# Unit III

## Data Acquiring

1. **Data Generation**

Data generates at devices that later on, transfer to the Internet through a gateway. Data generates as follows:

Passive devices data: Data generate at the device or system, following the result of interactions. A passive device does not have its own power source. An external source helps such a device to generate and send data. Examples are an RFID or an ATM debit card. The device may or may not have an associated microcontroller, memory and transceiver. A contactless card is an example of the former and a label or barcode is the example of the latter.

Active devices data: Data generates at the device or system or following the result of interactions. An active device has its own power source. Examples are active RFID, streetlight sensor or wireless sensor node. An active device also has an associated microcontroller, memory and transceiver.

Event data: A device can generate data on an event only once. For example, on detection of the traffic or on dark ambient conditions, which signals the event. The event on darkness communicates a need for lighting up a group of streetlights (Example 1.2). A system consisting of security cameras can generate data on an event of security breach or on detection of an intrusion. A waste container with associate circuit can generate data in the event of getting it filled up 90% or above. The components and devices in an automobile generate data of their performance and functioning. For example, on wearing out of a brake lining, a play in steering wheel and reduced airconditioning is felt. The data communicates to the Internet. The communication takes place as and when the automobile reaches near a Wi-Fi access point. Device real-time data: An ATM generates data and communicates it to the server instantaneously through the Internet. This initiates and enables Online Transactions Processing (OLTP) in real time.

Event-driven device data: A device data can generate on an event only once. Examples are: (i) a device receive command from Controller or Monitor, and then performs action(s) using an actuator. When the action completes, then the device sends an acknowledgement; (ii) when an application seeks the status of a device, then the device communicates the status.

## 2. Data acquisition

Data acquisition means acquiring data from IoT or M2M devices. The data communicates after the interactions with a data acquisition system (application). The application interacts and communicates with a number of devices for acquiring the needed data. The devices send data on demand or at programmed intervals. Data of devices communicate using the network, transport and security layers.

An application can configure the devices for the data when devices have configuration capability. For example, the system can configure devices to send data at defined periodic intervals. Each device configuration controls the frequency of data generation. For example, system can configure an umbrella device to acquire weather data from the Internet weather service, once each working day in a week. An ACVM can be configured to communicate the sales data of machine and other information, every hour. The ACVM system can be configured to communicate instantaneously in event of fault or in case requirement of a specific chocolate flavour needs the Fill service.

Application can configure sending of data after filtering or enriching at the gateway at the data-adaptation layer. The gateway in-between application and the devices can provision for one or more of the following functions—transcoding, data management and device management. Data management may be provisioning of the privacy and security, and data integration, compaction and fusion

Device-management software provisions for device ID or address, activation, configuring (managing device parameters and settings), registering, deregistering, attaching, and detaching

### 3. Data validation

Data acquired from the devices does not mean that data are correct, meaningful or consistent. Data consistency means within expected range data or as per pattern or data not corrupted during transmission. Therefore, data needs validation checks. Data validation software do the validation checks on the acquired data. Validation software applies logic, rules and semantic annotations. The applications or services depend on valid data. Then only the analytics, predictions, prescriptions, diagnosis and decisions can be acceptable.

Large magnitude of data is acquired from a large number of devices, especially, from machines in industrial plants or embedded components data from large number of automobiles or health devices in ICUs or wireless sensor networks, and so on. Validation software, therefore, consumes significant resources. An appropriate strategy needs to be adopted. For example, the adopted strategy may be filtering out the invalid data at the gateway or at device itself or controlling the frequency of acquiring or cyclically scheduling the set of devices in industrial systems. Data enriches, aggregates, fuses or compacts at the adaptation layer.

### 4. Data Categorization for Storage

Services, business processes and business intelligence use data. Valid, useful and relevant data can be categorized into three categories for storage—data alone, data as well as results of processing, only the results of data analytics are stored. Following are three cases for storage:

a. Data which needs to be repeatedly processed, referenced or audited in future, and therefore, data alone needs to be stored.

b. Data which needs processing only once, and the results are used at a later time using the analytics, and both the data and results of processing and analytics are stored. Advantages of this case are quick visualization and reports generation without reprocessing. Also the data is available for reference or auditing in future.

c. Online, real-time or streaming data need to be processed and the results of this processing and analysis need storage.

Data from large number of devices and sources categorizes into a fourth category called Big data. Data is stored in databases at a server or in a data warehouse or on a Cloud as Big data.

**5.** Assembly Software for the Events a device can generate events. For example, a sensor can generate an event when temperature reaches a preset value or falls below a threshold. A pressure sensor in a boiler generates an event when pressure exceeds a critical value which warrants attention. Each event can be assigned an ID. A logic value sets or resets for an event state. Logic 1 refers to an event generated but not yet acted upon. Logic 0 refers to an event generated and acted upon or not yet generated. A software component in applications can assemble the events (logic value, event ID and device ID) and can also add Date time stamp. Events from IoTs and logic-flows assemble using software.

