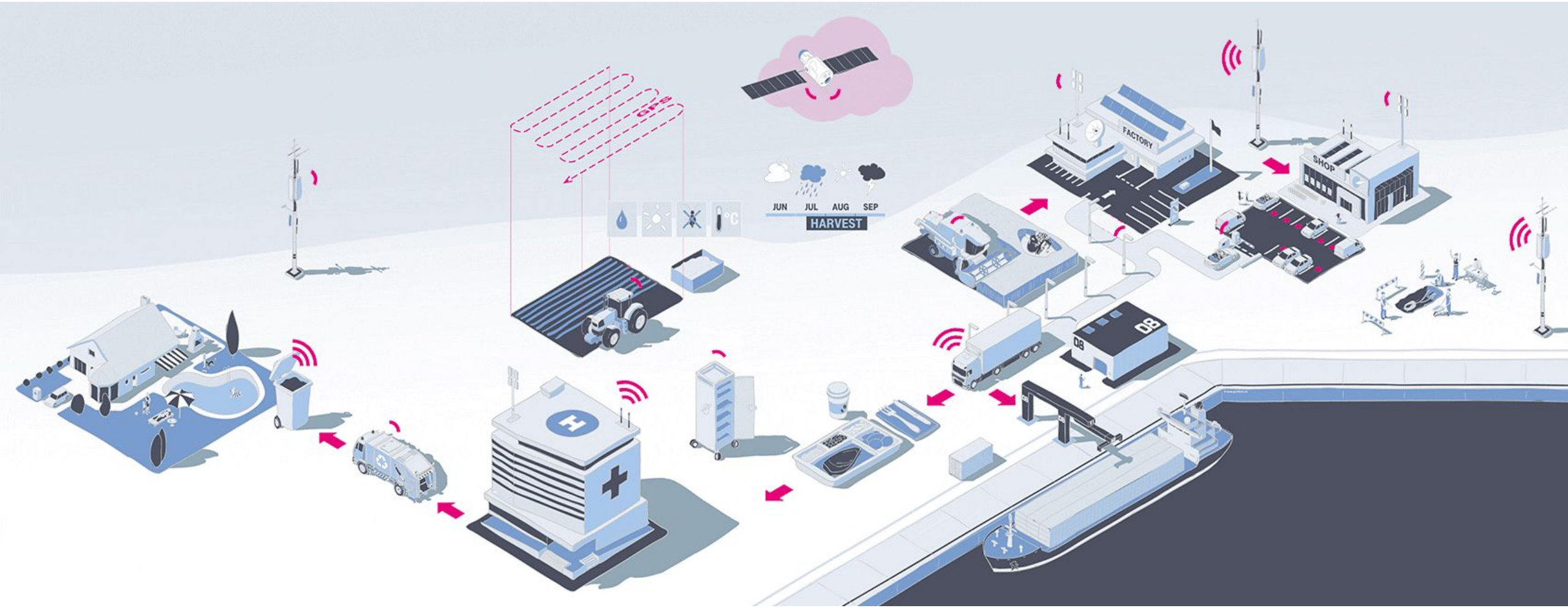
IoT

Md. Mahedi Hassan
Lecturer, CSE
Daffodil International University

IOT

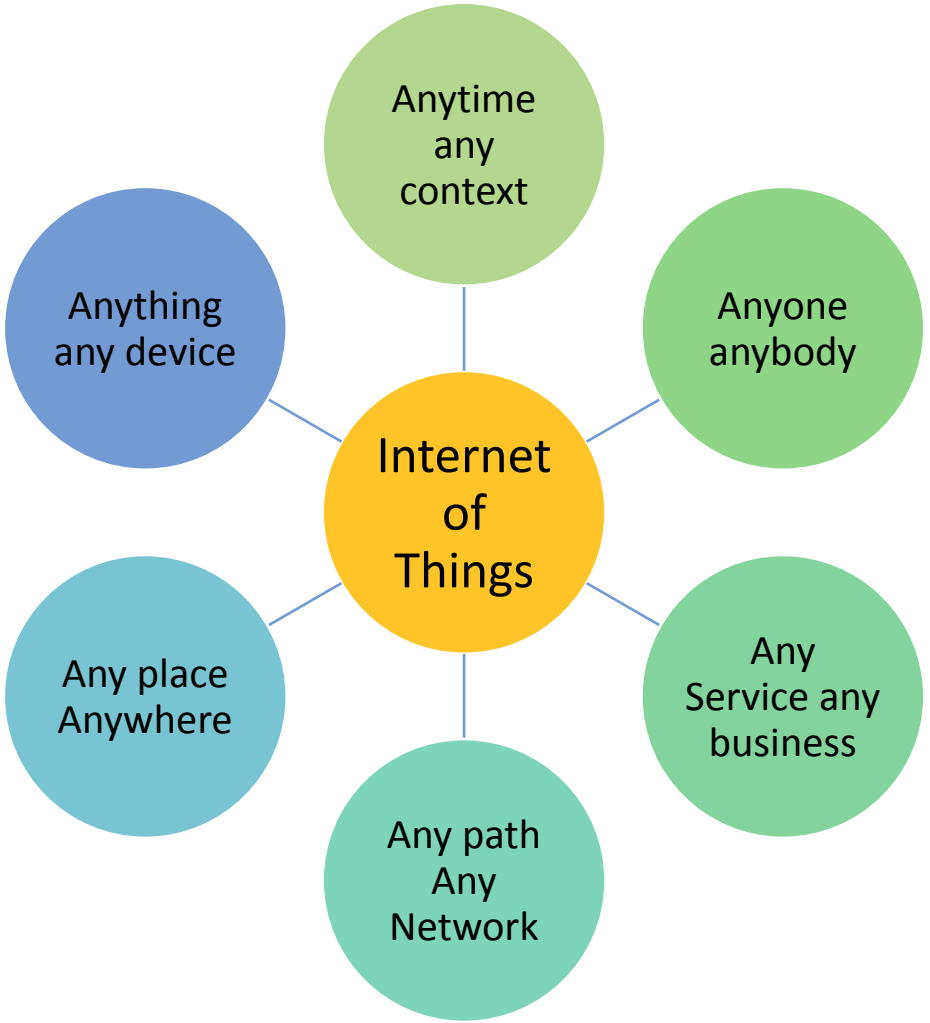


A phenomenon which connects a variety of things

-----Everything that has the ability to communicate

Any-**X** Point of View

The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/ network and Any service.



IoT Protocol

Single devices like smartphones and personal computers also use network protocols for communication. But general protocols that are used by these personal devices might not meet specific requirements like bandwidth, latency, and range of IoT-based solutions. Hence, a few improved versions of existing protocols and some new IoT protocols are evolved to meet the requirements of IoT devices.

IoT protocols and standards are broadly classified into two separate categories.

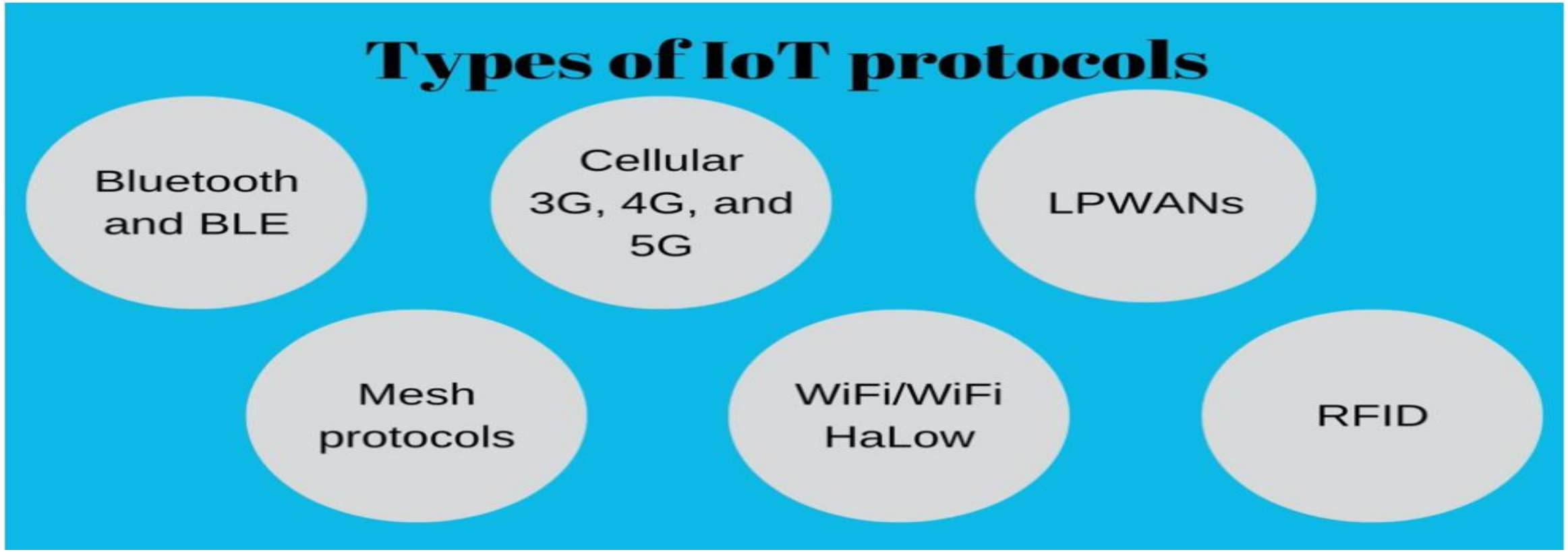
These are:

1. **IoT data protocols (Presentation / Application layers)**
   IoT data protocols are used to connect low-power IoT devices. They provide communication with hardware on the user side – without the need for any internet connection. For instance: **MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol) etc.**

1. **Network protocols for IoT (Datalink / Physical layers)**
   IoT network protocols are used to connect devices over a network. These sets of protocols are typically used over the internet. Here are some examples of various IoT network protocols. For instance: **WiFi, Bluetooth, ZigBee, Z-Wave etc.**

Six types of IoT protocols and network standards:

Devices are generally connected to the internet with an IP (internet protocol) network. But, devices can also be connected locally via Bluetooth or NFC (near-field communication). The differences between both types of connections are power, range, and memory used. IP connections are complex and require increased power and memory, but there are no range limitations. Bluetooth connections, on the other hand, are simple and require less power and memory, but the range is limited. There are many different types of IP and Bluetooth protocols that IoT devices can use.



