Unit – I Fundamental of IOT

#### IoT origins and history

The history of the term internet of things traces back to 1999, when it was coined by Kevin Ashton, co-founder of the Auto-ID Center at the Massachusetts Institute of Technology. Ashton, who was working on [supply chain optimization](https://www.techtarget.com/searcherp/definition/supply-chain-management-SCM) for Procter & Gamble, first used the term in a presentation about [RFID](https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification) (radio frequency identification).

The term internet of things didn't go mainstream until approximately 2010, however, due -- in part -- to the emergence of [Google's Street View](https://www.techtarget.com/whatis/definition/Google-Street-View). Street View provided end users with 360 pictures of the world from street-level and stored large quantities of data on end-user's wireless networks. This got people speculating that Google's long-term goal was to index the physical world (as an internet of things) as well as the internet.

IoT stands for internet of things. Most simply, it refers to physical objects linked through wired and wireless networks. More specifically, it refers to the collection of internet-connected devices that are able to communicate autonomously over the internet, without needing a person to initiate the communication.

You might be asking yourself, how is this different from the "internet" as most people commonly understand the term? Well, it really isn't that different -- it's just a way of talking about the internet with a specific focus on "things" instead of people.

What does IoT stand for and what does it mean?

Consultancy McKinsey & Company offered this basic description of IoT: "Sensors and [actuators](https://internetofthingsagenda.techtarget.com/definition/actuator) embedded in physical objects are linked through wired and wireless networks, often using the same Internet Protocol ([IP](https://www.techtarget.com/searchunifiedcommunications/definition/Internet-Protocol)) that connects the internet."

Kevin Ashton, who coined the term internet of things, preferred the term internet for things. While not widely used, this term provides a helpful way to understand the concept behind IoT. Think of the "normal" internet you access from your PC or smartphone as the internet for people and IoT as an internet of interrelated computing devices, mechanical and digital machines, objects, etc.

The internet of things is everywhere. [It is used in a range of industries](https://internetofthingsagenda.techtarget.com/tip/Top-8-IoT-applications-and-examples-in-business) and has both corporate and consumer uses. Today, for example, automobiles often have dozens of sensors that collect and transfer data for safety, maintenance, entertainment, fleet management and other purposes. These [internet-connected cars](https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/How-is-IoT-driving-the-future-of-connected-cars) are considered part of the internet of things, because they communicate with other devices over the internet based on input from the environment, not just from direct human manipulation.

The concept behind the internet of things -- that is, the idea of [internet-connected devices](https://internetofthingsagenda.techtarget.com/definition/IoT-device) -- existed decades before Ashton gave the concept its name, however. In the past, the industry commonly referred to this concept as the embedded internet or [pervasive computing](https://internetofthingsagenda.techtarget.com/definition/pervasive-computing-ubiquitous-computing), with Intel driving the former label until it became clear the term IoT was prevailing in the public's eye.

One notable example of IoT that preceded the term was a modified Coca-Cola vending machine that became the first internet connected appliance in 1982. The machine, which was located at Carnegie Mellon University, reported its inventory and whether the drinks it contained were cold.

In 1994, [IEEE](https://www.techtarget.com/whatis/definition/IEEE-Institute-of-Electrical-and-Electronics-Engineers) Spectrum magazine described the concept of "moving small packets of data to large sets of nodes," with the goal of integrating and automating everything from home appliances to entire factories. IoT in all but name.

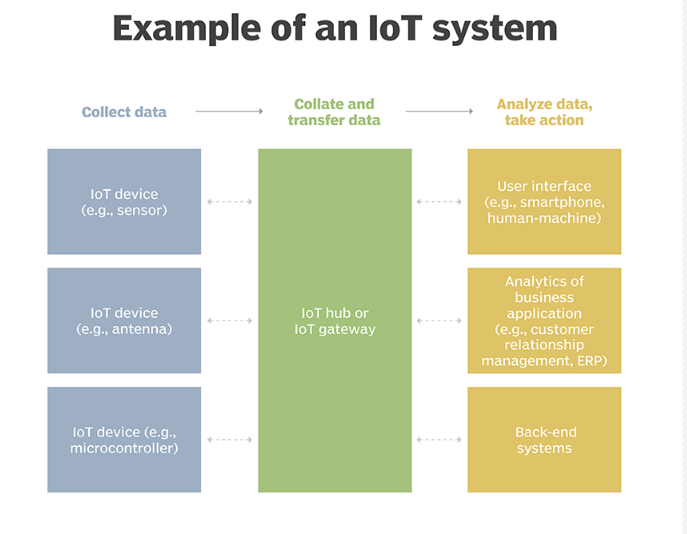
How does IoT work?

IoT works through a combination of [wireless networking technology](https://internetofthingsagenda.techtarget.com/feature/Determine-which-of-4-IoT-wireless-networks-fit-your-use-case), physical devices, advanced data analytics and cloud computing. The basic process of how IoT works is as follows:

* A group of physical devices is wired or wirelessly linked to each other and/or a central area.
* The devices collect data from the external world using some kind of sensor.
* That data is then stored somewhere, whether it be in the cloud, an intermediary network location, or on the device itself.
* The data is then processed, often by machine learning and artificial intelligence.
* The processed data is used by the physical device to perform some action.

For example, this process as applied to a [smart thermostat](https://internetofthingsagenda.techtarget.com/definition/Nest-Labs) would go like this:

* The thermostat has a sensor that reads the temperature in the room.
* The thermostat stores and processes that data.
* If the temperature exceeds a certain value, the thermostat automatically regulates the temperature to some predefined value.
* The thermostat transmits periodic temperature readings to the energy provider's external database over a wireless network.
* A data analytics application derives insights from the data over time to improve energy efficiency by adjusting the thermostat's temperature settings.



Basic IoT fundamentals, concepts and terms

The four pillars of IoT and the main concepts to understand are:

* Data. IoT technologies provide myriad ways to collect data about the physical world. Data is the fuel of IoT and is why it is so important.
* Device. The actual, physical components or things in the internet of things that collect this data.
* Analytics. The process of making collected data useful by turning raw data into actionable insights.
* Connectivity. Makes sharing data and insights possible, increasing the value of that data. This is the internet in internet of things.

The IoT can be defined in two ways based on

• existing Technology

• Infrastructure

Definition of IoT based on existing technology:

IoT is a new revolution to the internet due to the advancement in sensor networks, mobile devices, wireless communication, networking and cloud technologies.

Definition of IoT based on infrastructure:

IoT is a dynamic global network infrastructure of physical and virtual objects having unique identities, which are embedded with software, sensors, actuators, electronic and network connectivity to facilitate intelligent applications by collecting and exchanging data.