## Data store

A data store is a data repository of a set of objects which integrate into the store. Features of data store are:

Objects in a data-store are modeled using Classes which are defined by the database schemas

A data store is a general concept. It includes data repositories such as database, relational database, flat file, spreadsheet, mail server, web server, directory services and VMware. A data store may be distributed over multiple nodes. Apache Cassandra is an example of distributed data store. A data store may consist of multiple schemas or may consist of data in only one scheme. Example of only one scheme data store is a relational database. Repository in English means a group, which can be related upon to look for required things, for special information or knowledge. For example, a repository of paintings of artists. A database is a repository of data which can be relied upon for reporting, analytics, process, knowledge discovery and intelligence. A flat file is another repository.

**Computing Using a Cloud Platform for IoT/M2M Applications/Services** \A few conventional methods for data collection and storage are as follows:
● Saving devices' data at a local server for the device nodes
● Communicating and saving the devices' data in the files locally on removable media, such as micro SD cards and computer hard disks

● Communicating and saving the data and results of computations in a dedicated data store or coordinating node locally

● Communicating and saving data at a local node, which is a part of a distributed DBMS
● Communicating and saving at a remote node in the distributed DBMS
● Communicating on the Internet and saving at a data store in a web or enterprise server
● Communicating on the Internet and saving at data center for an enterprise
Cloud is a new generation method for data collection, storage and computing. cloud computing paradigm for data collection, storage, computing and services. describes cloud-computing service models in a software architectural concept, 'everything as a service'.Describes IoT-specific cloud-based services, Xively, Nimbits. describes platforms such as AWS IoT, Cisco IoT, IOx and Fog, IBM IoT Foundation, TCS Connected Universe (TCS CUP).
Different methods of data collection, storage and computing are shown in Figure 6.1. The figure shows (i) Devices or sensor networks data collection at the device web

server, (ii) Local files, (iii) Dedicated data store at coordinating node, (iii) Local node in a distributed DBMS, (iv) Internet-connected data centre, (v) Internet-connected server, (vi) Internet-connected distributed DBMS nodes, and (vii) Cloud infrastructure and services.

Cloud computing paradigm is a great evolution in Information and Communications Technology (ICT). The new paradigm uses XAAS at the Internet connected clouds for collection, storage and computing. Following are the key terms and their meanings, which need to be understood before learning about the cloud computing platform. Resource refers to one that can be read (used), written (created of changed) or executed (processed). A path specification is also a resource. The resource is atomic (not-further divisible) information, which is usable during computations. A resource may have multiple instances or just a single instance. The data point, pointer, data, object, data store or method can also be a resource.

**Devices or sensors network data collection at a device local-server, local files, dedicated data store, at a coordinating node, a local node of a distributed DBMS, Internet-connected server of data centre, server or distributed database nodes or a cloud infrastructure**

System resource refers to an operating system (OS), memory, network, server, software or application. Environment refers to an environment for programming, program execution or both. For example, cloud9 online provides an open programming environment for BeagleBone board for the development of IoT devices; Windows environment for programming and execution of applications; Google App Engine environment for creation and execution of web applications in Python or Java. Platform denotes the basic hardware, operating system and network, and is used for software applications or services over which programs can be run or developed.

A platform may provide a browser and APIs which can be used as a base on which other applications can be run or developed. Edge computing is a type of computing that pushes the frontier of computing applications, data and services away from centralised nodes to IoT data generating nodes, that means at logical extremes of the network.2 IoT device nodes are pushed by events, triggers, alerts, messages and data is collected for enrichment, storage and computations from the remote centralised database nodes. Pushing the computations from centralized nodes enables the usage of resources at device nodes, which could be a requirement in case of low power lossy networks. The processing can also be classified as edge computing at local cloud, grid or mesh computing. The nodes may be mobile or of a wireless sensor network or cooperative distributed in peer-to-peer and ad-hoc networks. Distributed computing refers to computing and usage of resources which are distributed at multiple computing environments over the Internet. The resources are logically-related, which means communicating among themselves using message passing and transparency concepts, and are cooperating with each other, movable without affecting the computations and can be considered as one computing system (location independent).

Service is a software which provides the capabilities and logically grouped and encapsulated functionalities. A service is called by an application for utilising the capabilities. A service has a description and discovery methods, such as advertisement for direct use or through a service broker. The service binds to Service Level Agreement (SLA) between service (provider end point) and application (end point). One service can also use another service. Web Service, according to the W3C definition, is an application identified by a URI, described and discovered using the XML based Web-Service Description Language (WSDL). A web service interacts with other services and applications using XML messages and exchanges the objects using Internet protocols. Service-oriented architecture consists of components which are implemented as independent services which can be dynamically bonded and orchestrated, and which possess loosely coupled configurations, while the communication between them uses messages.