❑ Bluetooth and BLE

Bluetooth is a 2.4GHz network for personal wireless network communication. 2.4GHz network is preferred for providing personal networks by network providers as it is cheaper and has a much better range than other networks. Bluetooth low energy (BLE) is the new and optimized version of Bluetooth for connections between IoT applications. BLE consumes lesser power than standard Bluetooth for communication. BLE-enabled devices are commonly used with electronic devices that can act as a hub for data transfer from IoT devices to the cloud. This makes BLE a perfect match for IoT wearables. BLE is widely integrated into health and fitness trackers, as well as some smart home devices like door locks. Data from BLE-enabled IoT wearables can be easily communicated to smartphones.

❑ Cellular (3G, 4G, and 5G)

Cellular networks, as the name suggests, are well-established in the mobile consumer market. 2G is an “old school” cellular network that, along with 3G, is being phased out in most parts of the world. But, the world is quickly embracing new high-speed cellular networks like 4G and 5G. Cellular networks provide high bandwidth and reliable broadband communication for voice calls or video streaming but with high operational costs and power consumption. Cellular networks cannot be used with most IoT devices due to their frequency, range, and security challenges. However, cellular networks can be viable options in some specific IoT devices like connected cars. Connected cars can use cellular networks for traffic routing with the help of GPS systems. GPS systems and cellular networks can help track road traffic in real-time as cellular networks can transfer high quantities of data over the network.

❑ LPWANs

LPWANs (Low Power Wide Area Networks) are new sets of protocols developed for IoT solutions but can also be used by other devices to communicate over a wide area. Even cellular networks can provide a wide-area communication network, but the cost of communication over cellular networks is high because of its high power consumption. LPWANs enable communications over wide area with the help of small and inexpensive batteries that can last for long-term making it a cost-saving option in comparison with cellular networks.

Mesh protocols

A mesh usually refers to a rich interconnection network of devices that are made up of devices organized in a mesh topology. Mesh topology is a networking infrastructure in which all connected devices can cooperate to transfer and share data amongst each other.

ZigBee is one of the most popular mesh protocols used for IoT applications. It is a short-range, low-power protocol that is commonly deployed to extend communication over multiple IoT devices

WiFi/WiFi HaLOW

Everyone would know what WiFi is because of its pervasiveness in both industrial and home environments. However, WiFi is not used with most of the IoT devices. Except for a few applications like digital signages and security cameras, WiFi does not provide a feasible option for IoT connectivity. The use of the WiFi network is limited in IoT devices, mainly because of its low range, high power consumption, and low scalability. A lesser-known derivative of WiFi known as WiFi HaLow is introduced for IoT devices

RFID

RFID (Radio-frequency identification) uses radio waves to transfer small data packets over the network within small areas. It is easy to embed an RFID chip in IoT devices. RFID readers can then read the tags and give information about the product that is attached to tags. One of the common applications of RFID is inventory management. By attaching RFID tags to all products and connecting it to IoT devices, businesses can keep track of the number of products available in stock. Thus RFID can help in better stock planning leading to an optimized supply chain management. RFID tags can also help smart home IoT devices. For instance, a smart washing machine that can read RFID tags can be controlled.

Communication Models in IoT

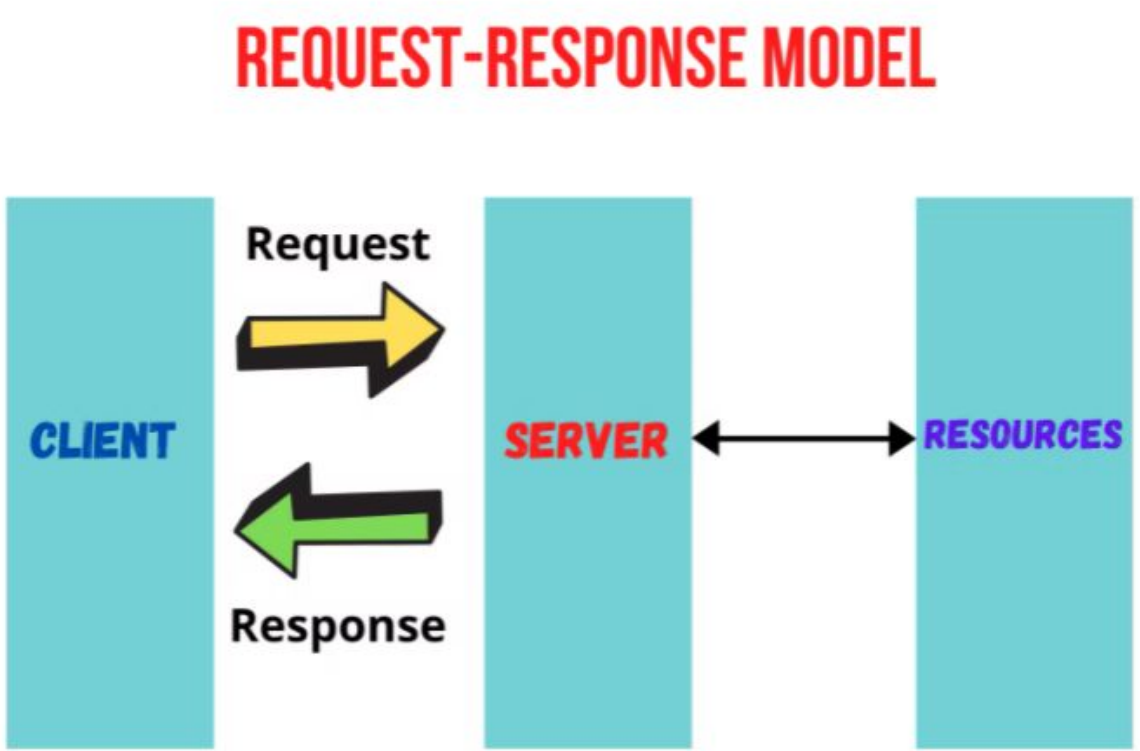
Understanding how the different IoT devices communicate with each other is important and useful cause IoT devices are found almost everywhere now. Communication models are the way to understand it. IoTs enable people and things to be connected anytime, in any space, with anything and anyone, through any network and service.