Goal of IoT:

The main goal of IoT is to configure, control and network the devices or things, to internet, which are traditionally not associated with the internet i.e thermostats, utility meters, a Bluetooth connected headset, irrigation pumps and sensors or control circuits for an electric car’s engine that make energy, logistics, industrial control, retail, agriculture and many other domain smarter.

Characteristics of IoT:

Various characteristics of IoT are:

• Dynamic and self-adapting

• Self-configuring

• Interoperable Communication protocols

• Unique identity

• Integrated into information network

Dynamic and self-adapting:

The IoT devices can dynamically adapt with sensed environment, their operating conditions, and user’s context and take actions accordingly. For ex: Surveillance System.

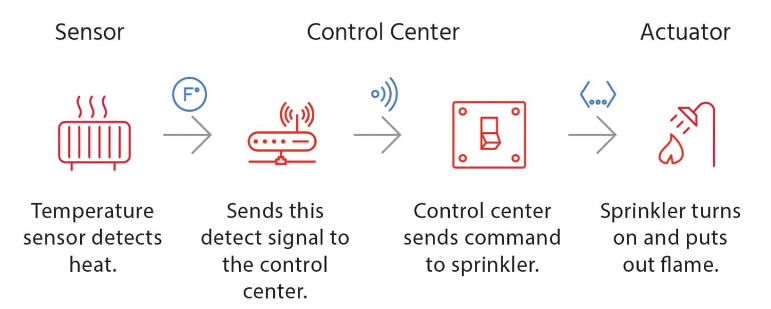
Self-configuring:

* 1. IoT devices can be able to upgrade the software with minimal intervention of user, whenever they are connected to the internet.
  2. II. They can also setup the network i.e a new device can be easily added to the existing network. For ex: Whenever there will be free wifi access one device can be connected easily.

Interoperable Communication: IoT allows different devices (different in architecture) to communicate with each other as well as with different network. For ex: MI Phone is able to control the smart AC and smart TV of different manufacturer. Unique identities: I. The devices which are connected to the internet have unique identities i.e IP address through which they can be identified throughout the network. II. The IoT devices have intelligent interfaces which allow communicating with users. It adapts to the environmental contexts. III. It also allows the user to query the devices, monitor their status, and control them remotely, in association with the control, configuration and management infrastructure. Integrated into information network: I. The IoT devices are connected to the network to share some information with other connected devices. The devices can be discovered dynamically in the network by other devices. For ex. If a device has wifi connectivity then that will be shown to other nearby devices having wifi connectivity. II. The devices ssid will be visible though out the network. Due to these things the network is also called as information network. III. The IoT devices become smarter due to the collective intelligence of the individual devices in collaboration with the information network. For Ex: weather monitoring system. Here the information collected from different monitoring nodes (sensors, arduino devices) can be aggregated and analysed to predict the weather.

The Internet of Things is a major contributing factor of the new Data Economy. The value of an IoT system goes beyond the original intended use case, for instance in automation. This is because further value lies in the intelligence that an IoT system creates. Sensors are the source of IoT data. Furthermore, sensors and actuators in IoT can work together to enable automation at industrial scale. Finally, analysis of the data that these sensors and actuators produce can provide valuable business insights over time.

Driven by new innovations in materials and nanotechnology, sensor technology is developing at a never before seen pace, with a result of increased accuracy, decreased size and cost, and the ability to measure or detect things that weren’t previously possible. In fact, sensing technology is developing so rapidly and becoming so advanced that we will see a trillion new sensors deployed annually within a few years.



## Sensors

A better term for a sensor is a transducer. A transducer is any physical device that converts one form of energy into another. So, in the case of a sensor, the transducer converts some physical phenomenon into an electrical impulse that determines the reading. A microphone is a sensor that takes vibrational energy (sound waves), and converts it to electrical energy in a useful way for other components in the system to correlate back to the original sound.

## Actuators

Another type of transducer that you will encounter in many [IoT systems](https://bridgera.com/iot-systems-overview/" \t "_blank) is an actuator. In simple terms, an actuator operates in the reverse direction of a sensor. It takes an electrical input and turns it into physical action. For instance, an electric motor, a hydraulic system, and a pneumatic system are all different types of actuators.

## Controller

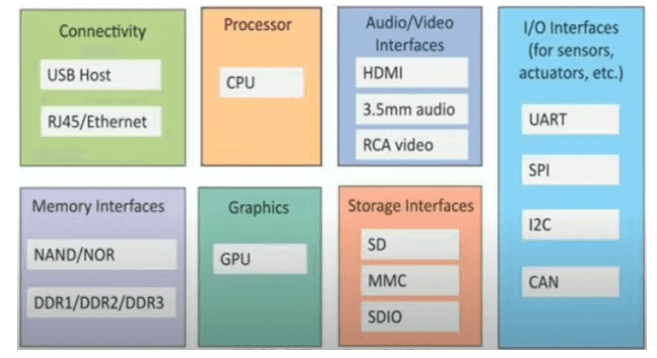
In a typical IoT system, a sensor may collect information and route to a control center. There, previously defined logic dictates the decision. As a result, a corresponding command controls an actuator in response to that sensed input. Thus, sensors and actuators in IoT work together from opposite ends. Later, we will discuss where the control center resides in the greater IoT system.

Physical Design of Internet of Things (IOT

The physical design of an IoT system is referred to as the Things/Devices and protocols that are used to build an IoT system. all these things/Devices are called Node Devices and every device has a unique identity that performs remote sensing, actuating and monitoring work. and the protocols that are used to establish communication between the Node devices and servers over the internet.

Things/Devices

Things/Devices are used to build a connection, process data, provide interfaces, provide storage, and provide graphics interfaces in an IoT system. all these generate data in a form that can be analyzed by an analytical system and program to perform operations and used to improve the system.

for example temperature sensor that is used to analyze the temperature generates the data from a location and is then determined by algorithms.

### Connectivity

Devices like USB hosts and ETHERNET are used for connectivity between the devices and the server.

### Processor

A processor like a CPU and other units are used to process the data. these data are further used to improve the decision quality of an IoT system.

### Audio/Video Interfaces

An interface like HDMI and RCA devices is used to record audio and videos in a system.

### Input/Output interface

To give input and output signals to sensors, and actuators we use things like UART, SPI, CAN, etc.

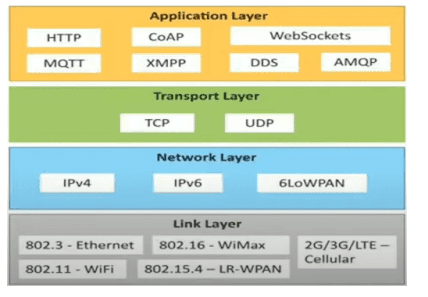
### Storage Interfaces

Things like SD, MMC, and SDIO are used to store the data generated from an IoT device.

