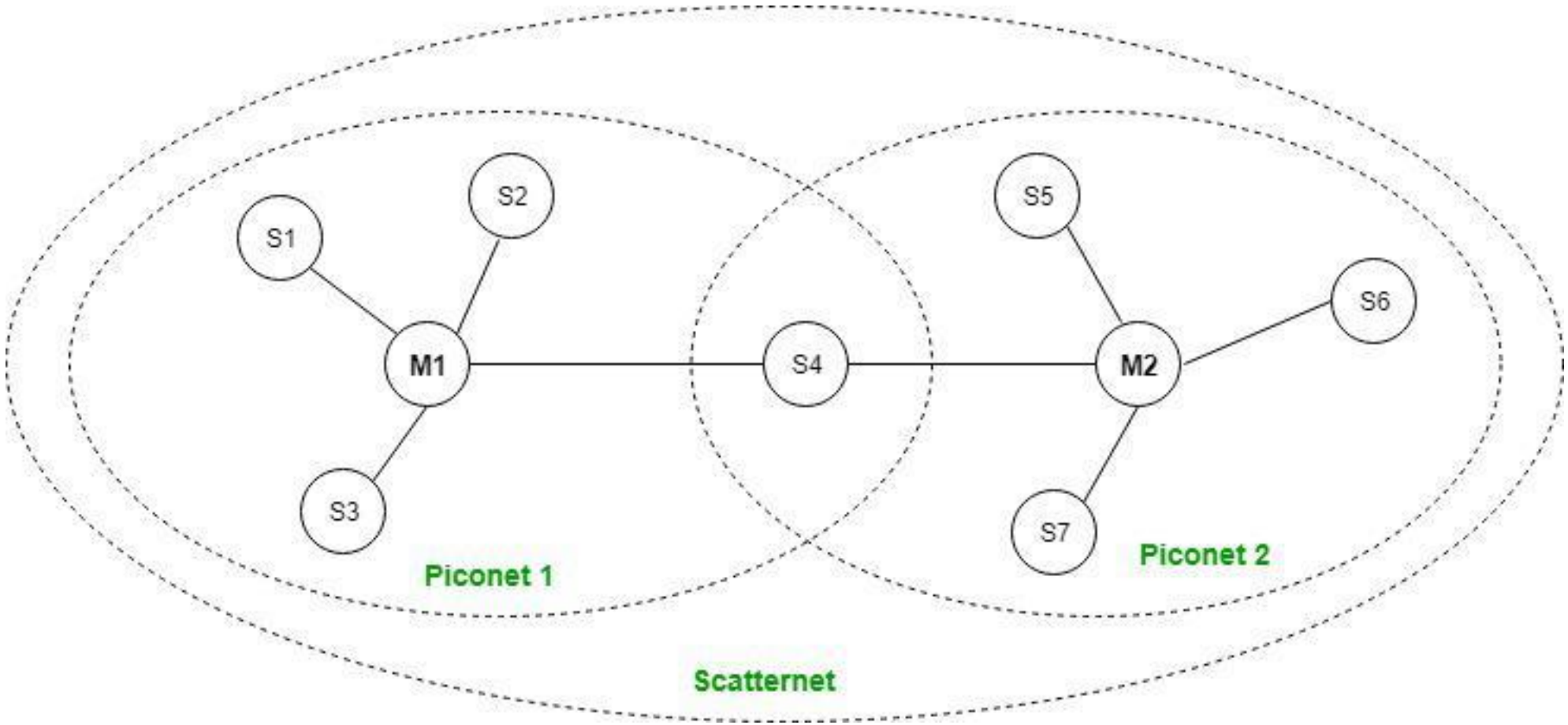
The architecture of Bluetooth defines two types of networks:

Piconet

Piconet is a type of Bluetooth network that contains one primary node called the master node and seven active secondary nodes called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

Scatternet

It is formed by using various piconets. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.


S1
S2
S3
M1
S4
S5
S6
S7
M2
Piconet 1
Piconet 2
Scatternet

Bluetooth Low Energy

- Enables IoT features
- Lowest cost and Easy to implement
- Discovery & connection improvements
- Low latency, fast transaction (3 ms from start to finish)
- Data Rate 1 Mb/s: sending just small data packets
- **Bluetooth 5**: 4x range, 2x speed and 8x broadcasting message capacity.

- **Bluejacking** - sending unsolicited messages (text, images, sounds) to nearby Bluetooth devices.
- **Bluesnarfing** - Any unauthorized access to or theft of information. A bluesnarfing attack can access information, such as email, contact lists, calendars, and text messages.
- **Bluebugging** - Bluebugging attacks allow an attacker to take over a mobile phone. Attackers can listen in on phone conversations, enable call forwarding, send messages, and more.