Now let us understand the different communication models in IoT.

Request & Response Model

- The communication takes place between a client and a server.
- Whenever required, the client will request information from the server. This request is usually in the encoded format.
- So in this model, basically a client sends requests to the server and the server responds to the requests. That is why it is called as Request-Response model.
- After receiving the request from the client, the server decides how to respond, fetches the data from the database and its resource representation, prepares a response and ultimately sends the response to the client.
- Request-Response model is a stateless model. Each request-response pair is independent of others.

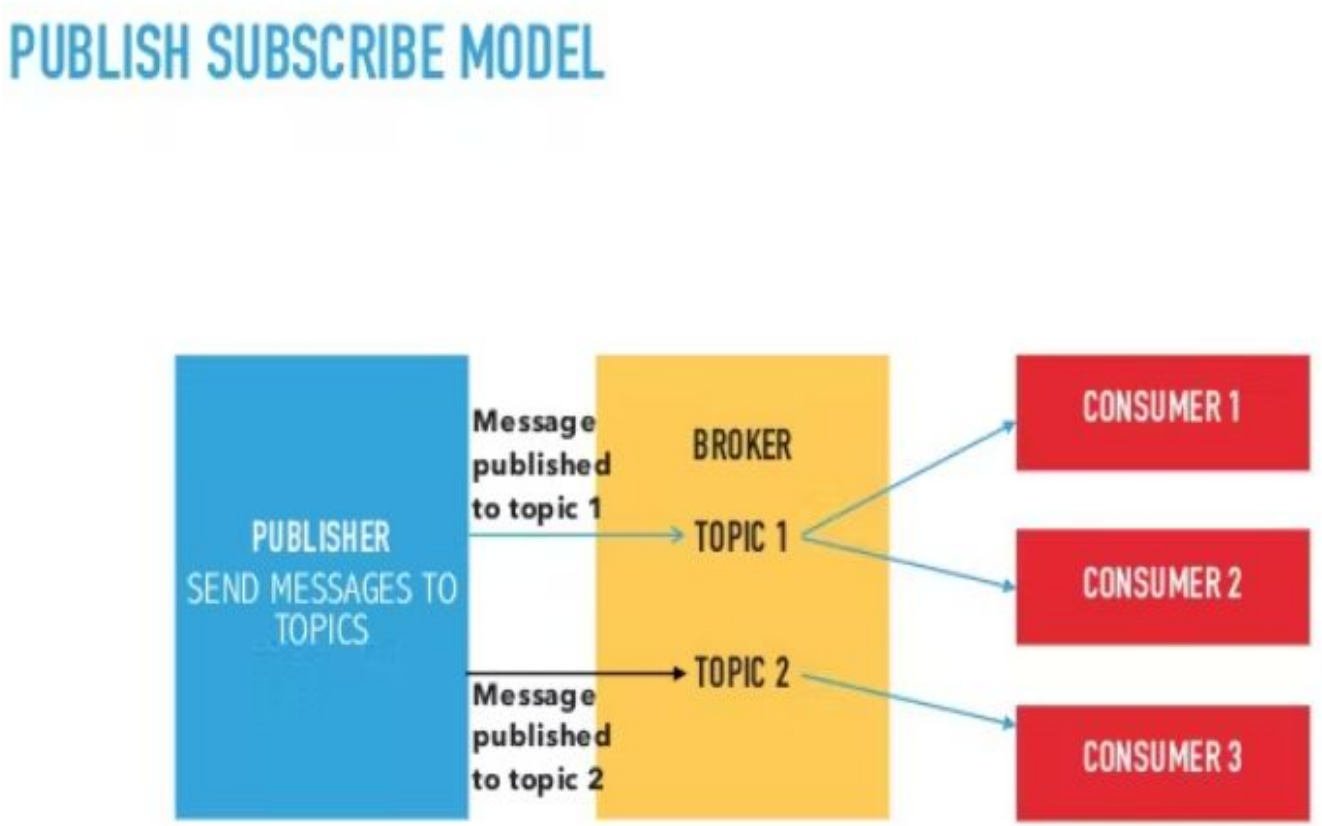
Example is HTTP, CoAP (Constrained Application Protocol)



Publish-Subscribe Model(Pub-Sub)

In this model, you will find three main entities:- Publisher, Broker and Consumer Let us see the roles of each of these 3 entities.

