Radio Frequency Identification Technology

Radio Frequency Identification Technology(RFID), also called electronic tag, wireless radio frequency identification, inductive electronic chip, and non-contact card, is a non-contact automatic identification technology, which can automatically identify the target object and obtain relevant data by a radio frequency signal. RFID technology can work in a variety of harsh environments without human intervention.

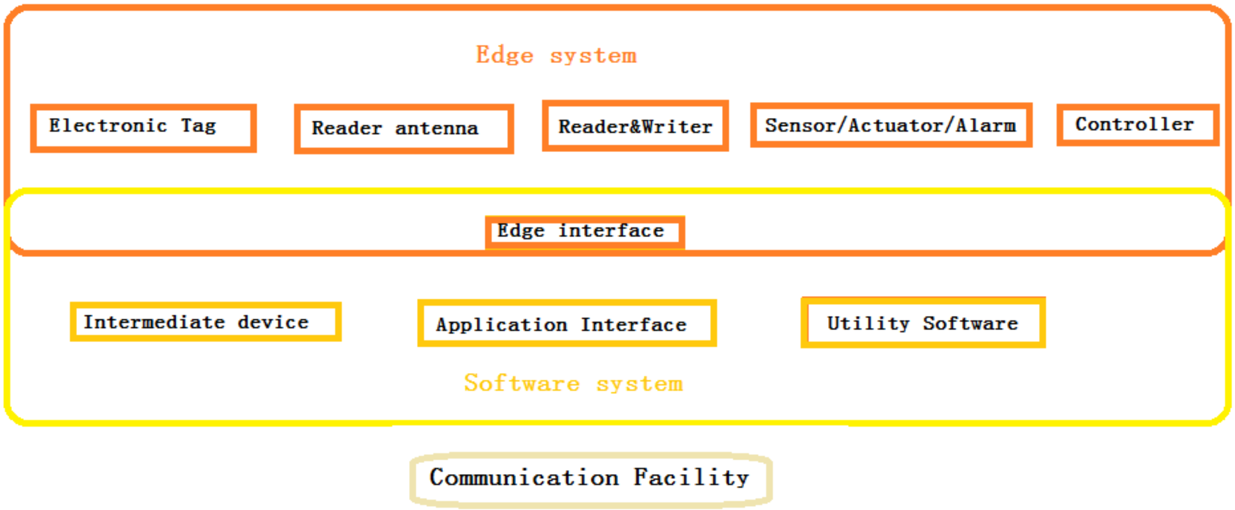
Moreover, it can identify high-speed moving objects and identify multiple tags at the same time, which is fast and convenient to operate. Short-range RF products are not afraid of oil stains, dust pollution and other harsh environments so that in such environments they can replace barcodes, such as tracking objects on factory assembly lines. Long-distance RF products are mostly used in traffic, which identification distance can reach tens of meters, such as automatic charging or vehicle identification

Classification

According to the availability of power, RFID is divided into Passive and Active.
1) Passive Tag: the Passive sensor itself does not have a power supply. Its power supply is generated by a sensor that is activated by emitting frequency from Reader, where the data is finally transmitted back to. The Passive Tag is thin and short and has a long service life but the sensing distance is relatively short.
2) Active Tag: the price is relatively high, volume is larger than the Passive tag because of the built-in battery. It has longer service life and longer sensing distance.

According to the frequency, RFID can be divided into three types: LF, HF, UF:
1) Low-Frequency RFID (100~500KHz): low-frequency RFID has a shorter inductive distance, the reading speed is slower. Low-frequency RFID of 125KHz is commonly used, whose penetration ability is good.
2) High-Frequency RFID(10~15MHz): high-frequency RFID has a longer sensing distance, the reading speed is relatively high. A High-frequency RFID of 13.56MHz is mainly used.
3) Ultra High-Frequency RFID (850~950MHz~2.45GHz)： Ultra High-Frequency RFID has the longest sensing distance and fastest reading speed, but penetration ability is bad.

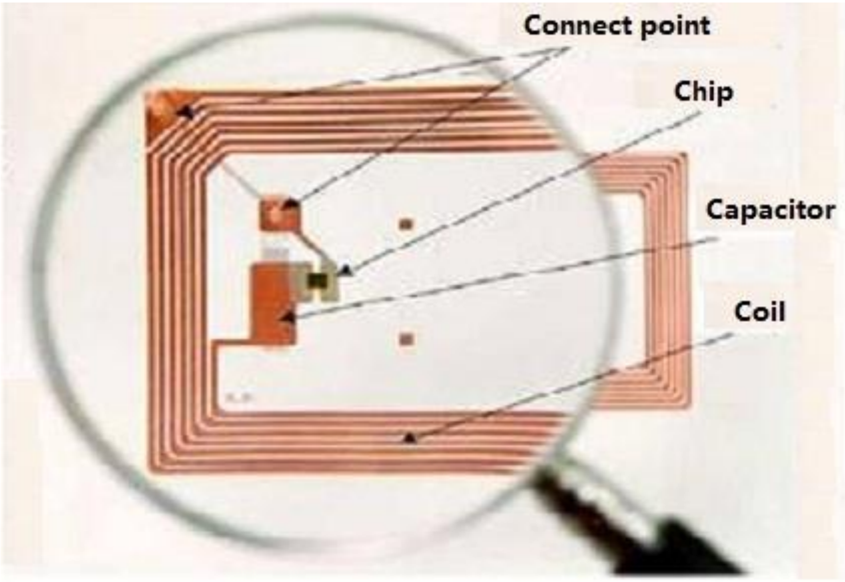
System Architecture :
According to the function, the RFID system can be divided into an Edge system and a Software system. Edge system mainly completes information perception and belongs to the hardware component. The software system completes information processing and application. The communication facility is responsible for the information transmission of the entire RFID system.



The basic composition of the RFID system

Electronic Tag

Electronic Tag is also known as the transponder or Smart Label, is a miniature wireless transceiver consisting mainly of built-in antennas and chips.



Reader&Writer

Reader & Writer is a device that captures and processes RFID tag data, either as an individual or embedded in other systems. Reader&Writer is also one of the important components of the RFID system, and its name comes from it can write data to RFID. The hardware of the reader is usually composed of the transceiver, microprocessor, memory, external sensor/actuator, alarm input/output interface, communication interface and power supply.