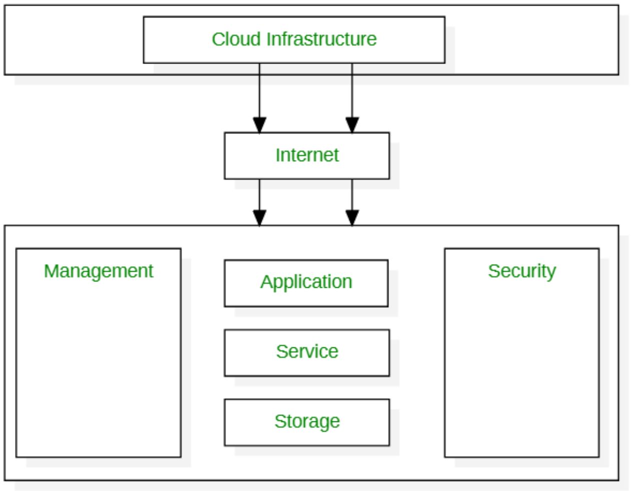
Orchestrating means a process which predefines an order of calling the services (in sequences and in parallel) and the data and message exchanges. Web computing refers to computing using resources at computing environment of web server(s) or web services over the Internet. Grid computing refers to computing using the pooled interconnected grid of computing resources and environments in place of web servers. Utility computing refers to computing using focus on service levels with optimum amount of resources allotted when required and takes the help of pooled resources and environments for hosting applications. The applications utilise the services. Cloud computing refers to computing using a collection of services available over the Internet that deliver computational functionality on the infrastructure of a service provider for connected systems and enables distributed grid and utility computing. Key Performance Indicator (**Cloud Computing Paradigm**

Cloud computing means a collection of services available over the Internet. Cloud delivers the computational functionality. Cloud computing deploys infrastructure of a cloud-service provider. The infrastructure deploys on a utility or grid computing or webservices environment that includes network, system, grid of computers or servers or data centres. Just as we—users of electricity—do not need to know about the source and underlying infrastructure for electricity supply service, similarly, a user of computing service or application need not know how the infrastructure deploys or the details of the computing environment. Just as the user does not need to know Intel processor inside a computer, similarly, the user uses the data, computing and intelligence in the cloud, as part of the services. Similarly, the services are used as a utility at the cloud.

**Cloud Computing :**

Cloud is defined as the usage of someone else’s server to host, process or store data. Cloud computing is defined as the type of computing where it is the delivery of on-demand computing services over the internet on a pay-as-you-go basis. It is widely distributed, network-based and used for storage.

There type of cloud are public, private, hybrid and community and some cloud providers are Google cloud, AWS, Microsoft Azure and IBM cloud.



**Sensor Technology**

The Internet of Things (IoT) couldn't exist without smart sensors, and the growing use of smart technology is already transforming how manufacturers implement the IoT. Smart sensors are also bringing more connectivity and analytics to the supply chain. There are some things to know about how and why this is happening.

First, smart sensors are indispensable enablers of the IoT and the industrial IoT. Smart sensors, including radio frequency identification (RFID) tags, serve three broad purposes. They identify items, locate them and determine their environmental conditions, all of which have major implications for the supply chain and manufacturing. Smart sensors are particularly useful in plants or warehouses because they can keep track of temperature and humidity, log data for historical records and quality management, or be used as triggers for alarms or process management.

Second, smart sensors impact the supply chain by being embedded in products, which can help improve the manufacturing process or the products themselves. "ensors can live inside products to create "smart products" and new revenue sources from the enhanced features. They can also permeate the manufacturing process to monitor, control, and improve operations, or be added to logistics to streamline how products are delivered. There are a number of specific purposes of sensors, such as measuring temperature, humidity, vibrations, motion, light, pressure and altitude. Companies will need to develop new applications to take advantage of all the big data that the sensors are generating.

A sensor is a device that detects and responds to some type of input from the physical environment. The specific input could be light, heat, motion, moisture, pressure, or any one of a great number of other environmental phenomena. The output is generally a signal that is converted to a human-readable display at the sensor location or transmitted electronically over a network for reading or further processing.

Here are a few examples of the many different types of sensors:

**In a mercury-based glass thermometer,** the input is temperature. The liquid contained expands and contracts in response, causing the level to be higher or lower on the marked gauge, which is human-readable.

**An oxygen sensor** in a car's emission control system detects the gasoline/oxygen ratio, usually through a chemical reaction that generates a voltage. A computer in the engine reads the voltage and, if the mixture is not optimal, readjusts the balance.

**Motion sensors** in various systems including home security lights, automatic doors and bathroom fixtures typically send out some type of energy, such as microwaves, ultrasonic waves or light beams and detect when the flow of energy is interrupted by something entering its path.

A photo sensor detects the presence of visible light, infrared transmission (IR), and/or ultraviolet (UV) energy.

Sensing is the process whereby individuals and communities use ever- more-capable mobile phones and cloud services to collect and analyze systematic data for use in discovery. The convergence of technology and analytical innovation with a citizenry that is increasingly comfortable using mobile phones and online social networking sets the stage for this technology to dramatically impact many aspects of our daily lives.

## 1. Applications and Usage Models

One application of participatory sensing is as a tool for health and wellness. For example, individuals can self-monitor to observe and adjust their medication, physical activity, nutrition, and interactions. Potential contexts include chronic-disease management and health behavior change. Communities and health professionals can also use participatory approaches to better understand the development and effective treatment of disease.

The same systems can be used as tools for sustainability. For example, individuals and communities can explore their transportation and consumption habits, and corporations can promote more sustainable practices among employees.

In addition, participatory sensing offers a powerful “make a case” technique to support advocacy and civic engagement. It can provide a framework in which citizens can bring to light a civic bottleneck, hazard, personal-safety concern, cultural asset, or other data relevant to urban and natural-resources planning and services, all using data that are systematic and can be validated.