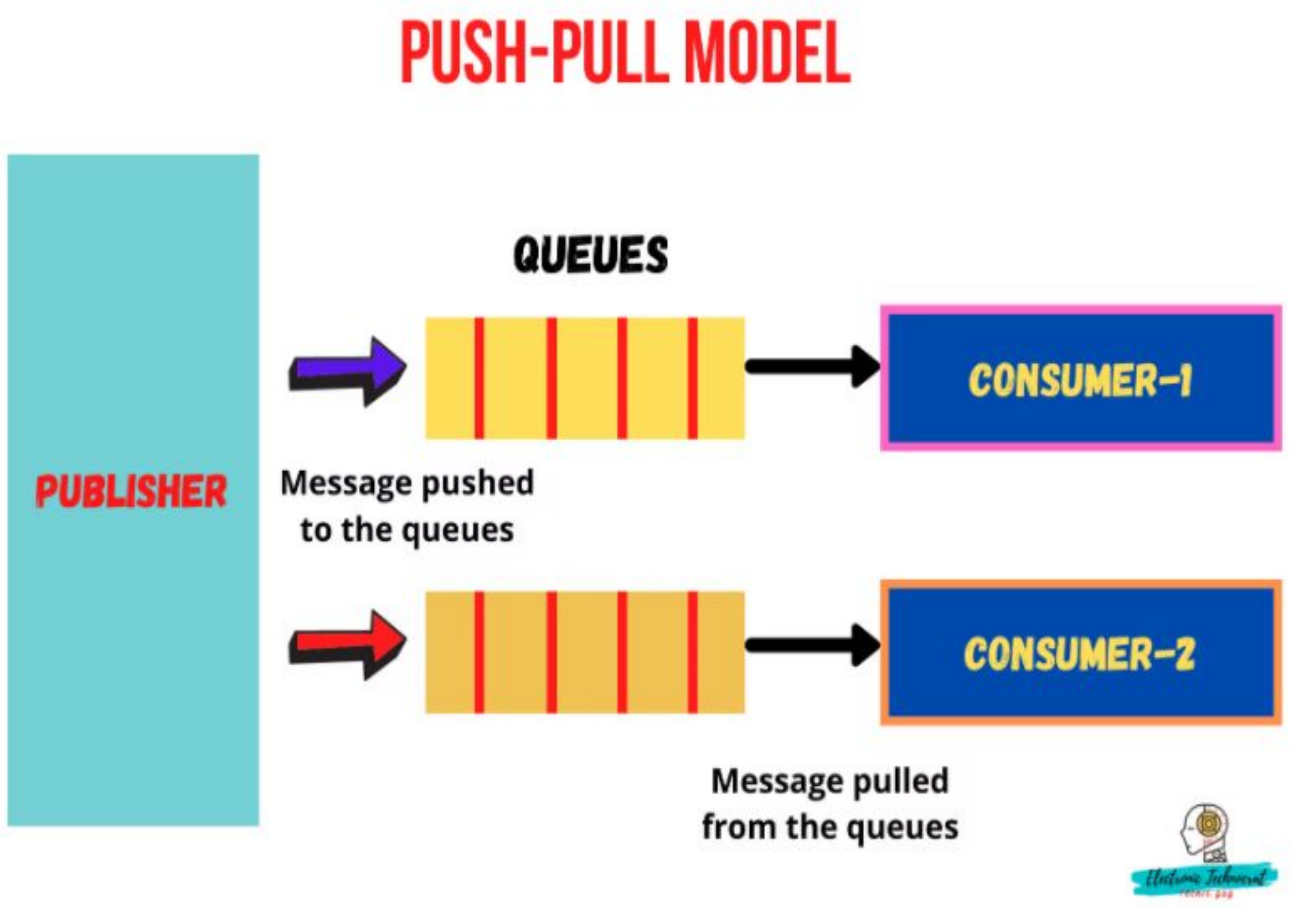
- Publishers, send the data to the topics that are managed by the broker. They are the source of data.
- The Man in the Middle, the Broker, has the responsibility to accept the data sent by the publisher and deliver that data to the consumers.
- What is the task of the Consumers? Consumers will subscribe to the broker-managed topics.
- Publishers aren't aware of who the consumers are.
- Once the data is published on a topic, the broker sends this message to all consumers who have subscribed to the specific topic. It works a bit like YouTube. When you subscribe to a channel and tap the Bell icon, you'll get notifications if the YouTube channel posts a video.



Push-Pull Model

Here too, we have 3 entities:- Publisher, Queues and Consumers.

- Push-Pull is a communication model where data producers push data into queues and consumers pull data out of queues.
- What are Queues? They are used to separate out single producer-consumer communication.
- At times, there might be some mismatch in the push-pull rates. Queues 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 consumer pull data. So they work as a buffer and flow control mechanisms whenever there is any mismatch in the push-pull rates.