Controller

The controller is the command center for the orderly operation of the reader chip. Its main functions:

- Communicate with application system software;
- Execute the action instructions sent from the application system software;
- Control the communication process with the tag;
- Encoding and decoding of baseband signals;
- Implement anti-collision algorithm;
- Encrypting and decrypting data transmitted between the reader and the tag;
- Implement identity authentication between the reader and the electronic tag;
- Control of other external devices such as keyboards and display devices.
- Controls operation of the reader chip(the most important).

Reader Antenna

The antenna is a device that receives or radiates the front-end RF signal in the form of electromagnetic waves. It is an interface device between the circuit and space, which is used to realize the conversion of the guided wave and the free space wave energy. In the RFID system, the antenna is divided into an electronic tag antenna and reader antenna, which respectively bear the functions of receiving energy and transmitting energy. The features of the reader antenna are:

- Small enough to be attached to what is needed
- Directionality with omnidirectional or hemispherical coverage
- Capable of providing the chip with the largest possible signal
- Polarization of the antenna can match the interrogation signal of the card regardless of the direction
- Robust
- Cheap price

Communication Facilities

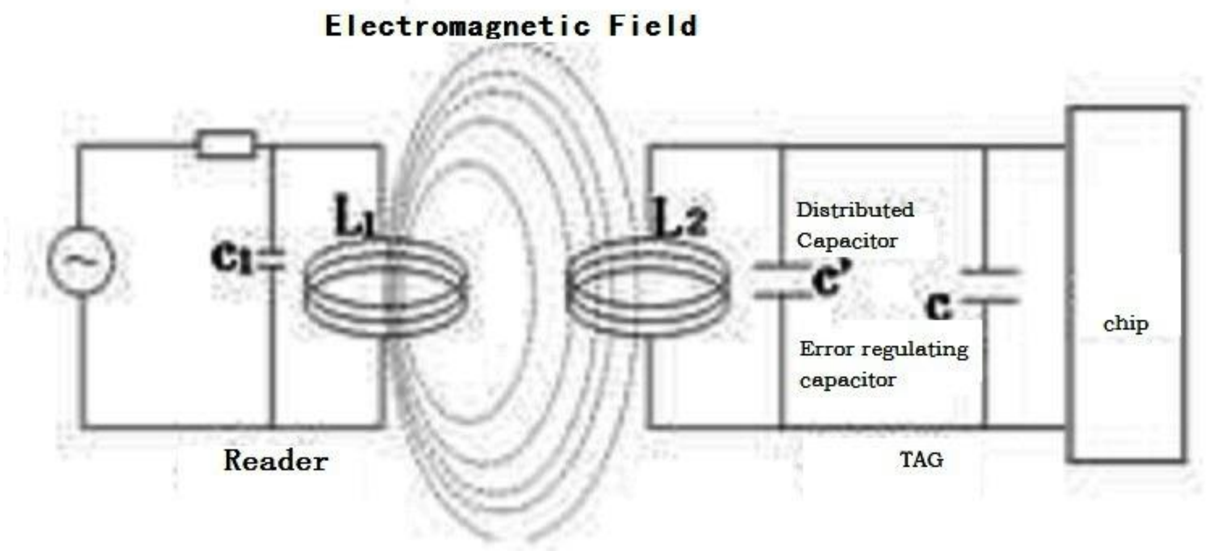
Communication facilities provide secure communication connections for different RFID system management and are an important part of RFID systems. Communication facilities include wired or wireless networks and serial communication interfaces for readers and controllers to be connected to a computer. The wireless network can be a personal area network (such as Bluetooth technology), a local area network (such as 802.11x, WiFi), or a wide area network (such as GPRS, 3G technology), and a satellite communication network (such as a synchronous orbit satellite L-band RFID system).

Antenna Type of RFID

RFID has three basic types: coil type, microstrip patch type and dipole type. Among them, the RFID antenna less than 1 meter used by the short distance application system generally adopts the coil type antenna, which has a simple process and low cost. It mainly works in the middle and low-frequency stages. The RFID antenna of more than 1 meter usually adopts microstrip patch type or dipole type, which is used in the application system. They work in the high frequency and microwave frequency stages. The principles of these antennas are different.

Coil Antenna

When the RFID coil antenna enters the alternating magnetic field generated by the reader, the interaction between the RFID antenna and the reader antenna is similar to that of the transformer, and the coils of both are equivalent to the primary and secondary coils of the transformer. The resonant loop formed by the coil antenna of the RFID is shown below



It includes the coil inductance L of RFID antenna, parasitic capacitance Cp and parallel capacitor C2, and its resonant frequency is:

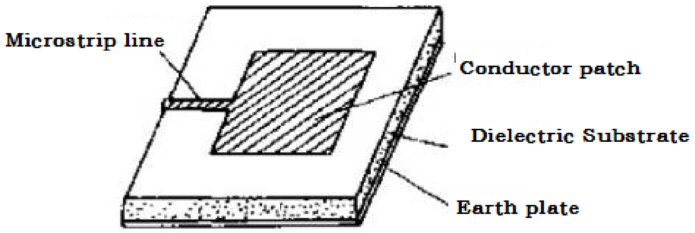
$$f = \frac{1}{2\pi\ \sqrt{L\ \cdot C}}$$

Capacitance C is the parallel equivalent capacitance of Cp and C2. The RFID application system realizes two-way data communication through this frequency carrier. The appearance of the ID1 non-contact IC card is a small plastic card (85.72mm × 54.03 mm × 0.76 mm), antenna coil resonance frequency is usually 13.56 MHz. A short-range RFID application system with a minimum area of 0.4mm × 0.4 mm coil antenna has been developed so far.

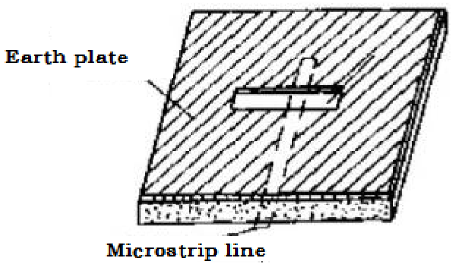
When the antenna coil area is small, the mutual inductance between RFID and reader is obviously not suitable for practical application. Generally, ferrite materials with high magnetic conductivity are inserted into the antenna coil of RFID to increase the mutual inductance and compensate for the decrease of the cross-section of the coil.