Other things like DDR and GPU are used to control the activity of an IoT system.

## IoT Protocols

These protocols are used to establish communication between a node device and a server over the internet. it helps to send commands to an IoT device and receive data from an [IoT](https://www.programmingoneonone.com/2021/04/internet-of-things.html) device over the internet. we use different types of protocols that are present on both the server and client-side and these protocols are managed by network layers like application, transport, network, and link layer.



### Application Layer protocol

In this layer, protocols define how the data can be sent over the network with the lower layer protocols using the application interface. these protocols include HTTP, WebSocket, XMPP, MQTT, DDS, and AMQP protocols.

#### HTTP

Hypertext transfer protocol is a protocol that presents in an application layer for transmitting media documents. it is used to communicate between web browsers and servers. it makes a request to a server and then waits till it receives a response and in between the request server does not keep any data between two requests.

#### WebSocket

This protocol enables two-way communication between a client and a host that can be run on an untrusted code in a controlled environment. this protocol is commonly used by web browsers.

#### MQTT

It is a machine-to-machine connectivity protocol that was designed as a publish/subscribe messaging transport. and it is used for remote locations where a small code footprint is required.

### Transport Layer

This layer is used to control the flow of data segments and handle the error control. also, these layer protocols provide end-to-end message transfer capability independent of the underlying network.

#### TCP

The transmission control protocol is a protocol that defines how to establish and maintain a network that can exchange data in a proper manner using the internet protocol.

#### UDP

a user datagram protocol is a part of an internet protocol called the connectionless protocol. this protocol is not required to establish the connection to transfer data.

### Network Layer

This layer is used to send datagrams from the source network to the destination network. we use IPv4 and IPv6 protocols as host identification that transfers data in packets.

#### IPv4

This is a protocol address that is a unique and numerical label assigned to each device connected to the network. an IP address performs two main functions host and location addressing. IPv4 is an IP address that is 32-bit long.

#### IPv6

It is a successor of IPv4 that uses 128 bits for an IP address. it is developed by the IETF task force to deal with long-anticipated problems.

 Link Layer

Link-layer protocols are used to send data over the network's physical layer. it also determines how the packets are coded and signaled by the devices.

#### Ethernet

It is a set of technologies and protocols that are used primarily in LANs. it defines the physical layer and the medium access control for wired ethernet networks.

#### WiFi

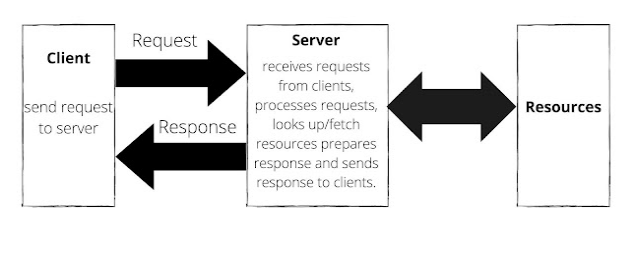
It is a set of LAN protocols and specifies the set of media access control and physical layer protocols for implementing wireless local area networks.

# IoT Communication Models

The fact is that IoT devices will be found everywhere and will enable circulatory intelligence in the future. So, the communication models used in IoT, have a great value. The follows people and things to be connected anytime, in any space, with anything and anyone. using any network and any service. From an operational, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models, before making decisions:

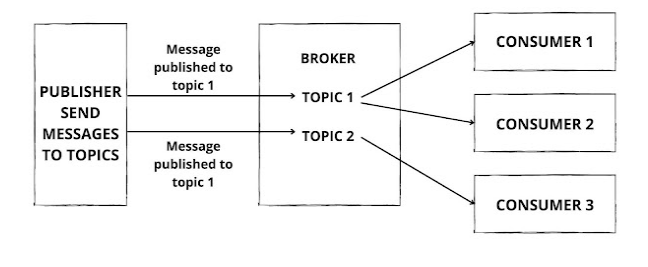
## Request-Response Model

The Request response model is stateless and each request is independently handled. The client is the IoT device that sends a request to the server. The request may be for the transfer of data or upload of data. The server may be remote or local and can handle requests of multiple clients. The server can receive the request, decide its response and fetch the data.



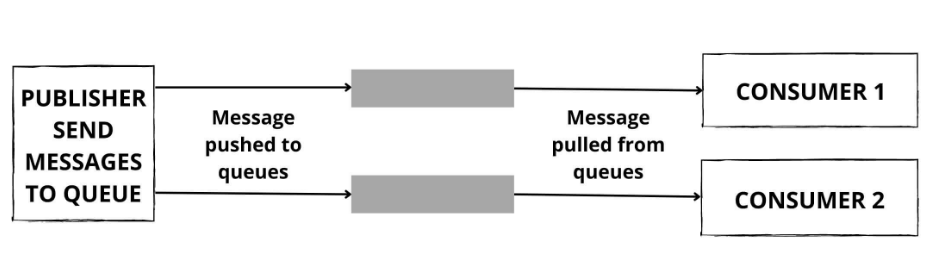
## Publish-Subscribe Model

There are three entities publisher, broker, and consumers. Publishers send the data to the brokers on topics managed by the brokers. Consumers subscribe to topics and brokers send the data on the topics to the consumers. Hence, brokers' responsibility is to accept data from publishers and send it to the appropriate consumer.



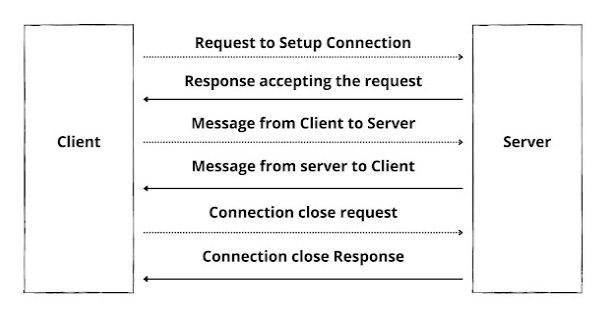
## Push-pull Model

This is a communication model. In this model data producers push data to queues and consumers pull data from queues Producers and consumers are not aware of each other. Queues act as buffers and are useful when there is a mismatch between the rate at which the producer push data and the rate at which the consumers pull data.



## Exclusive Pair Model

This model is a full-duplex communication model that uses a cond connection between client and server, The connection is constant and remains on till the client sends a request to close the connection. This is a stateful connection not and the server is aware of all open connections.