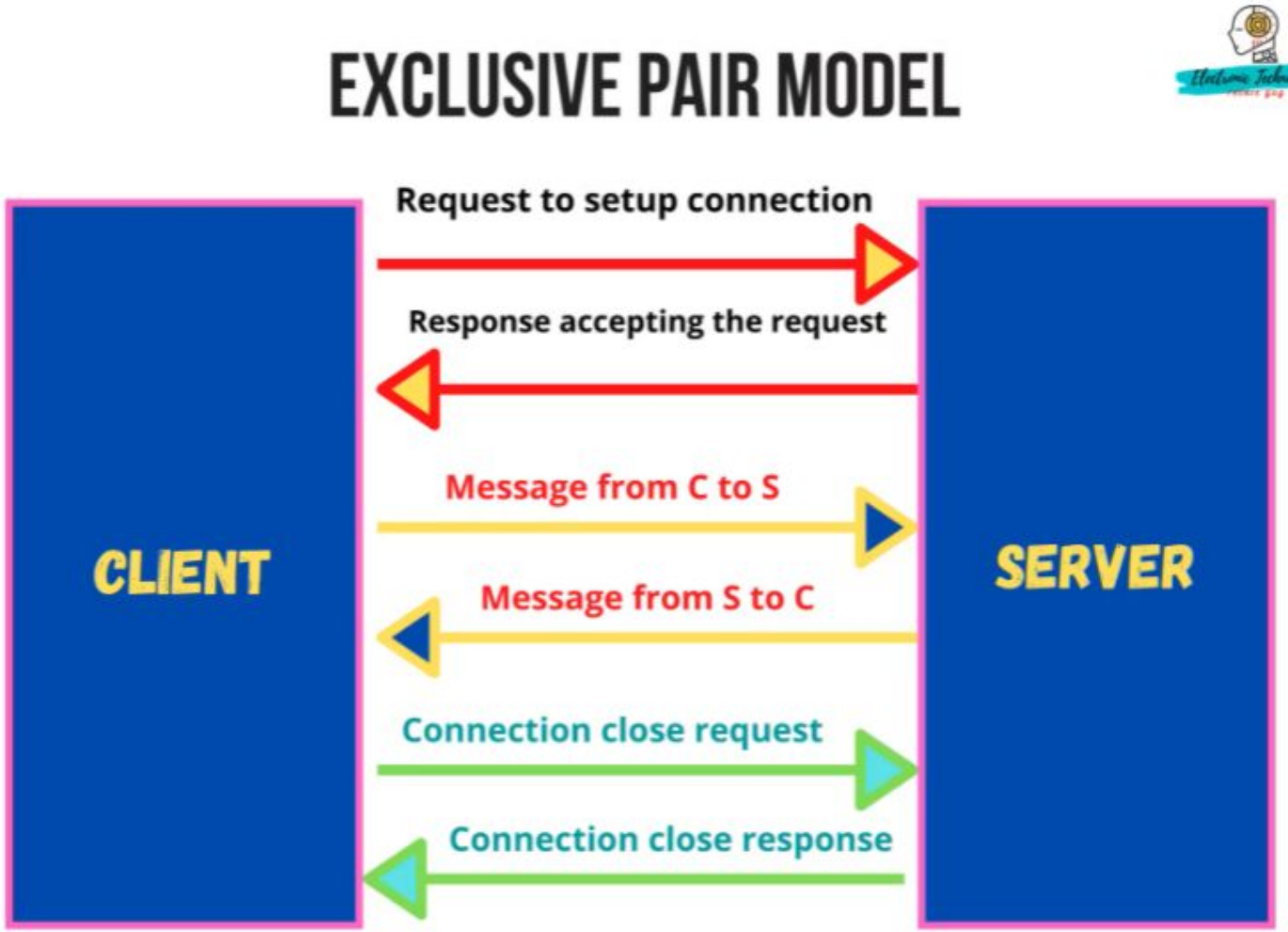


Exclusive Pair Model

It's a bi-directional, fully duplex communication model in which a dedicated communication link is set between the client and the server.

- The connection remains open until the client sends a request to close the connection.
- The client and server can send messages to one another after configuring the connection. As soon as the connection is terminated, no exchange of messages would take place between the client and the server.
- The Server has the record of all the connections which has been opened.
- This model is a stateful type.

Example:- Websockets.



IoT enabling Technologies

It is enabled by several Technologies including:

- Wireless sensor networks
- Cloud computing
- Big Data Analytics
- Embedded system
- Security protocols and architectures
- Communication protocols
- Web service
- Mobile internet and semantic search engine .

IOT Advantages

- **Improved Customer Engagement –** Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.
- **Technology Optimization –** The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.