Microstrip antenna

A microstrip antenna is an antenna that is fed by a microstrip line or coaxial probe on a thin dielectric substrate. On one side, a thin metal layer is attached as a grounding plate, and on the other side, a metal patch with a certain shape is made by the photoetching etching method. Microstrip antennas can be divided into 2 types: ①microstrip patch antennas ② Microstrip slot antenna



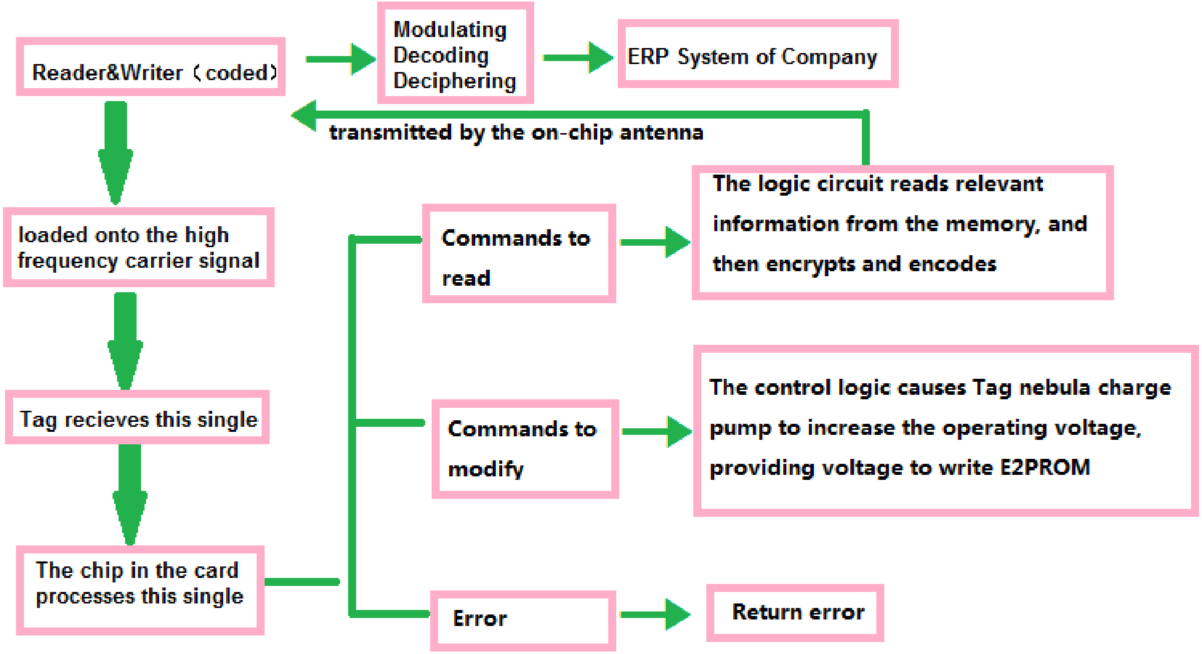
Microstrip patch antenna



Microstrip slot antenna

Operational Principal of RFID

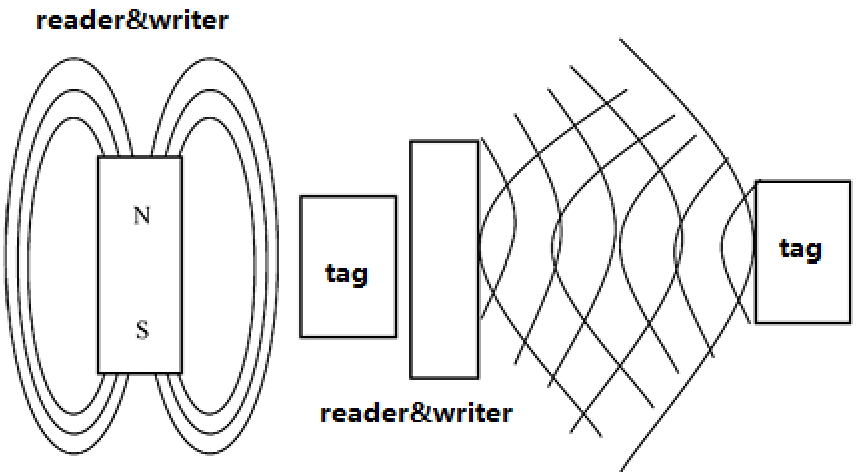
The basic principle of **RFID technology**: the RF signal to be transmitted by the reader&writer is coded and loaded onto the high-frequency carrier signal, and then sent out through the antenna. The electronic label entering the working area of the reader&writer receives the signal. The relevant circuits of the chip in the card perform voltage doubling rectifying, modulating, decoding, deciphering, and then judging the command request, password, authority, etc. Finally, the signal is processed by tag according to the command.


Reader&Writer（coded）
Modulating
Decoding
Deciphering
ERP System of Company
transmitted by the on-chip antenna
loaded onto the high frequency carrier signal
Tag recieves this single
The chip in the card processes this single
Commands to read
The logic circuit reads relevant information from the memory, and then encrypts and encodes
Commands to modify
The control logic causes Tag nebula charge pump to increase the operating voltage, providing voltage to write E2PROM
Error
Return error

Schematic of RFID Basic Working Principle

Fundamental

From the point of view of communication and energy-sensing between electronic tags and readers, systems can generally be divided into two types, namely, the Inductive Coupling system and the Electromagnetic Backscatter Coupling system. Inductive coupling is achieved by the spatial high-frequency alternating magnetic field, which is based on the law of electromagnetic induction; Electromagnetic back-scattering coupling, that is, the radar principle model: the emitted electromagnetic wave hits the target and then reflects, and carries back the target information, which is based on the law of the electromagnetic wave propagation in space.