These different applications imply several different usage models. These models range from public contribution, in which individuals collect data in response to inquiries defined by others, to personal use and reflection, in which individuals log information about themselves and use the results for personal analysis and behavior change. Yet across these varied applications and usage models, a common workflow is emerging, as Figure 4.1 illustrates.

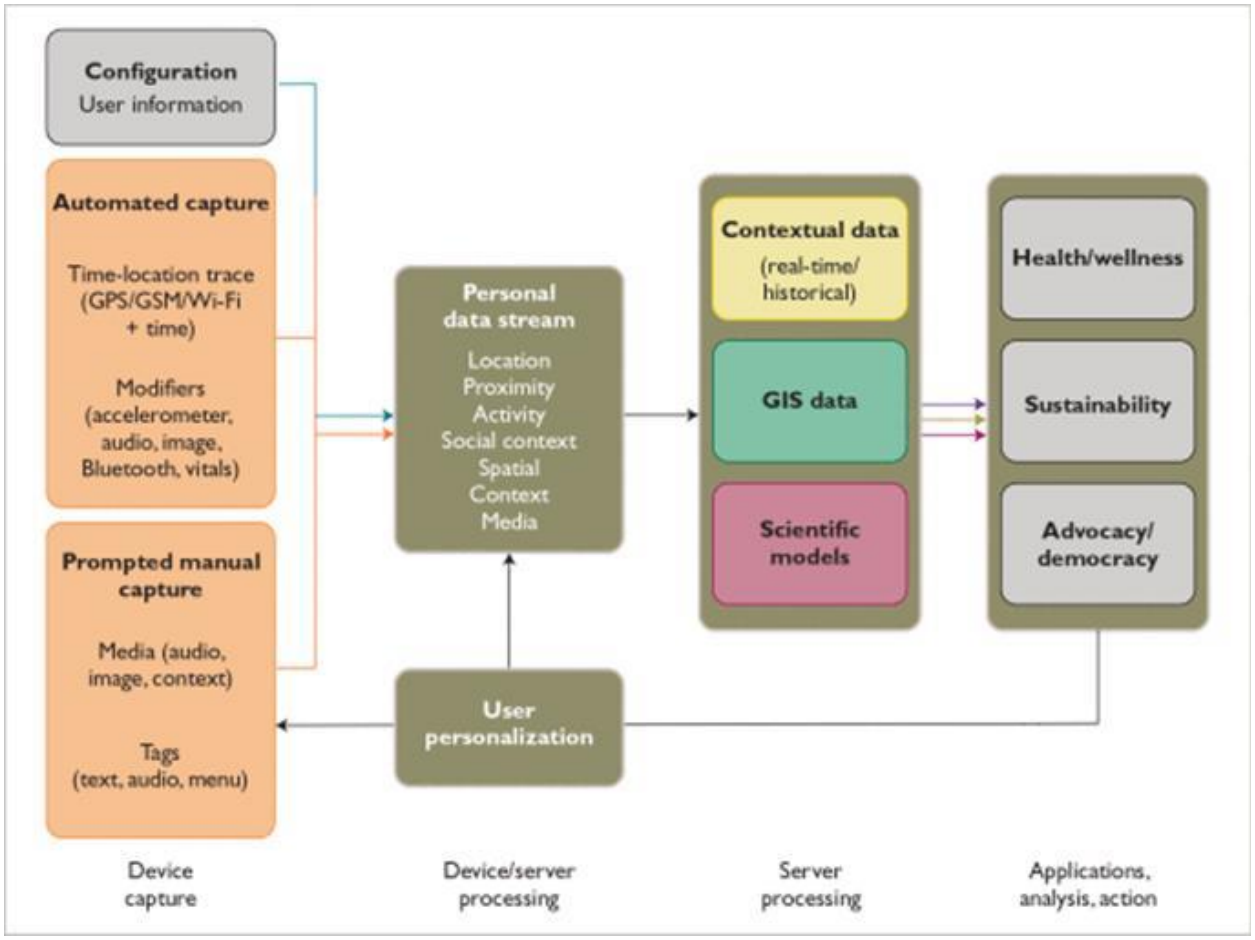


Fig Participatory Sensing Model Workflow

## 2. Essential Components

### Ubiquitous Data Capture

While empirical data can be collected in a variety of ways, mobile phones are a special and, perhaps, unprecedented tool for the job. These devices have become mobile computing, sensing, and communication platforms, complete with image, audio, video, motion, proximity, and location data capture and broadband communication, and they are capable of being programmed for manual, automatic, and con-text-aware data capture.

Because of the sheer ubiquity of mobile phones and associated communication infrastructure, it is possible to include people of all backgrounds nearly everywhere in the world. Because these devices travel with us, they can help us make sustainable observations on an intimately personal level. Collectively, they provide unmatched coverage in space and time.

### Leveraged Data Processing and Management

In some cases, the data collected with a mobile device are enough to reveal an interesting pattern on their own. However, when processed through a series of external and cross-user data sources, models, and algorithms, simple data can be used to infer complex phenomena about individuals and groups. Mapping and other interactive capabilities of today's Web enhance the presentation and interpretation of these patterns for participants. Many applications will call for the comparison of current measures to past trends, so robust and long term storage and management of this data is a central requirement.