## IoT Communication APIs

Generally we used Two APIs For IoT Communication. These IoT Communication APIs are:

* REST-based Communication APIs
* WebSocket-based Communication APIs

REST-based Communication APIs

Representational state transfer (REST) is a set of architectural principles by which you can design Web services the Web APIs that focus on systems’s resources and how resource states are addressed and transferred. REST APIs that follow the request response communication model, the rest architectural constraint apply to the components, connector and data elements,  within a distributed hypermedia system.  The rest architectural constraint are as follows:

Client-server –  The principle behind the client-server constraint is the separation of concerns. for example clients should not be concerned with the storage of data which is concern of the serve. Similarly the server should not be concerned about the user interface, which is concern of the clien.  Separation allows client and server to be independently developed and updated.

**Stateless** – Each request from client to server must contain all the information necessary to understand the request, and cannot take advantage of any stored context on the server. The session state is kept entirely on the client.

**Cache-able** – Cache constraints requires that the data within a response to a request be implicitly or explicitly leveled as cache-able or non cache-able. If a response is cache-able, then a client cache is given the right to reuse that repsonse data for later, equivalent requests. caching can partially or completely eliminate some instructions and improve efficiency and scalability.

**Layered system** – layered system constraints, constrains the behavior of components such that each component cannot see beyond the immediate layer with they are interacting. For example, the client cannot tell whether it is connected directly to the end server or two an intermediaryalong the way. System scalability can be improved by allowing intermediaries to respond to requests instead of the end server, without  the client having to do anything different.

**Uniform interface**– uniform interface constraints requires that the method of communication between client and server must be uniform. Resources are identified in the requests (by URIsin web based systems) and are themselves is separate from the representations of the resources data returned to the client. When a client holds a representation of resources it has all the information required to update or delete the resource you (provided the client has required permissions). Each message includes enough information to describe how to process the message.

**Code on demand** – Servers can provide executable code or scripts for clients to execute in their context. this constraint is the only one that is optional.

A RESTful web service is a ” Web API ” implemented using HTTP and REST principles. REST is most popular IoT Communication APIs.

# Internet of Things (IoT) Enabling Technologies

1. Wireless Sensor Network
2. Cloud Computing
3. Big Data Analytics
4. Communications Protocols
5. Embedded System

1. Wireless Sensor Network(WSN) :  
A WSN comprises distributed devices with sensors which are used to monitor the environmental and physical conditions. A wireless sensor network consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects WSN to the internet.  
Example –

* Weather monitoring system
* Indoor air quality monitoring system
* Soil moisture monitoring system
* Surveillance system
* Health monitoring system

2. Cloud Computing :  
It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations.  
With Cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.  
Characteristics –

1. Broad network access
2. On demand self-services
3. Rapid scalability
4. Measured service
5. Pay-per-use

* IaaS (Infrastructure as a service)  
  Infrastructure as a service provides online services such as physical machines, virtual machines, servers, networking, storage and data center space on a pay per use basis. Major IaaS providers are Google Compute Engine, Amazon Web Services and Microsoft Azure etc.   
  Ex : Web Hosting, Virtual Machine etc.
* PaaS (Platform as a service)  
  Provides a cloud-based environment with a very thing required to support the complete life cycle of building and delivering West web based (cloud) applications – without the cost and complexity of buying and managing underlying hardware, software provisioning and hosting. Computing platforms such as hardware, operating systems and libraries etc. Basically, it provides a platform to develop applications.  
  Ex : App Cloud, Google app engine
* SaaS (Software as a service)  
  It is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management.  
  SaaS Applications are sometimes called web-based software on demand software or hosted  software.  
  SaaS applications run on a SaaS provider’s service and they manage security availability and performance.  
  Ex : Google Docs, Gmail, office etc.

3. Big Data Analytics :  
It refers to the method of studying massive volumes of data or big data. Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases.  
Big data is gathered from a variety of sources including social network videos, digital images, sensors and sales transaction records.  
Several steps involved in analyzing big data –

1. Data cleaning
2. Munging
3. Processing
4. Visualization

Examples –

* Bank transactions
* Data generated by IoT systems for location and tracking of vehicles
* E-commerce and in Big-Basket
* Health and fitness data generated by IoT system such as a fitness bands

4. Communications Protocols :  
They are the backbone of IoT systems and enable network connectivity and linking to applications. Communication protocols allow devices to exchange data over the network. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.  
They are used in

1. Data encoding
2. Addressing schemes

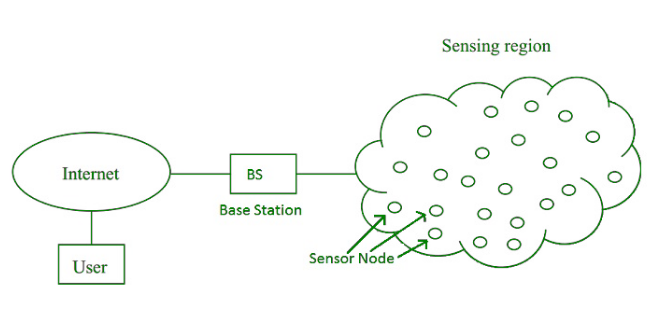
5. Embedded Systems :  
It is a combination of hardware and software used to perform special tasks.  
It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input output units (display keyword etc. ) and storage devices (flash memory).  
It collects the data and sends it to the internet.  
Embedded systems used in  
Examples –

1. Digital camera
2. DVD player, music player
3. Industrial robots
4. Wireless Routers etc.

**Wireless Sensor Network (WSN)**

**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

**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.

# IoT and Cloud Computing

One component that improves the success of the [Internet of Things](https://www.geeksforgeeks.org/introduction-to-internet-of-things-iot-set-1/) is [Cloud Computing](https://www.geeksforgeeks.org/cloud-computing/). Cloud computing enables users to perform computing tasks using services provided over the Internet. The use of the Internet of Things in conjunction with cloud technologies has become a kind of catalyst: the Internet of Things and cloud computing are now related to each other. These are true technologies of the future that will bring many benefits.

Due to the rapid growth of technology, the problem of storing, processing, and accessing large amounts of data has arisen. Great innovation relates to the mutual use of the Internet of Things and cloud technologies. In combination, it will be possible to use powerful processing of sensory data streams and new monitoring services. As an example, sensor data can be uploaded and saved using cloud computing for later use as intelligent monitoring and activation using other devices. The goal is to transform data into insights and thus drive cost-effective and productive action.