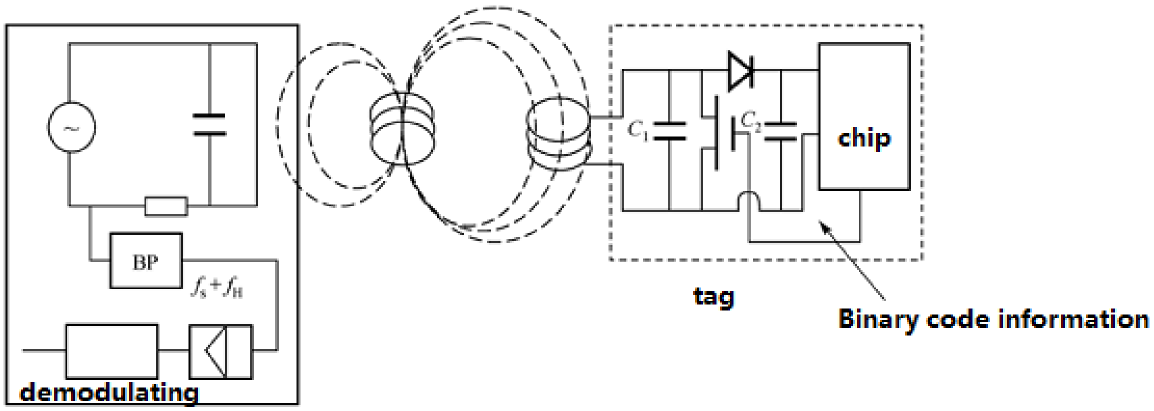


(a) Proximity inductance coupling (b) Remote inductance coupling

Inductive Coupling of RFID

The inductive coupling of RFID corresponds to the ISO/IEC 14443 protocol. The inductively coupled electronic tag consists of an electronic data carrier, which usually consists of a single microchip and an antenna made by a large area coil.

Almost all the tags in inductively coupled-mode work passively, and all the energy needed to work on the microchip in the tag is provided by the inductive electromagnetic energy transmitted by the reader. The high frequency strong electromagnetic field is generated by the antenna coil of the reader, which traverses the cross-section and surrounding space of the coil to make the nearby electronic tag produce electromagnetic induction.



Back-scatter Coupling RFID System

① Back-scattering modulation
Radar technology provides a theoretical and practical basis for the back-scattering coupling of RFID. When the electromagnetic wave meets a space target, one part of the energy is absorbed by the target and the other part is scattered in various directions with different intensities. In the scattering energy, a small part（echo） reflected back to the transmitting antenna and receives by the antenna (so the transmitting antenna is also the receiving antenna). The received signal can be amplified and processed, and the relevant information of the target can be obtained. In radar technology, this reflected wave can be used to measure the distance and orientation of the target.

For the RFID system, the electromagnetic back-scattering coupling can be used to transmit the data from the electronic tag to the reader by using the electromagnetic wave reflection. This operating mode is mainly used in systems of 915 MHz， 2.45 GHz or higher frequency.

②RFID backscattering coupling mode
The frequency of a target's reflected electromagnetic wave is determined by its cross-section. The cross-section is related to a series of parameters, such as the size, shape and material of the target, the wavelength and polarization direction of the electromagnetic wave, etc. Because the reflection performance of the target is usually enhanced with the increase of the frequency, UHF and UHF are used in the RFID backscattering coupling mode, and the distance between the transponder and the reader is more than 1 meter. Readers, electronic tags and antennas constitute a transceiver communication system.

4.4 Characteristic of RFID Technology

① Advantages:

- Fast scan: RFID recognizers can read and write multiple RFID tags at the same time, and the reading speed is very fast. The sketch capability of an active RFID system can be used for interactive services such as process tracking and maintenance tracking.
- Miniaturization and variety of shapes: RFID labels develop into miniaturization and variety for different products. The reading of the information is not limited by the size and shape of the chip, and it is not necessary to match the fixed size or printing quality of the paper to read accurately. Moreover, the RFID tags are being miniaturized and diversified to be used in different products.
- The RFID label is to store the data in the chip: The RFID chip and the RFID card reader have a strong resistance to water, oil and chemicals, which is not only free from contamination but also easy to preserve.
- Reusable: RFID tags repeatedly add, modify, delete the data stored in the RFID volume label, facilitate the update of information.
- Penetration and unbarrier reading: **RFID technology** is more accurate than traditional smart chips, and the distance of recognition is more flexible. It can achieve penetration and non-barrier reading. RFID can penetrate materials such as paper, wood and plastics for penetrating communication. It also can read labels through snow, fog, ice, paint, dirt and other harsh environments like bar code can not be used.

- Large memory capacity: The maximum capacity of RFID is several megabytes, which can be recorded in large quantities. And as technology advances, capacity has increased.
- Safety: Since RFID carries electronic information, its data content can be protected by passwords, making its content difficult to be forged and altered.

② Shortcomings:

- Technological maturity is not enough: RFID technology is new and is not very mature in technology. Due to the reverse reflective nature of UHF RFID tags, it is difficult to apply in metal, liquid and other commodities.
- High cost: RFID electronic tags are relatively expensive compared to ordinary bar code labels, which are costing dozens of times than ordinary bar code labels. If the usage is large, the cost will be too high, which greatly reduces the enthusiasm of the market for using RFID technology.
- Technical standards are not uniform: RFID technology has not yet formed a unified standard. Multiple standards coexist in the market resulting in the incompatibility of different enterprise products. The main manufacturers of RFID systems provide dedicated systems, which lead to different applications and industries adopting frequency and protocol standards of different manufacturers. Incompatible standards have caused confusion in the application of RFID technology, restricting the entire growth of RFID.

Electronic Product Code Information Services (EPCIS)

Electronic Product Code Information Services (EPCIS) is a global GS1 Standard for creating and sharing visibility event data, both within and across enterprises, to enable users to gain a shared view of physical or digital objects within a relevant business context. "Objects" in the context of EPCIS typically refers to physical objects that are handled in physical steps of an overall business process involving one or more organizations. Examples of such physical objects include trade items (products), logistic units, returnable assets, fixed assets, physical documents, etc. “Objects” may also refer to digital objects which participate in comparable business process steps. Examples of such digital objects include digital trade items (music downloads, electronic books, etc.), digital documents (electronic coupons, etc.), and so forth.

An EPCIS system is consist of two major top level standards, Capture and Share to record every events generated by all parties involved and share them with the required parties.