IOT Advantages

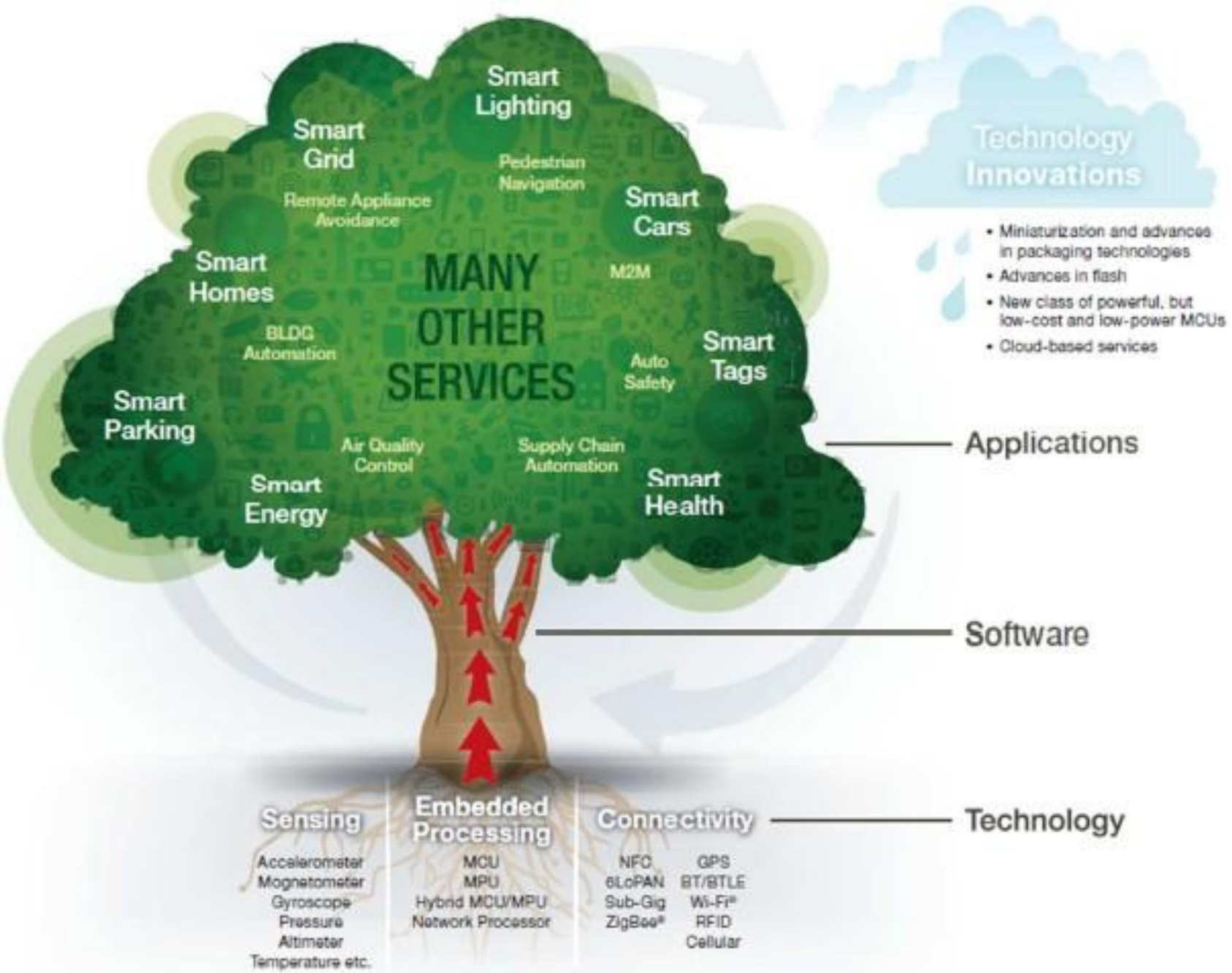
- **Reduced Waste –** IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.
- **Enhanced Data Collection –** Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

IOT Disadvantages

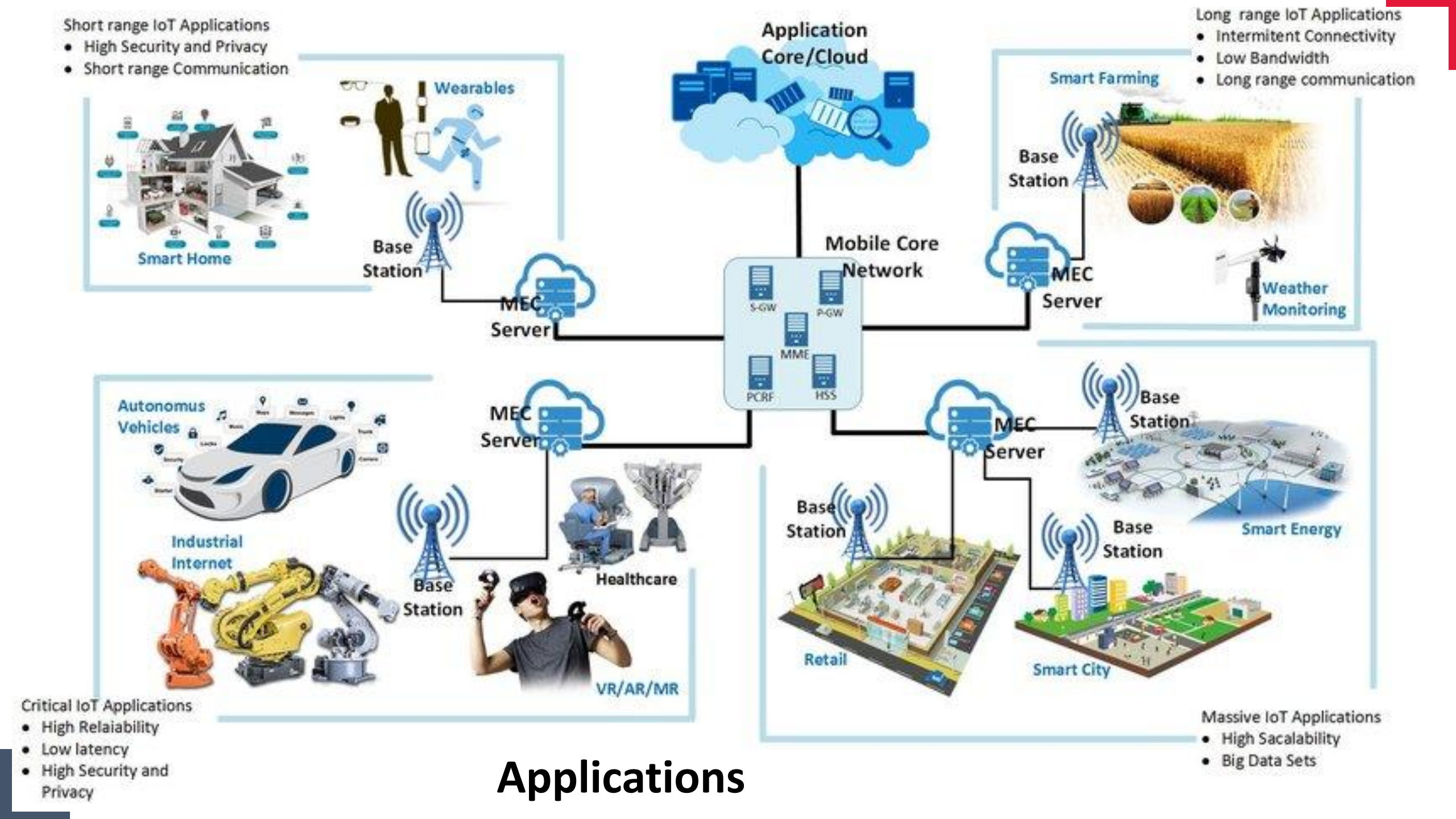
- **Security –** IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.
- **Privacy –** The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.
- **Complexity –** Some find IoT systems complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.