### The Personal Data Vault

A common feature uniting these applications is the highly individualized, and therefore personal, nature of the data. By building mechanisms for protecting personal data directly into the emerging participatory sensing architecture’ we can create a healthy marketplace of content and services in which the individual has visibility and negotiating power with respect to the use and disposition of his or her personal data streams. By specifying standard mechanisms instead of standard policy, we enable support of diverse policies that are tailored to particular applications and users - this is the *narrow waist* of this participatory- sensing architecture. Without such architecture, critical applications will be encouraged to create bundled, vertically integrated, non-interoperable, and nontransferable vehicles for personal data streams, thereby making those streams opaque to their creators. By creating such a user-transparent architecture that places individuals and communities at the locus of control over information flow, we will simultaneously support participant rights and create a healthier market for competitive services.

To support this function, we propose the personal data vault. It decouples the capture and archiving of personal data streams from the sharing of that information. Instead of individuals sharing their personal data streams directly with services, we propose the use of secure containers to which only the individual has complete access. The personal data vault would then facilitate the selective sharing of subsets of this information with various services over time. Selective sharing may take the form of exporting filtered information from specific times of day or places in space, or may import service computations to the data vault and export resulting computational outputs. Essential to this scheme are tools to audit information flows and support meaningful usage. Finally, legal consideration is essential to protect and preserve the individual's control over his or her own data streams.

**Industrial IOT -** The IIoT is part of a larger concept known as the Internet of Things (IoT). The IoT is a network of intelligent computers, devices, and objects that collect and share huge amounts of data. The collected data is sent to a central Cloud-based service where it is aggregated with other data and then shared with end users in a helpful way. The IoT will increase automation in homes, schools, stores, and in many industries.

The application of the IoT to the manufacturing industry is called the IIoT (or Industrial Internet or Industry 4.0). The IIoT will revolutionize manufacturing by enabling the acquisition and accessibility of far greater amounts of data, at far greater speeds, and far more efficiently than before. A number of innovative companies have started to implement the IIoT by leveraging intelligent, connected devices in their factories.

**Benefits of IIOT**

The IIoT can greatly improve connectivity, efficiency, scalability, time savings, and cost savings for industrial organizations. Companies are already benefitting from the IIoT through cost savings due to predictive maintenance, improved safety, and other operational efficiencies. IIoT networks of intelligent devices allow industrial organizations to break open data silos and connect all of their people, data, and processes from the factory floor to the executive offices. Business leaders can use IIoT data to get a full and accurate view of how their enterprise is doing, which will help them make better decisions.

**Challenges of IIOT**

Interoperability and security are probably the two biggest challenges surrounding the implementation of IIoT. As technology writer Margaret Rouse observes, “A major concern surrounding the Industrial IoT is interoperability between devices and machines that use different protocols and have different architectures.” Ignition is an excellent solution for this since it is cross-platform and built on open-source, IT-standard technologies.

Companies need to know that their data is secure. The proliferation of sensors and other smart, connected devices has resulted in a parallel explosion in security vulnerabilities. This is another factor in the rise of MQTT since it is a very secure IIoT protocol.

**Future of IIOT**

The IIoT is widely considered to be one of the primary trends affecting industrial businesses today and in the future. Industries are pushing to modernize systems and equipment to meet new regulations, to keep up with increasing market speed and volatility, and to deal with disruptive technologies. Businesses that have embraced the IIoT have seen significant improvements to safety, efficiency, and profitability, and it is expected that this trend will continue as IIoT technologies are more widely adopted.

The Ignition IIoT solution greatly improves connectivity, efficiency, scalability, time savings, and cost savings for industrial organizations. It can unite the people and systems on the plant floor with those at the enterprise level. It can also allow enterprises to get the most value from their system without being constrained by technological and economic limitations. For these reasons and more, Ignition offers the ideal platform for bringing the power of the IIoT into your enterprise.

**Automotive IOT-**With the number of networked sensors increasing across production, supply chains and products, manufacturers are beginning to tap into a new generation of systems that enables real-time, automatic interactions among machines, systems, assets and things. The pervasiveness of connected devices is finding applicability across multiple segments of manufacturing and “upply chain throughout the value chain. Following are the functions provided by Automotive IOT:

- Ability to view the status of the Assets at anytime, Anywhere & Faster service response from dealer.
- By hooking equipment into the IoT, original equipment manufacturers (OEMs) or dealers could use that stream of data to adjust preventative maintenance schedules based on actual wear and be able to better optimize uptime
- Understand, monitor, predict and control process variability
- Enhance equipment and process diagnostics capabilities
- IoT helps more hands-off way to track goods and the progress of work. RFID tags and readers can play a role in this by allowing materials, locations, or tooling to essentially talk with each other.
- Faster Response time and less operations cost for machine configuration requests that could be services remotely
- Ability to view the entire population of connected products together marketing data and product trends

& increased trouble shooting ability for Manufacturer’s tech support

- Real-time remote monitoring of performance
- Multi site monitoring improving the operational efficiency and reducing the site downtime
- Availability of real time data for the production environment and alerts generated to the local administrators mobile phone reducing the clean room downtime
- Full manufacturing & SCM traceability
- Predictive Maintenance and quality

**Actuator-**An actuator is a component of a machine that is responsible for moving or controlling a mechanism or system, for example by actuating (opening or closing) a valve; in simple terms, it is a mover. An actuator requires a control signal and a source of energy. The control signal is relatively low energy and may be electric voltage or current, pneumatic or hydraulic pressure, or even human power. The supplied main energy source may be electric current, hydraulic fluid pressure, or pneumatic (gas pressure). When the control signal is received, the actuator responds by converting the energy into mechanical motion.