The Capture Standard

The capture standard consist of various interfaces allowing the other connected applications to send events into the EPCIS system along with the System Components required to perform certain operations on the shared data.

Interfaces

There are three major interfaces into the EPCIS system which are

1. EPICS Capture Interface
2. Application specific Interface
3. IoT Interfaces

EPCIS Capture Interface acts as a bridge between EPCIS Capture and Share standards. The Application specific Interfaces are the interfaces shared among other third party application using the EPCIS for sending events to capture. The IoT Interfaces are similar to Application specific Interfaces designed specifically for IoT devices involved into the process. These IoT devices can be RFID Tag, RFID Reader, Bar Code Reader etc.

System Components

There two major system components consist in capture standard which are

1. Filtering and Collection Engine
2. Data Capture Workflow

The filtering and collection engine is to filter and collect the required events emitted by the IoT devices or sent from various application interfaces. Whereas the data capture workflow is the process created to capture the events.

The Share Standard

The Share standard also consist of various interfaces and system components as follows:

Interfaces

The available interfaces in share standards are

1. EPCIS Query Interface
2. Interface exposed to other parties

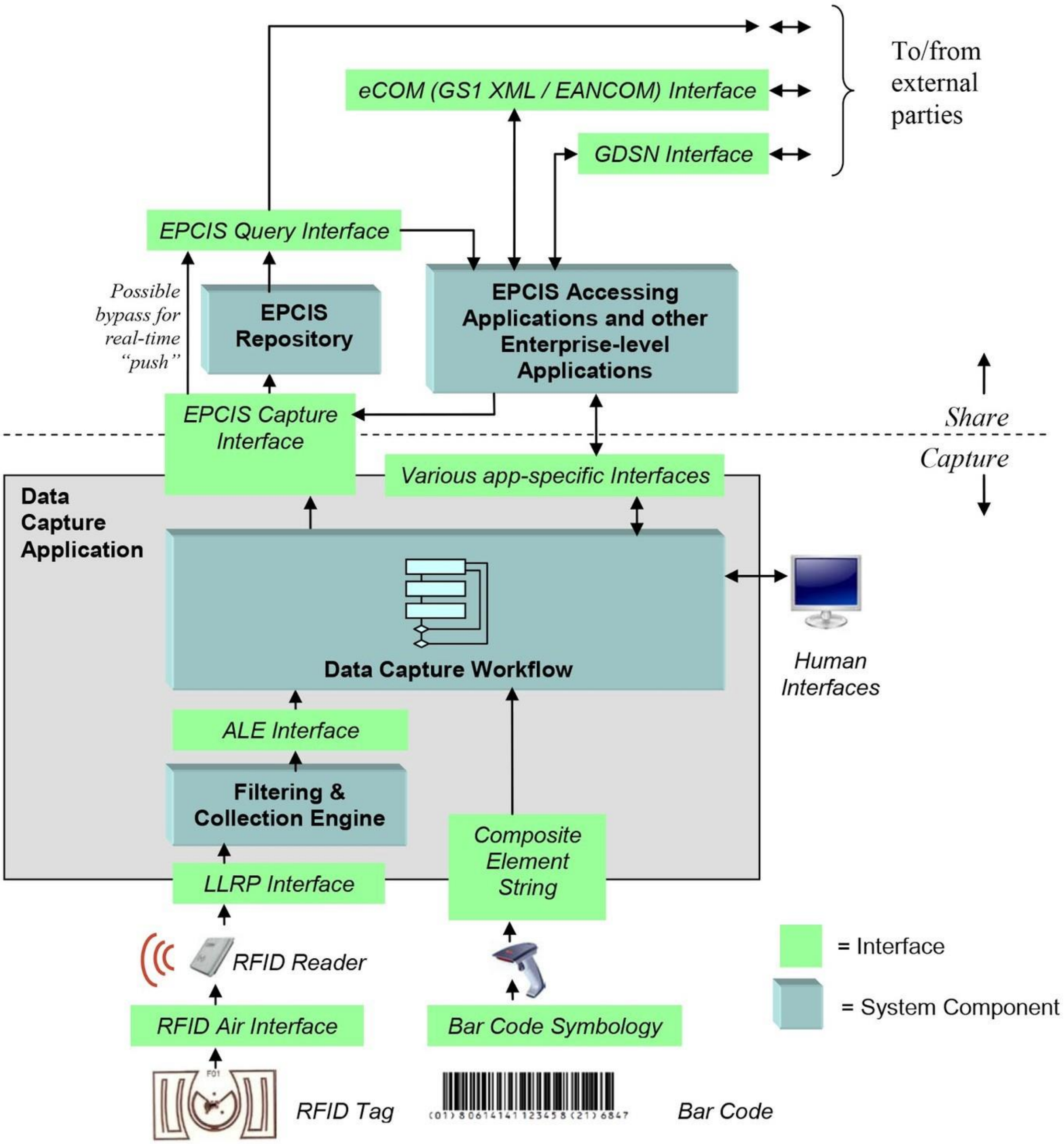
The EPCIS query interface provide a tool to query the EPICS repository for various events sent and captured by the EPICS system. Whereas the third party interfaces are there to provide detailed guidelines on the standards for various data type and format to the involved parties.