**Benefits And Functions of IoT Cloud:**  
There are many benefits of combining these services –

1. IoT Cloud Computing provides many connectivity options, implying large network access. People use a wide range of devices to gain access to cloud computing resources: mobile devices, tablets, laptops. This is convenient for users but creates the problem of the need for network access points.
2. Developers can use IoT cloud computing on-demand. In other words, it is a web service accessed without special permission or any help. The only requirement is Internet access.
3. Based on the request, users can scale the service according to their needs. Fast and flexible means you can expand storage space, edit software settings, and work with the number of users. Due to this characteristic, it is possible to provide deep computing power and storage.
4. Cloud Computing implies the pooling of resources. It influences increased collaboration and builds close connections between users.
5. As the number of IoT devices and automation in use grows, security concerns emerge. Cloud solutions provide companies with reliable authentication and encryption protocols.
6. Finally, IoT cloud computing is convenient because you get exactly as much from the service as you pay. This means that costs vary depending on use: the provider measures your usage statistics. A growing network of objects with IP addresses is needed to connect to the Internet and exchange data between the components of the network.

It is important to note that cloud architecture must be well-designed since reliability, security, economy, and performance optimization depends upon it. Using well-designed CI/CD pipelines, structured services, and sandboxed environments results in a secure environment and agile development.

**Comparison of Internet of Things and Cloud Computing:**  
Cloud is a centralized system helping to transfer and deliver data and files to data centers over the Internet. A variety of data and programs are easy to access from a centralized cloud system.  
The Internet of Things refers to devices connected to the Internet. In the IoT, data is stored in real-time, as well as historical data. The IoT can analyze and instruct devices to make effective decisions, as well as track how certain actions function.

Cloud computing encompasses the delivery of data to data centers over the Internet. IBM divides cloud computing into six different categories:

1. **Platform as a Service (PaaS) –**  
   The cloud contains everything you need to build and deliver cloud applications so there is no need to maintain and buy equipment, software, etc.
2. **Software as a Service (SaaS) –**  
   In this case, applications run in the cloud and other companies operate devices that connect to users’ computers through a web browser.
3. **Infrastructure as a Service (IaaS) –**   
   IaaS is an option providing companies with storage, servers, networks and hubs processing data for each use.
4. **Public cloud –**   
   Companies manage spaces and provide users with quick access through the public network.
5. **Private cloud –**   
   The same as a public cloud, but only one person has access here, which can be an organization, an individual company, or a user.
6. **Hybrid cloud –**   
   Based on a private cloud, but provides access to a public cloud.

Now, the Internet of Things refers to connecting devices to the Internet. Everyday devices such as cars and household appliances may have an Internet connection, and with the advancement of the Internet of Things, more and more devices will join this list.

**Pairing with edge computing:**  
Data processing at the network edge or edge computing is used with IoT solutions and enables faster processing and response times. To get a better understanding of how this works, consider a large factory with many implemented IoT sensors. In this situation, it makes sense, before sending data to the cloud for processing, to aggregate it close to the border to prevent cloud overload by reducing direct connections.

Data centers with this approach make data processing much faster. Yet, an approach that is only based on the edge will never provide a complete view of business operations. If there is no cloud solution, then the factory only controls each unit individually. Also, it has no way of imagining how these units work in relation to each other. This is why only the combination of the edge and the cloud will enable businesses to benefit from IoT developments.

**The Role of Cloud Computing on the Internet of Things:**  
Cloud computing works to improve the efficiency of daily tasks in conjunction with the Internet of Things. Cloud computing is about providing a path for data to reach its destination while the Internet of Things generates a huge amount of data.

According to Amazon Web Services, there are four benefits of cloud computing:

1. No need to pre-guess infrastructure capacity needs
2. Saves money, because you only need to pay for those resources that you use, the larger the scale, the more savings
3. In a few minutes, platforms can be deployed around the world
4. Flexibility and speed in providing resources to developers

Thus, the role of cloud computing in IoT is to work together to store IoT data, providing easy access when needed. It’s important to note that cloud computing is an easy way to move large data packets across the Internet generated by the IoT.

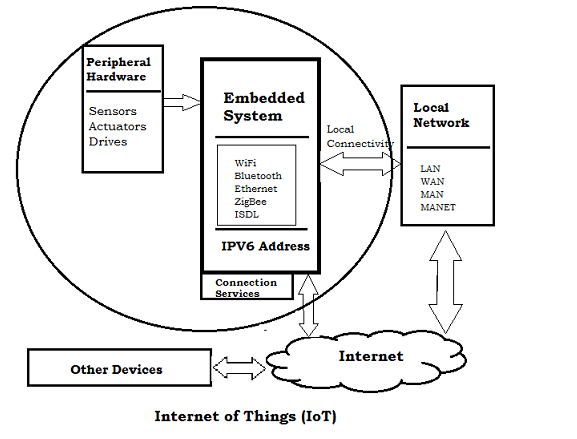
**Conclusion:**  
In conclusion, cloud computing in combination with the Internet of Things will make fundamental changes to the life of mankind, particularly in how information is managed. The cloud is the only technology that can analyze, store, and access the IoT depending on the deployment model. Because of the nature of on-demand information, cloud computing with an Internet connection is available on any device at any time. As hybrid cloud adoption grows, many companies are realizing its benefits and the need to implement it. Cloud computing will continue to open up new opportunities for the IoT for a long time to come.   
The three main components of the cloud listed below will revolutionize the Internet of Things:-

1. Computing power
2. Reliability
3. Connectivity

# Embedded Devices (System) in (IoT)

It is essential to know about the embedded devices while learning the IoT or building the projects on IoT. The embedded devices are the objects that build the unique computing system. These systems may or may not connect to the Internet.

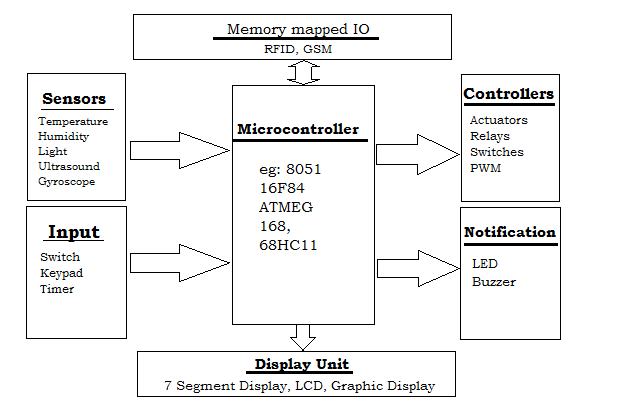
An embedded device system generally runs as a single application. However, these devices can connect through the internet connection, and able communicate through other network devices.



## Embedded System Hardware

The embedded system can be of type microcontroller or type microprocessor. Both of these types contain an integrated circuit (IC).

The essential component of the embedded system is a RISC family microcontroller like Motorola 68HC11, PIC 16F84, Atmel 8051 and many more. The most important factor that differentiates these microcontrollers with the microprocessor like 8085 is their internal read and writable memory. The essential embedded device components and system architecture are specified below.