An actuator is the mechanism by which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), a human, or any other input.

In typical IoT systems, a sensor may collect information and route to a control center where a decision is made and a corresponding command is sent back to an actuator in response to that sensed input.

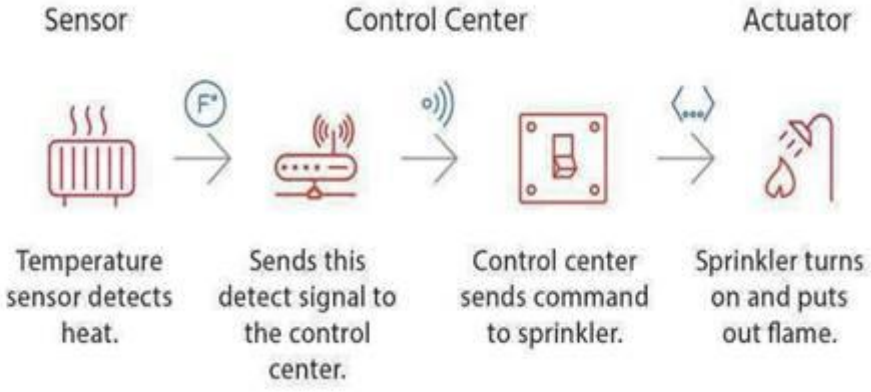

Sensor
Control Center
Actuator
F°
Temperature sensor detects heat.
Sends this detect signal to the control center.
Control center sends command to sprinkler.
Sprinkler turns on and puts out flame.

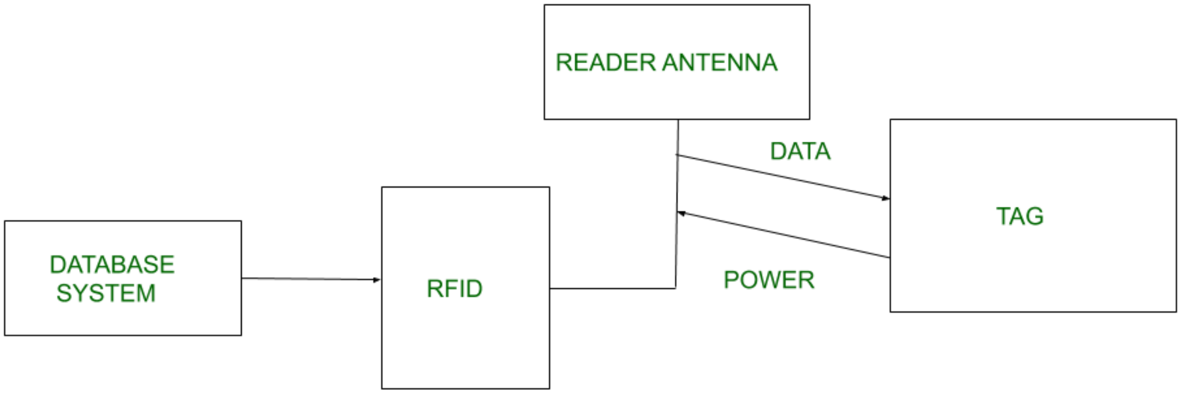
Fig  Sensor to Actuator Flow

There are many different types of sensors. Flow sensors, temperature sensors, voltage sensors, humidity sensors, and the list goes on. In addition, there are multiple ways to measure the same thing. For instance, airflow might be measured by using a small propeller like the one you would see on a weather station. Alternatively, as in a vehicle measuring the air through the engine, airflow is measured by heating a small element and measuring the rate at which the element is cooling.

**Radio Frequency Identification Technology-**Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture (AIDC).

RFID tags are used in many industries, for example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals can be tracked through warehouses; and implanting RFID microchips in livestock and pets allows for positive identification of animals.

**Radio Frequency Identification (RFID)** is a method that is used to track or identify an object by radio transmission uses over the web. Data digitally encoded in an RFID tag which might be read by the reader. This device work as a tag or label during which data read from tags that are stored in the database through the reader as compared to traditional barcodes and QR codes. It is often read outside the road of sight either passive or active RFID.



There are many kinds of RFID, each with different properties, but perhaps the most fascinating aspect of RFID technology is that most RFID tags have neither an electric plug nor a battery. Instead, all of the energy needed to operate them is supplied in the form of radio waves by RFID readers. This technology is called passive RFID to distinguish it from the(less common) active RFID in which there is a power source on the tag.

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

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

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

**There are two types of RFID :**

1. **Passive RFID –**

In this device, RF tags are not attached by a power supply and passive RF tag stored their power. When it is emitted from active antennas and the RF tag are used specific frequency like 125-134MHZ as low frequency, 13.56MHZ as a high frequency and 856MHZ to 960MHZ as ultra-high frequency.