System Components

The two system components are available in the Share standard,

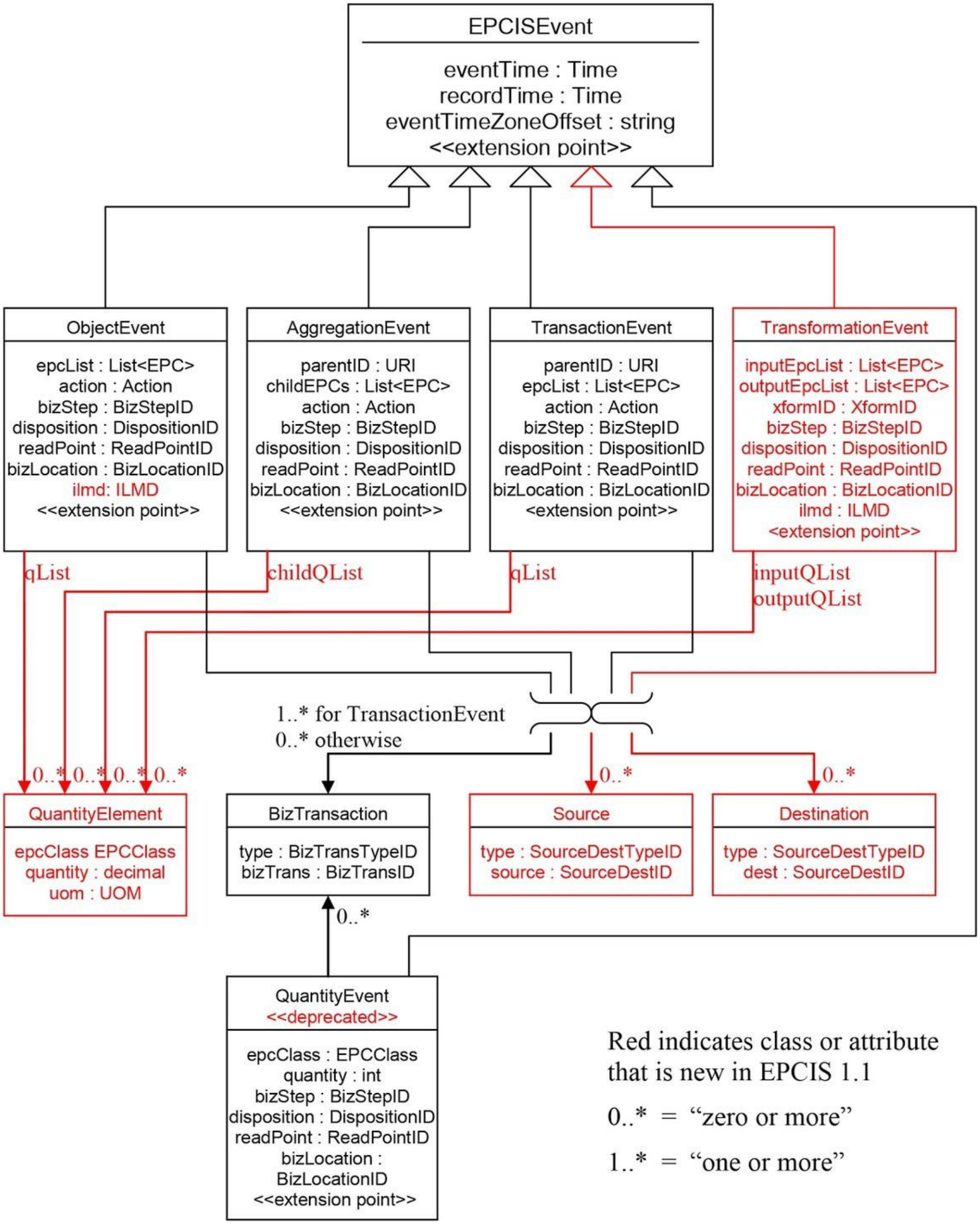
1. EPCIS Repository
2. EPCIS Accessing Applications

The EPICS Repository consist all information captured by the Capture standard and stored in a time series fashion. Whereas the EPICS accessing applications are the other required systems to provide access on the EPICS Repository, an ACL (Access Control List) to manage the various access level on the EPICS repository is a good example for the same.



EPICS Events

Events in EPCIS are the points where data can be generated by other processes and emit to the EPICS capture standard to store into the EPICS repository. A typical EPICS event consist of



Red indicates class or attribute that is new in EPCIS 1.1

0..* = “zero or more”

1..* = “one or more”

Object Event

An EPCIS event used to mark an observation or assertion about an object or objects.

Aggregation Event

An EPCIS event used to associate one object or a number of contained objects with their containers. This association is often called aggregation, containment, or packing.

Transaction Event

An EPCIS event used to associate or disassociate objects to business transactions.

Transformation Event

An EPCIS event used to represent objects that are consumed in one form and produced in another form.

Wireless Sensor Networks (WSN)

Nowadays an efficient design of a Wireless Sensor Network has become a number one area of research. A Wireless Sensor Network is a technology that responds and detects some kind of input from both the physical or environmental conditions, like heat, pressure, light, etc.The output of the sensor is an electrical signal that's transmitted to a controller for further processing.

What Is Wireless Sensor Network

SNs stands for Wireless Sensor Networks can be defined as a self-configured and infrastructure-less wireless network to observe physical or environmental conditions, like temperature, pressure, motion, sound, vibration, or pollutants, and to directly pass their data or information through the network to a sink which is also called the main location where the information is often observed and analyzed.

A base station or sink seems like an interface between the users and the network. It can convert back some required information from the network by injecting some queries and gathering results from the sink. Typically a wireless sensor network contains many thousands of sensor nodes.

The sensory nodes can communicate with each other by using radio signals. The wireless sensor nodes are equipped with sensing and radio transceivers, computing devices, and power components.

A sensor node in a wireless sensor network is inherently resource-constrained, also it has limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are installed, they're responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them.

Then the onboard sensors begin to collect information of their interest. And then the specifically designed devices of wireless sensor networks reply to those queries sent from a "control site" to perform specific instructions or provide sensing samples.

The working mode of the sensor nodes could also be either continuous or event-driven. GPS or Global Positioning System and LPA or local positioning algorithms can be used to obtain location and positioning information.

Wireless sensor devices are often equipped with actuators to "act" upon certain conditions. These networks are sometimes or normally called Wireless Sensor Network and Actuator Network.

Types of Wireless Sensor Networks

There are five types of Wireless Sensor Networks depending on the environment. Different Types of WSNs are:

1. Terrestrial Wireless Sensor Networks: Terrestrial WSNs are used for communicating base stations efficiently, and comprise thousands of wireless sensor nodes deployed either in an unstructured (ad hoc) or structured (Pre-planned) manner.

In an unstructured mode (ad hoc), the sensor nodes are randomly distributed within the target area that's dropped from a set plane.

In WSNs, the battery power is limited, however, the battery is provided with solar cells as a secondary power source. The conservation of energy of the WSNs gets by using low duty cycle operations, optimal routing, minimizing delays, and so on.

2. Underground Wireless Sensor Networks: In terms of deployment, maintenance, equipment cost considerations, and careful planning, underground wireless sensor networks are more expensive than terrestrial WSNs.