How to Stop Bluetooth Attacks

- Turn off Bluetooth on your device or make your device undiscoverable.
- Stop passive connections.
- Never accept a pairing request from a source you do not know or trust.
- Mind your surroundings.

Hedy Lamarr and George Antheil
Hedy Lamarr (1914-2000) and George Antheil (1900 – 1959) invented a system which allowed radio waves to jump onto different frequencies.

The idea was originally to stop the US Navy's radio signals from being jammed by their enemy in World War 2.

Dr John O'Sullivan led a team of scientists in Australia who worked on groundbreaking technology to reduce the echo of radiowaves. This led to the development of the wireless LAN.

Vic Hayes is often called the Father of Wi-Fi.

Vic Hayes is often called the Father of Wi-Fi. He was the head of the committee that introduced the international standard for wireless networking in 1997.

What is Wi-Fi?

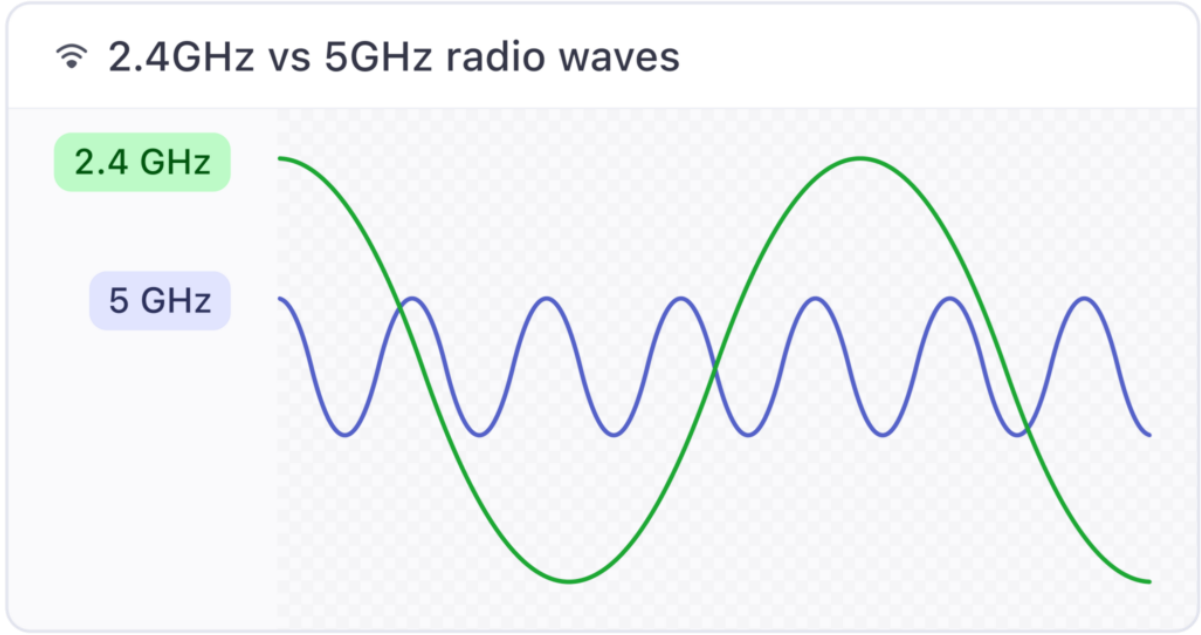
Wi-Fi is a wireless networking technology that allows wireless devices such as laptops and mobile phones to access the internet.
It’s also known as WLAN which is short for wireless local area network.

Most people use a small wireless router to connect to the internet.

Bluetooth	Wi-Fi
Used for connecting devices to each other.	Used for connecting devices to the internet.
Slower transfer rate and shorter range.	Faster transfer rate and longer range.
Uses less power / longer battery life.	Uses more power / shorter battery life.
Less vulnerable to interference.	Vulnerable to interference.
Simpler to use / no password.	Often requires a password.

What radio frequencies are used for Wi-Fi?

Currently, radio frequencies of 2.4 gigahertz and 5 gigahertz are used.



Wi-Fi (IEEE 802.11)

Type: Wireless Local Area Network (WLAN)