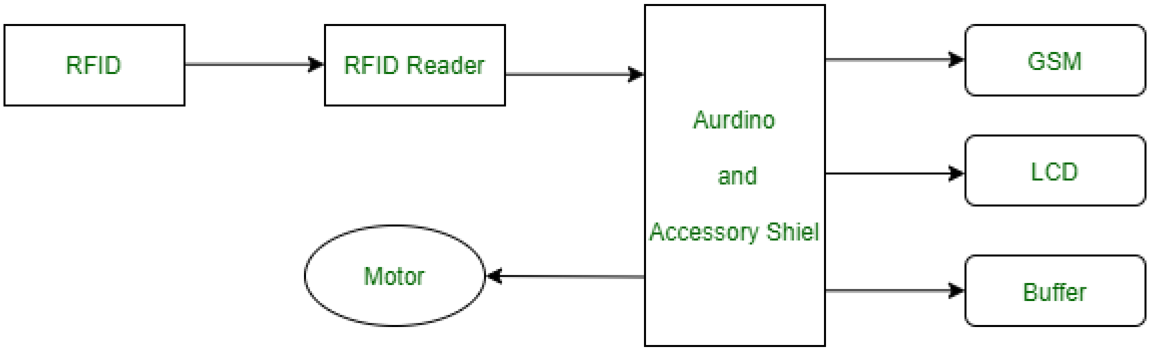
2. **Active RFID –**

   In this device, RF tags are attached by a power supply that emits a signal and there is an antenna which receives the data.

**Working Principle of RFID :**

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

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



**Features of RFID :**

- An RFID tag consists of two-part which is an microcircuit and an antenna.
- This tag is covered by protective material which acts as a shield against the outer environment effect.

- This tag may active or passive in which we mainly and widely used passive RFID.

**Application of RFID :**

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

**Advantages of RFID :**

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

**Disadvantages of RFID :**

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

**Wireless Sensor Network Technology-**Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on.

These are similar to wireless ad hoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. Sometimes they are called dust networks, referring to minute sensors as small as dust. WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

**A wireless sensor network (WSN)** is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes (see Figure 1). The wireless protocol you select depends on your application requirements. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.

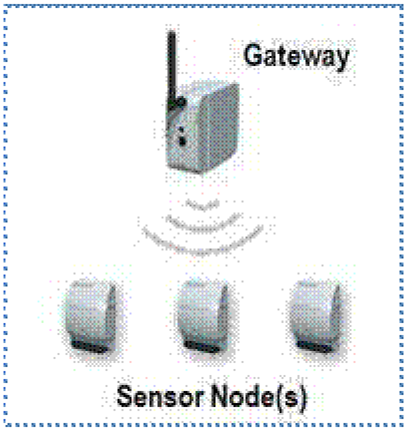


Fig WSN Components, Gateway, and Distributed Nodes

**Potential Applications-**Engineers have created WSN applications for areas including health care, utilities, and remote monitoring. In health care, wireless devices make less invasive patient monitoring and health care possible. For utilities such as the electricity grid, streetlights, and water municipals, wireless sensors offer a lower-cost method for collecting system health data to reduce energy usage and better manage resources. Remote monitoring covers a wide range of applications where wireless systems can complement wired systems by reducing wiring costs and allowing new types of measurement applications. Remote monitoring applications include:

- Environmental monitoring of air, water, and soil
- Structural monitoring for buildings and bridges
- Industrial machine monitoring
- Process monitoring
- Asset tracking