The Underground Wireless sensor networks UWSNs comprises several sensory nodes that are hidden in the ground to observe underground conditions.

Additional sink nodes are located above the bottom to transfer information from the sensor nodes to the base station, These underground WSNs deployed into the ground are difficult to recharge.

The sensor battery nodes equipped with limited battery power are also difficult to recharge. Additionally, the underground environment makes wireless communication a challenge because of the high attenuation and signal loss level.

3. Underwater Wireless Sensor Networks: About more than 70% of the earth's planet is occupied with water. These networks contain several sensor nodes and vehicles deployed underwater. Autonomous underwater devices and vehicles are used to collect data from these sensor nodes.

A challenge of underwater communication may be a long propagation delay, and bandwidth and sensor failures. Underwater, WSNs are equipped with a limited battery that can't be recharged or replaced.

The difficulty of energy conservation for underwater WSNs involves the development of underwater communication and networking techniques.

4. Multimedia Wireless Sensor Networks: Multimedia wireless sensor networks are proposed to enable tracking and monitoring of events in the sort of multimedia, like video, imaging, and audio.

These networks contain low-cost sensor nodes equipped with cameras and microphones. These sensory nodes of Multimedia WSNs are interconnected together over a wireless connection for data retrieval, data compression, and correlation.

5. Mobile Wireless Sensor Networks MWSNs: Mobile WSNs networks comprise a group of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes can also compute sense and communicate respectively.

Mobile wireless sensor networks are way more versatile than static sensor networks. The benefits of Mobile WSNs over Static WSNs include better and improved coverage, superior channel capacity, better energy efficiency, and so on.

Classification of Wireless Sensor Networks

Classification of Wireless Sensor Networks are as follows:

1. Static and Mobile WSN: All the sensor nodes are connected without movement and these are static networks in many applications. Some applications especially in biological systems- mobile sensor nodes are needed. These are called mobile networks. An example of a mobile network is animal monitoring.

2. Deterministic and Nondeterministic WSN: In deterministic wireless sensor networks, the sensor node position is calculated and fixed.

The deployment of sensor nodes is possible in a limited number of applications. The position of sensor nodes determination isn't possible because of several factors like harsh environments or hostile operating conditions. Such kinds of networks are non-deterministic and need a complex system.

3. Single Base Station and Multi Base Station WSN: In single base station WSNs, only one base station is used that is found close to the sensor node region.

All the nodes communicate with this base station, in the case of a multi-base station WSNs, more than one base station is used and a sensor node can transfer data to the closest base station.

4. Static Base Station and Mobile Base Station WSN: It is similar to sensor nodes, even base stations of the WSN are often either static or mobile. A static base station contains a fixed position usually close to the sensing region.

A mobile base station WSN moves around the sensing region because a load of sensor nodes is balanced.

5. Single-hop and Multi-hop WSN: In single-hop WSNs, the sensor nodes are directly connected to the base station. And in the case of multi-hop WSNs, peer nodes and cluster heads are used to relay the information to reduce energy consumption.

6. Self Reconfigurable and Non- Self Configurable WSN: In non-Self Configurable WSNs, the sensor networks cannot organize themselves in a network and consider a control unit to gather data.

In many WSNs, the sensor nodes can be able to organize and maintain the connection and work collaboratively with other sensor nodes to accomplish the task.

7.Homogeneous and Heterogeneous WSN: In the case of homogeneous WSNs, all the sensor nodes have the same energy consumption, storage capabilities, and computational power.

And in the case of heterogeneous WSNs, some sensor nodes have higher computational power and energy requirements than others and also the processing and communication tasks are divided accordingly.

Structure of Wireless Sensor Network

The structure of WSNs includes different types of topologies for radio communications networks.

1. Star Network: A star network is also called a single point-to-multipoint is a communications topology where one base station can send and receive a message to a variety of remote nodes. The remote nodes aren't permitted to send messages.

The benefit of these kinds of networks for wireless sensor networks includes simplicity, ability to keep the remote node's power consumption to a minimum. It allows low-power communications between the remote node and the base station.

The disadvantage of such a network is that the base station must be within the radio transmission range of all the individual nodes and isn't as robust as other networks because of its dependency on a single node to manage the whole network.

2. Mesh Network: A mesh network allows transmitting data from one node to another in the network that's within its radio transmission range.

This enables what is called multi-hop communications, i.e. if a node wants to send a message to a different node that's out of radio communications range, it can use an intermediate node to forward the message to the particular node.

This topology has the power of redundancy and scalability. When an individual node fails to work, a remote node still can communicate to the other node in its range, which successively, can forward the message to the specified location.

Additionally, the range of the network isn't necessarily limited by the range in between single nodes, it can simply be extended by adding more nodes to the system.

3. Hybrid Star: A hybrid Star is a combination between the star network and a mesh network that provides a strong and versatile communications network while maintaining the ability to keep the wireless sensor node's power consumption to a minimum.

In network topology, the sensor nodes with the lowest power aren't enabled with the ability to forward messages. This permits for minimal power consumption to be maintained.

Similarly, the various other nodes on the network are having multi-hop capability, allowing them to forward messages from the low power nodes to another on the network.

You can read also: **What is a Microcontroller, and How does it Work?**

The nodes whose having the multi-hop capability are of a higher power, and if possible, are often plugged into the electrical mains line.

Applications of wireless sensor network

Wireless sensor networks have been used widely over the world. The applications of wireless sensor networks are:

- **Military applications:** The military domain isn't only the primary field of human activity that is used by WSNs but it's also considered to have motivated the initiation of sensor network research.Tracking and environment monitoring surveillance applications use these kinds of networks. The sensor nodes from sensor networks are dropped to the sector of interest and are remotely controlled by a user.Security detections and enemy tracking are also performed by using these networks.

- **Health applications:** These networks are generally used by doctors to track and monitor patients.

- **Transport systems:** Most frequently used wireless sensor networks are in the transport systems like dynamic routing management, monitoring of traffic, and monitoring of parking lots, etc., use these networks.

- **Environmental trackings:** Wireless Sensor Networks have been used widely in the field of environment changes and their tracking.Forest detection, animal tracking, weather prediction, flood detection, forecasting, and also commercial applications like seismic activity prediction and also monitoring are using these networks like Air pollution monitoring, water quality monitoring, etc.