IOT Disadvantages

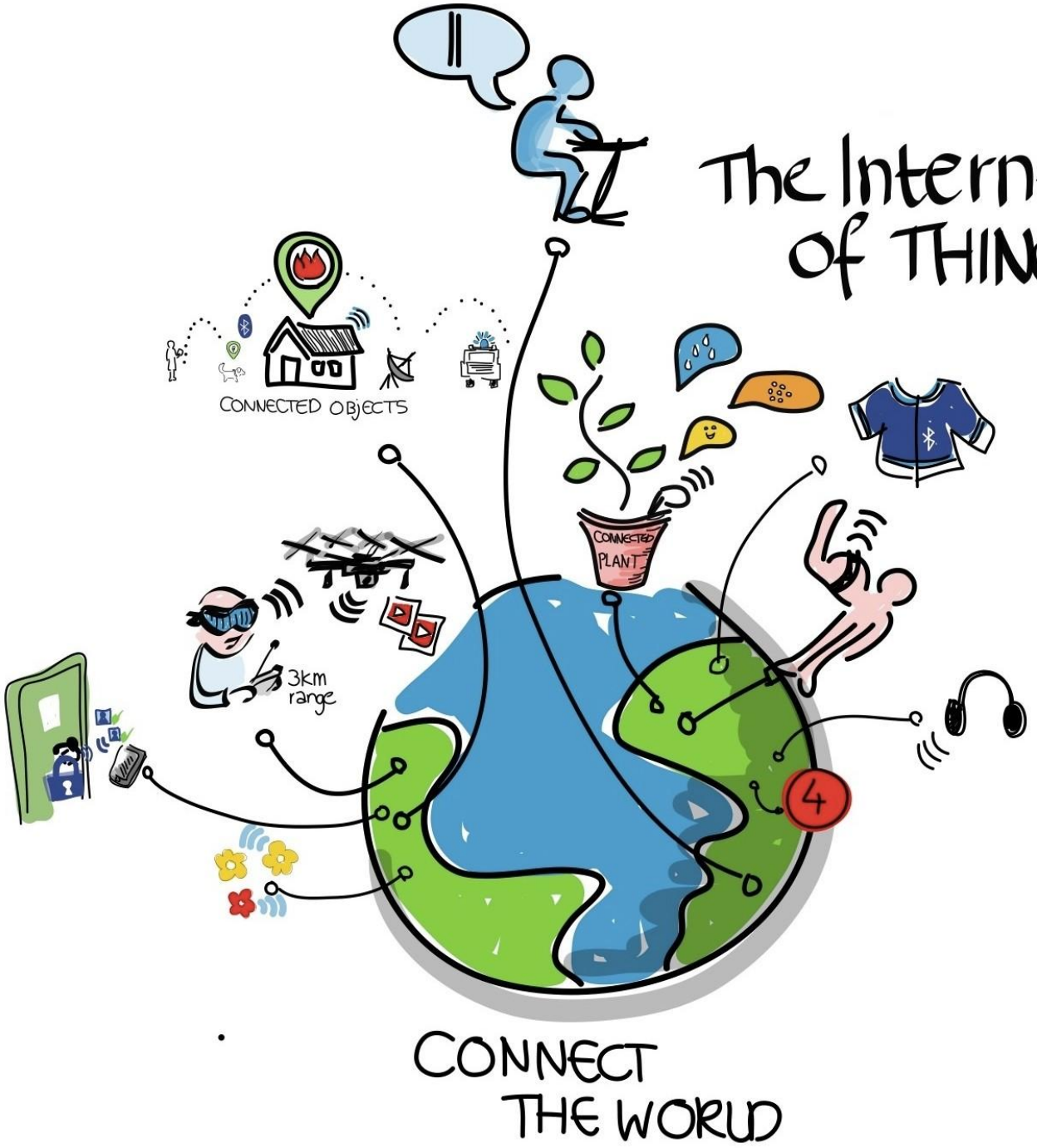
- **Flexibility –** Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.
- **Compliance –** IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.



Putting it All Together



Applications


The Internet of THINGS
CONNECTED OBJECTS
CONNECTED PLANT
3km range
4
CONNECT THE WORLD

THANK YOU