Transport: TCP/IP

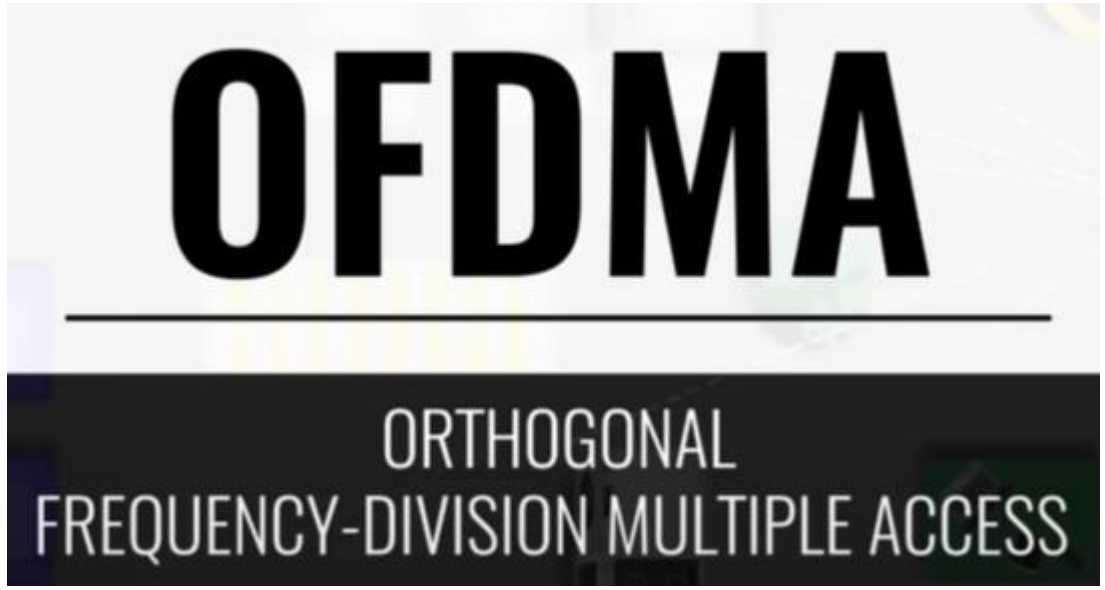
Key Features:

- **High Bandwidth:** Suitable for IoT applications that require fast data transfer (e.g., video streaming).
- **Infrastructure:** Ubiquitous in homes and businesses, providing seamless integration with existing networks.
- **Power Consumption:** Typically higher compared to protocols like BLE or Zigbee, making it less ideal for battery-powered devices.
- **Line-of-Sight Range:** Up to 100 to 150 meters (328 to 492 feet).

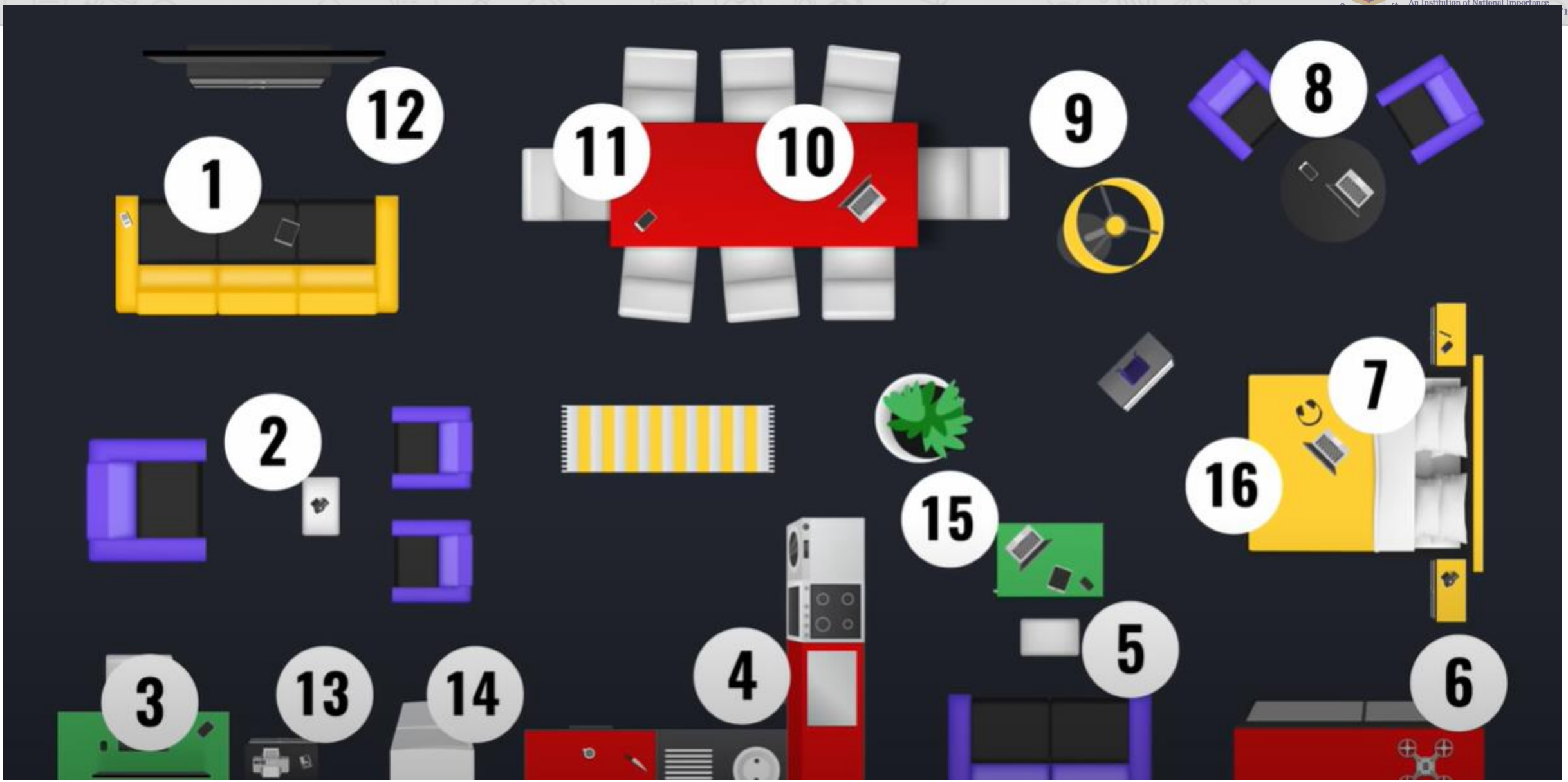
Wi-Fi 1	802.11b	1999
Wi-Fi 2	802.11a	1999
Wi-Fi 3	802.11g	2003