## Embedded System Software

The embedded system that uses the devices for the operating system is based on the language platform, mainly where the real-time operation would be performed. Manufacturers build embedded software in electronics, e.g., cars, telephones, modems, appliances, etc. The embedded system software can be as simple as lighting controls running using an 8-bit microcontroller. It can also be complicated software for missiles, process control systems, airplanes etc.

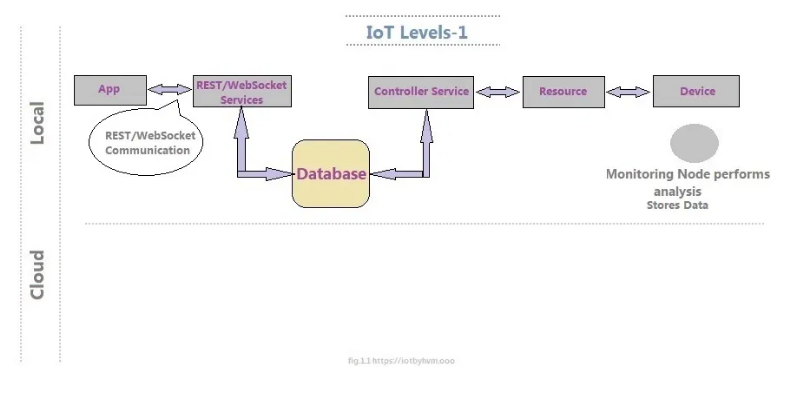
# IoT Levels and Deployment Templates

An IoT system comprises of the following components:

* **Device:** Allows identification, remote sensing, actuating and remote monitoring capabilities. IoT devices include wireless sensors, software, actuators, and computer devices. They are attached to a particular object that operates through the internet, enabling the transfer of data among objects or people automatically without human intervention. [Read more…](https://iotbyhvm.ooo/iot-device-what-is-an-iot-device/)
* **Resource:**These are Software components on the IoT device for accessing, processing, and storing sensor information, or controlling  
  actuators connected to the device.
* **Controller Service:** A native service that runs on the device and work between node device and web services. Controller service sends data from the device to the web service and receives commands from the application (via web services) for controlling the device.
* **Database:**A storage place for Collected or generated data. It can be local or cloud based.
* **Web Service:** Web services serve as a link between the IoT device, application, database and analysis components. Web service can be either implemented using HTTP and REST principles (REST service) or using WebSocket protocol (WebSocket service).
* **Analysis Component:** Responsible for analyzing the IoT data and generate results in a form which are easy for the user to understand.
* **Application:** IoT applications provide an interface that the users can use to control and monitor various aspects of the IoT system. It allow users to view the system Monitor and processed data.

IoT Level-1

• A level-1 IoT system has a single node/device that performs sensing and/or actuation, stores data, performs analysis and hosts the application • TIt is suitable for modeling low- cost and low-complexity solutions where the data involved is not big and the analysis requirements are not computationally intensive.

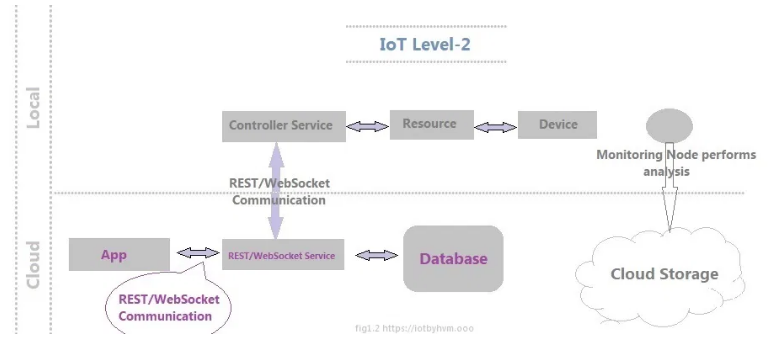


IoT Level-2

• It has a single node that performs sensing and/or actuation and local analysis (IoT Device and collected data).

• In this IoT Level Database and application establish in Cloud.

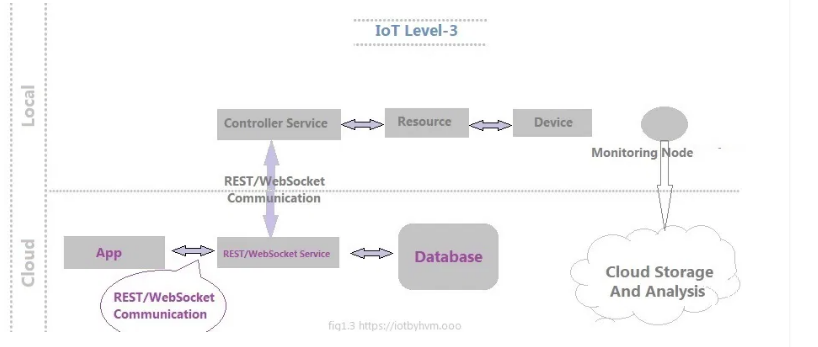
• It is useful for solutions where the data involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself.



IoT Level-3

• It has has a single node. Database and application establish in the cloud.

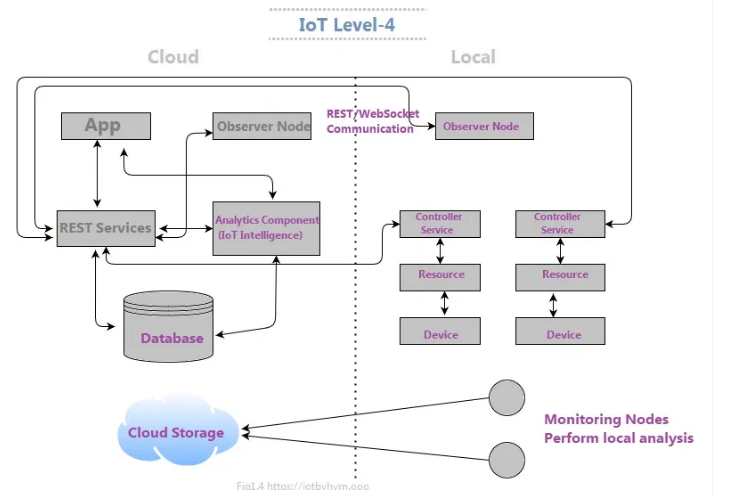
• It is suitable for solutions where the data involved is big and the analysis requirements are computationally intensive.



IoT Level-4

• It has multiple nodes that perform local analysis. It has Cloud based application and database. These IoT System contains local and cloud- based observer nodes which can subscribe to and receive information collected in the cloud from IoT node devices.

• It is suitable for solutions where we are using multiple nodes, the data involved is big and the analysis requirements are computationally intensive.