**WSN System Architecture**

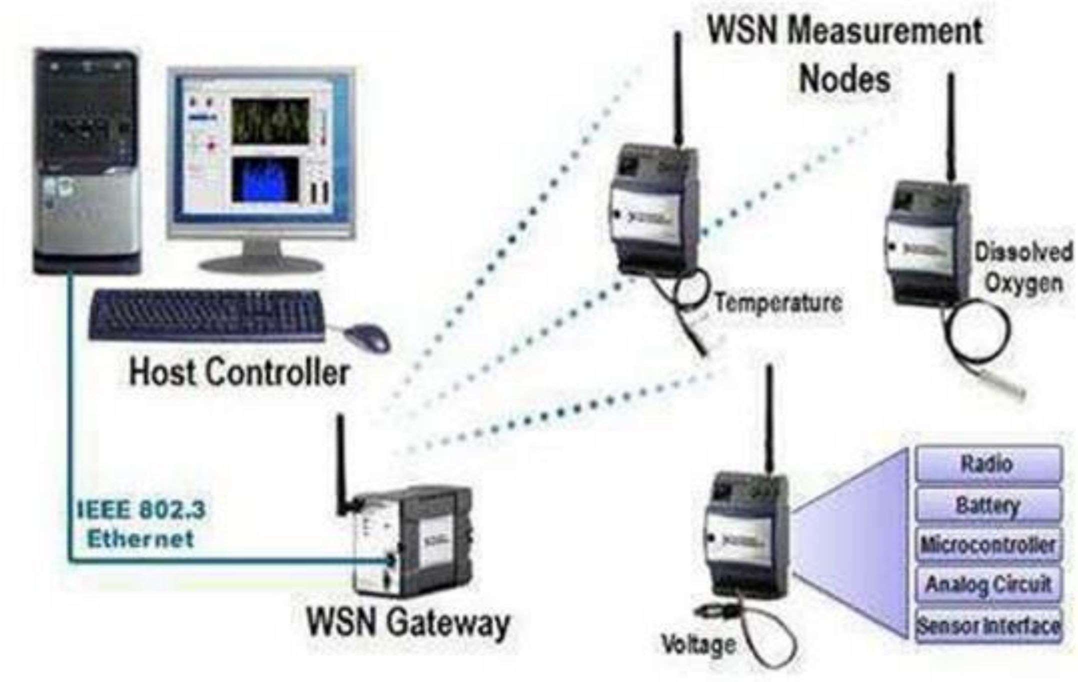


Fig. WSN System Architecture

Wireless technology offers several advantages for those who can build wired and wireless systems and take advantage of the best technology for the application. To do this, you need flexible software architecture like the NI Lab VIEW graphical system design platform. Lab VIEW offers the flexibility needed to connect a wide range of wired and wireless devices.

**WSN Network Topologies-**WSN nodes are typically organized in one of three types of network topologies. In a star topology, each node connects directly to a gateway. In a cluster tree network, each node connects to a node higher in the tree and then to the gateway, and data is routed from the lowest node on the tree to the gateway. Finally, to offer increased reliability, mesh networks feature nodes that can connect to multiple nodes in the system and pass data through the most reliable path available. This mesh link is often referred to as a router.

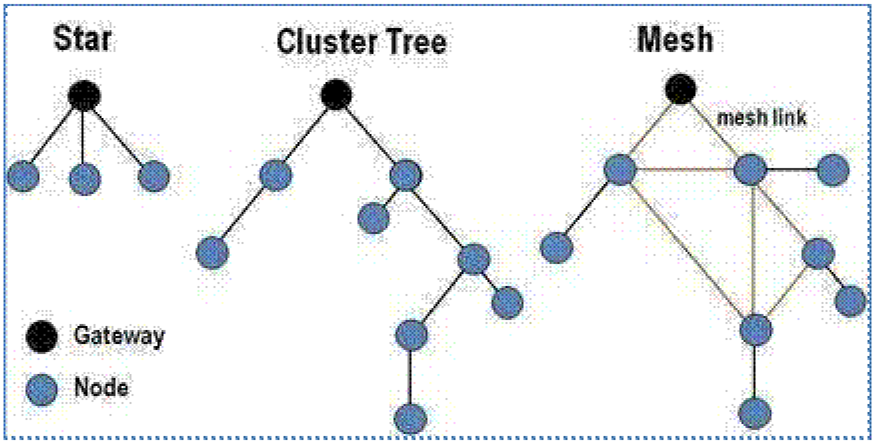


Fig. Common WSN Network Topologies

**Components of a WSN Node-**A WSN node contain several technical components. These include the radio, battery, microcontroller, analog circuit, and sensor interface. When using WSN radio technology, you must make important trade-offs. In battery-powered systems, higher radio data rates and more frequent radio use consume more power. Often three years of battery life is a requirement, so many of the WSN systems today are based on ZigBee due to its low-power consumption.

The second technology consideration for WSN systems is the battery. In addition to long life requirements, you must consider the size and weight of batteries as well as international standards for shipping batteries and battery availability. The low cost and wide availability of carbon zinc and alkaline batteries make them a common choice. To extend battery life, a WSN node periodically wakes up and transmits data by powering on the radio and then powering it back off to conserve energy. WSN radio technology must efficiently transmit a signal and allow the system to go back to sleep with minimal power use. This means the processor involved must also be able to wake power up, and return to sleep mode efficiently. Microprocessor trends for WSNs include reducing power consumption while maintaining or increasing processor speed. Much like your radio choice, the power consumption and processing speed trade-off is a key concern when selecting a processor for WSNs. This makes the x86 architecture a difficult option for battery-powered devices.

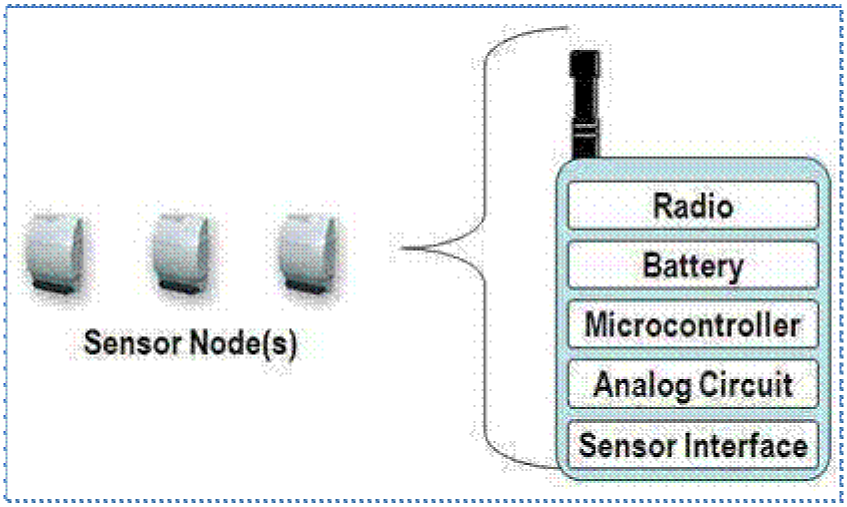


Fig WSN Sensor Node Components