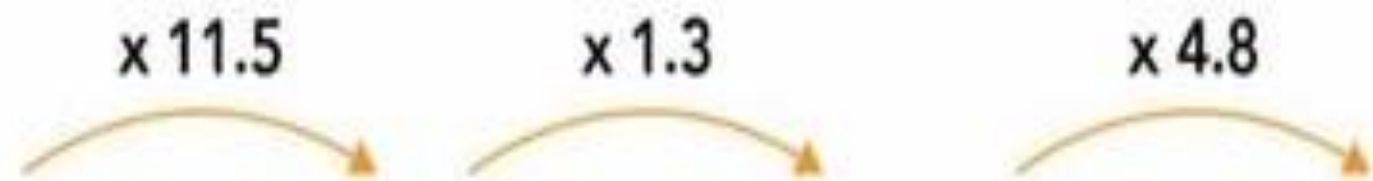
IEEE Standard	Versions	Time	Frequency Band	Security	Maximum Theoretical Speed
802.11n	Wi-Fi 4	2008	2.4 / 5 GHz	WPA 2	600 Mbps
802.11ac	Wi-Fi 5	2014	5 GHz	WPA 2	6.9 Gbps
802.11ax	Wi-Fi 6	2019	2.4 / 5 GHz	WPA 3	9.6 Gbps
802.11ax	Wi-Fi 6E	2020	6 GHz	WPA 3	9.6 Gbps
802.11be	Wi-Fi 7	2024	2.4 / 5 / 6GHz	WPA 3	46 Gbps

TFT - Target Wake Time



MU-MIMO





	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6/6E	Wi-Fi 7
Standard	802.11n	802.11ac	802.11ax	802.11be
Max Speed with 1 Spatial Stream	150 Mbps	866.7 Mbps	1.2 Gbps	2.9 Gbps
Max Speed with 2 Spatial Streams	300 Mbps	1.73 Gbps	2.5 Gbps	5.8 Gbps
Max Speed with Max # Spatial Streams	600 Mbps	6.92 Gbps	9.6 Gbps	46.4 Gbps

Summary

- IoT refers to the interconnection of computing devices embedded in everyday objects via the Internet, enabling them to send and receive data.
- IoT is not owned by any one engineering branch. It is a reality when multiple domains join forces and combine efforts.
- IoT is all about providing service to any device, anywhere, anybody, and any network.
- IoT has certain characteristics which are important: a. Connectivity. b. Intelligence and identity. c. Scalability. d. Dynamic and self-adapting (complexity). e. Safety.
- “Things” refer to variety of devices. At times, even humans in the loop becomes a thing. For anything to qualify as a “thing”, it requires identity. The “thing” can monitor, measure, etc.; for example, a temperature sensor could be a “thing”.
- One should understand that “THINGS” = HARDWARE + SOFTWARE + DATA + SERVICE
- IoT stack has seven layers, starting with sensor layer and ending with application layer just as OSI.

Summary

- Security/personnel safety, privacy, data extraction with consistency from complex environments, connectivity, power requirements, complexity involved, and storage are the major challenges we face while building an IoT application.
- IoT application can be classified as Level 1, 2, 3, 4 or 5 based on the complexity and architecture involved.
- IoT is all about sense, connect, store, analyze, control and sharing.
- Physical design indicates importance and role of each physical component in IoT Ecosystem.
- Logical design presents logical data flow between source and destination of data.
- At last, key properties are presented to showcase fundamental properties of a robost IoT system.