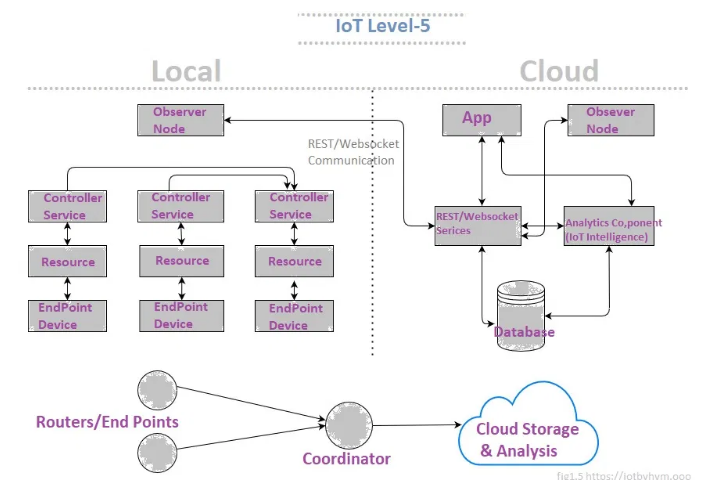


IoT Level-5

• It has multiple end nodes and one coordinator node. The end nodes use for sensing and/or actuation.

• In this model Coordinator node collects data from the end nodes and transfer to the cloud. In this model we used Cloud-based Database for store and Analyze data.

• It is suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive.

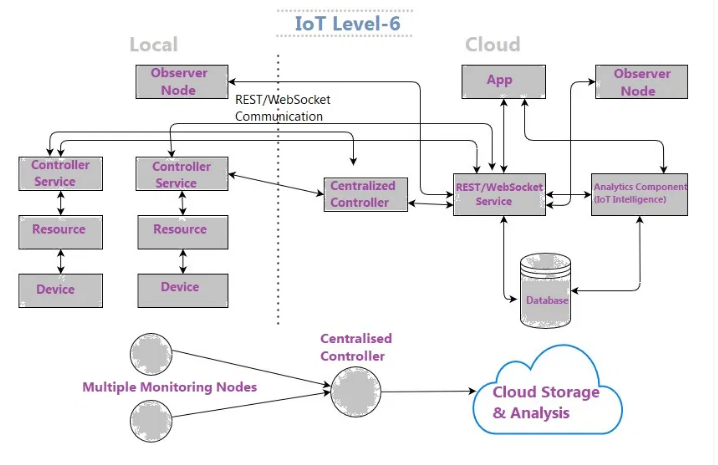


**IoT Level-6**

• It has multiple independent end nodes that used for sensing and/or actuation and transfer data to the cloud. We used Cloud-based database.

• The analytics component analyzes the data and stores the results in the cloud database and results are visualized with the cloud-based application.

• The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes



Domain Specific IoT Applications

In this article we are going to learn about domain specific iot applications like smart lighting, weather monitoring, etc.

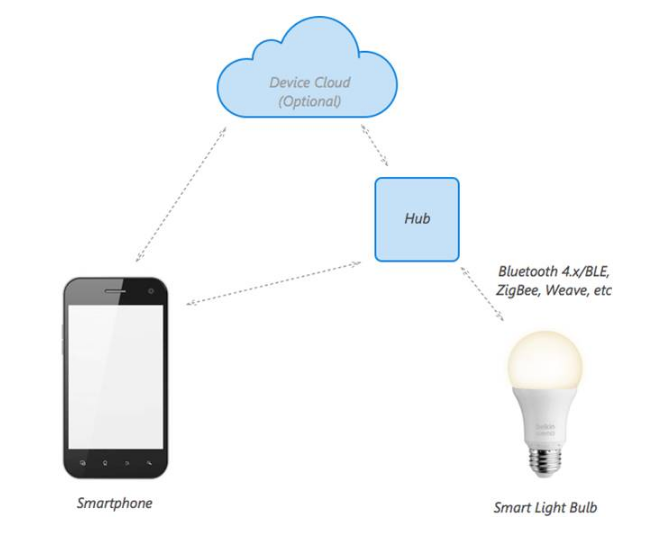
 IoT applications span a wide range of domains like:

* Home Automation
* Smart Cities
* Environment
* Energy systems
* Retail
* Logistics
* Industry
* Agriculture
* Health

**Home Automation**

Smart Lighting

Smart lighting for home helps in saving the energy by adapting the lighting to the ambient conditions. Energy can be saved by sensing human movements and their environment. Wireless and Internet connected lights can be operated remotely using mobile or web application.



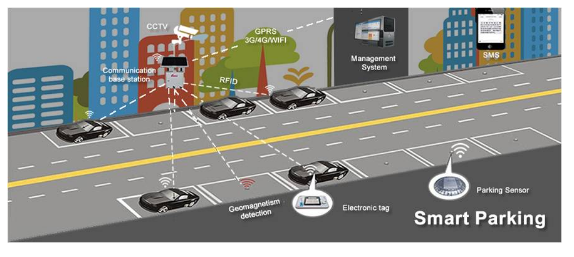
Smart Appliances

Smart appliances makes the management easier and also provide status information to the users remotely. For example, a smart refrigerator can keep track of items and notify the user when a item is low on stock. Examples of smart appliances are TVs, refrigerators, music systems, washing machines, etc.

Smart Cities

Smart Parking

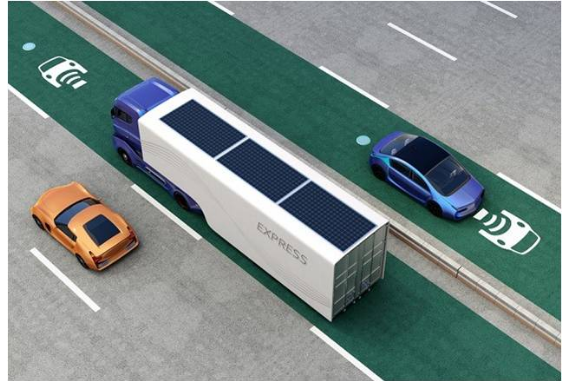
Smart parking makes the search for parking space easier and convenient for drivers. In smart parking, sensors are used for each parking slot, to detect whether the slot is occupied or not. This information is aggregated by local controllers and sent over the Internet to the database. Drivers can use an application to know about empty parking slots.



Smart Lighting

Smart lighting systems for roads, parks, and buildings can help in saving energy. Smart lighting allows lighting to be dynamically controlled and also adaptive to the ambient conditions. Smart lights connected to the Internet can be controlled remotely to configure lighting intensity and lighting schedule.

Smart Roads



Smart roads equipped with sensors can alert the users about poor driving conditions, traffic congestion, and accidents. Information sensed from the roads can be sent via Internet to applications or social media. This helps in reducing traffic jams.

Environment

Weather Monitoring



IoT-based weather monitoring systems use different sensors to gather data. That data is sent to the cloud-based storage. The collected can be analyzed and visualized with applications. Weather alerts can be subscribed by users from such applications.

Weather Monitoring

It collects data from a number of sensor attached such as temperature, humidity, pressure, etc and send the data to cloud-based applications and store back-ends.

The data collected in the cloud can then be analyzed and visualized by cloud-based applications.

Weather alert can be sent to the subscribed users from such applications.

AirPi is a weather and air quality monitoring kit capable of recording and uploading information about temperature, humidity, air pressure, light levels, UV levels, carbon monoxide, nitrogen dioxide and smoke level to the Internet.

Paper:

PeWeMoS Pervasive Weather Monitoring System [ICPCA, 2008] Presented a pervasive weather monitoring system that is integrated with buses to measure weather variables like humidity, temperature, and air quality during the bus path.

Air Pollution Monitoring

loT based air pollution monitoring system can monitor emission of harmful gases by factories and automobiles using gaseous and meteorological sensors.

The collected data can be analyzed to make informed decisions on pollutions control approaches.

Paper:

Wireless sensor network for real-time air pollution monitorings (ICCSPA, 2013] Presented a real time air quality monitoring system that comprises of several distributed monitoring stations that communicate via wireless with a back- end server using machine-to machine communication.

Noise Pollution Monitoring

Noise pollution monitoring can help in generating noise maps for cities.

It can help the policy maker in making policies to control noise levels near residential areas, school and parks.

It uses a number of noise monitoring stations that are deployed at different places in a city.

The data on noise levels from the stations is collected on servers or in the cloud and then the collected data is aggregate to generate noise maps.

Papers:

Noise mapping in urban environments: Applications at Suez city center [ICCIE, 2009]Presented a noise mapping study for a city which revealed that the city suffered from serious noise pollution.

SoundOfCity Continuous noise monitoring for a health city [PerComW,2013] Designed a smartphone application that allows the users to continuously measure noise levels and send to a central server here all generated information is aggregated and mapped to a meaningful noise visualization

Energy

loT applications for smart energy systems:

1. Smart Grid

2. Renewable Energy Systems

3. Prognostics

Smart Grids

Smart grid technology provides predictive information and recommendations to utilize, their suppliers, and their customers on how best to manage power.

Smart grid collect the data regarding :

Electricity generation

Storage

- Distribution and equipment health data

By analyzing the data on power generation, transmission and consumption of smart grids can improve efficiency throughout the electric system. Storage collection and analysis of smarts grids data in the cloud can help in dynamic optimization of system operations, maintenance, and planning.

Cloud-based monitoring of smart grids data can improve energy usage usage levels via energy feedback to users coupled with real-time pricing information.

• Condition monitoring data collected from power generation and transmission systems can help in detecting faults and predicting outages.

Renewable Energy System

Due to the variability in the output from renewable energy sources (such as solar and wind). integrating them into the grid can cause grid stability and reliability problems.

loT based systems integrated with the transformer at the point of interconnection measure the electrical variables and how much power is fed into the grid.

Sun

. To ensure the grid stability, one solution is to simply cut off the overproductions.

Paper:

Communication systems for grid integration of renewable energy resources (IEEE Network, 2011] → Provided the closed-loop controls for wind energy system that can be used to regulate the voltage at point of interconnection which coordinate wind turbine outputs and provides reactive power support.

Prognostics

loT based prognostic real-time health management systems can predict performance of machines of energy systems by analyzing the extent of deviation of a system from its normal operating profiles.

In the system such as power grids, real time information is collected using specialized electrical sensors called Phasor Measurement Units (PMU)

Agriculture

loT applications for smart agriculture:

1. Smart Irrigation

2. Green House Control

Smart Irrigation

Smart irrigation system can improve crop yields while saving water.

Smart irrigation systems use loT devices with soil moisture sensors to determined the amount of moisture on the soil and release the flow of the water through the irrigation pipes only when the moisture levels go below a predefined threshold.

It also collect moisture level measurements on the server on in the cloud where the collected data can be analyzed to plan watering schedules.

- Cultivar's Rain Could is a device for smart irrigation that uses water valves, soil sensors, and a WiFi enabled programmable computer. [http://ecultivar.com/rain-cloud-product-project/

Green House Control

It controls temperature, humidity, soil, moisture, light, and carbon dioxide level that are monitored by sensors and climatological conditions that are controlled automatically using actuation devices.

-loT systems play an importance role in green house control and help in improving productivity.

The data collected from various sensors is stored on centralized servers or in the cloud where analysis is performed to optimize the control strategies and also correlate the productivity with different control strategies.

Paper:

Wireless sensing and control for precision Green house management [ICST, 2012] Provided a system that uses wireless sensor network to monitor and control the agricultural parameters like temperature and humidity in the real time for better management and maintenance of agricultural production.

Industry

loT applications in smart industry:

1. Machine Diagnosis & Prognosis

2. Indoor Air Quality Monitoring

Machine Diagnosis & Prognosis

- Machine prognosis refers to predicting the performance of machine by analyzing the data on the current operating conditions and how much deviations exist from the normal operating condition.

Machine diagnosis refers to determining the cause of a machine fault.

Sensors in machine can monitor the operating conditions such as temperature and vibration levels, sensor data measurements are done on timescales of few milliseconds to few seconds which leads to generation of massive amount of data.

- Case-based reasoning (CBR) is a commonly used method that finds solutions to new problems based on past experience.

CBR is an effective technique for problem solving in the fields in which it is hard to establish a quantitative mathematical model, such as machine diagnosis and prognosis.

Indoor Air Quality Monitoring

Harmful and toxic gases such as carbon monoxide (CO), nitrogen monoxide (NO), Nitrogen Dioxide, etc can cause serious health problem of the workers.

-loT based gas monitoring systems can help in monitoring the indoor air quality using various gas sensors.

The indoor air quality can be placed for different locations

Wireless sensor networks based loT devices can identify the hazardous zones, so that corrective measures can be taken to ensure proper ventilation.

Papers:

A hybrid sensor system for indoor air quality monitoring (IEEE International Conference on Distributed Computing in Sensor System, 2013] presented a hybrid sensor system for indoor air quality monitoring which contains both stationary sensor and mobile sensors.

Indoor air quality monitoring using wireless sensor network [International Conference on Sensing Technology. 2012] → provided a wireless solution for indoor air quality monitoring that measures the environmental parameters like temperature, humidity, gaseous pollutants, aerosol and particulate matter to determine the indoor air quality.