- **Threat detection**: The Wide Area Tracking System (WATS) is a device and a prototype network for detecting a ground-based nuclear device such as a nuclear bomb, and many other WSNs are also used for threat detection.

- Industrial process monitoring, rapid emergency response, automated building climate control, area monitoring, civil structural health monitoring, ecosystem, and habitat monitoring, etc., use these networks to monitor things.

Characteristics of Wireless Sensor Network

Some basic characteristics of Wireless Sensor Networks are as follows:

- Power consumption constraints for nodes using energy harvesting or mainly batteries are used.
- Examples of suppliers are ReVibe Energy and Perpetuum

- Having the ability to deal with node failures (resilience)
- Having some mobility of nodes (for highly mobile nodes see Mobile Wireless Sensor Networks)
- Scalability to the large scale of deployment
- Ability to resist harsh environmental conditions
- Heterogeneity of nodes
- Homogeneity of nodes
- Easy to use
- Cross-layer optimization

Issues in Wireless Sensor Networks

Various issues are occurring in wireless sensor networks WSNs such as design issues, topology issues, and other issues.

The complications in design in different types of wireless sensor networks include:

- Low latency
- Transmission Media
- Fault
- Coverage Problems
- Scalability

The complications in the topology of wireless sensor networks include the following.

- Sensor Holes
- Coverage Topology
- Geographic Routing

The big issues of a wireless sensor network WSNs include the following. These issues mainly affect the design and performance of wireless sensor networks.

- Operating System & Hardware for WSN
- Schemes for Medium Access
- Deployment
- Middleware
- Characteristics of Wireless Radio Communication
- Architecture
- Calibration
- Database Centric and Querying

- Network Layer
- Localization
- Sensor Networks Programming Models
- Synchronization
- Transport Layer
- Data Dissemination & Data Aggregation

The Advantages and Disadvantages of wireless sensor networks:

The advantages of wireless sensor networks WSNs are as follows:

- It is suitable for non-reachable places like over the sea, mountains, rural areas, or deep forests.
- It avoids lots of wiring.
- It might accommodate new devices at any time.
- It can also be accessed by using a centralized monitor.
- Flexible if there’s a random situation when the additional workstation is required.
- Implementation pricing is affordable.
- It’s flexible to undergo physical partitions.

The disadvantages of Wireless sensor networks are as follows:

- Less secure because hackers can enter the access point and obtain all the data.
- Lower speed as compared to a wired network.
- It’s easy for hackers to hack it we couldn’t control the propagation of waves.
- It is even more complicated compared to a wired network.
- Easily troubled by surroundings (walls, microwave, large distances because of signal attenuation, etc).
- Comparatively low speed of communication.
- Gets distracted by various elements like Blue-tooth.
- Still Costly (most importantly).

WSN Architecture

Types of WSN Architectures

The architecture used in WSN is sensor network architecture. This kind of architecture is applicable in different places such as hospitals, schools, roads, buildings as well as it is used in different applications such as security management, disaster management & crisis management, etc. There are two types of architectures used in wireless sensor networks which include the following. There are 2 types of wireless sensor architectures: Layered Network Architecture, and Clustered Architecture. These are explained as following below.

- Layered Network Architecture

- Clustered Network Architecture

Layered Network Architecture

This kind of network uses hundreds of sensor nodes as well as a base station. Here the arrangement of network nodes can be done into concentric layers. It comprises five layers as well as 3 cross layers which include the following.

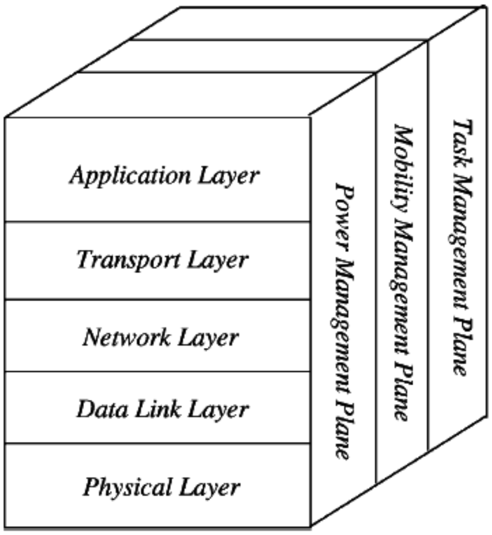
The five layers in the architecture are:

- Application Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer

The three cross layers include the following:

- Power Management Plane
- Mobility Management Plane
- Task Management Plane

These three cross layers are mainly used for controlling the network as well as to make the sensors function as one in order to enhance the overall network efficiency. The above mentioned five layers of WSN are discussed below.



Wireless Sensor Network Architecture

Application Layer

The application layer is liable for traffic management and offers software for numerous applications that convert the data in a clear form to find positive information. Sensor networks arranged in numerous applications in different fields such as agricultural, military, environment, medical, etc.

Transport Layer

The function of the transport layer is to deliver congestion avoidance and reliability where a lot of protocols intended to offer this function are either practical on the upstream. These protocols use dissimilar mechanisms for loss recognition and loss recovery. The transport layer is exactly needed when a system is planned to contact other networks.

Providing a reliable loss recovery is more energy-efficient and that is one of the main reasons why TCP is not fit for WSN. In general, Transport layers can be separated into Packet driven, Event-driven. There are some popular protocols in the transport layer namely STCP (Sensor Transmission Control Protocol), PORT (Price-Oriented Reliable Transport Protocol and PSFQ (pump slow fetch quick).

Network Layer

The main function of the network layer is routing, it has a lot of tasks based on the application, but actually, the main tasks are in the power conserving, partial memory, buffers, and sensor don't have a universal ID and have to be self-organized.

The simple idea of the routing protocol is to explain a reliable lane and redundant lanes, according to a convincing scale called a metric, which varies from protocol to protocol. There are a lot of existing protocols for this network layer, they can be separated into; flat routing and hierarchal routing or can be separated into time-driven, query-driven & event-driven.

Data Link Layer

The data link layer is liable for multiplexing data frame detection, data streams, MAC, & error control, confirm the reliability of point–point (or) point– multipoint.

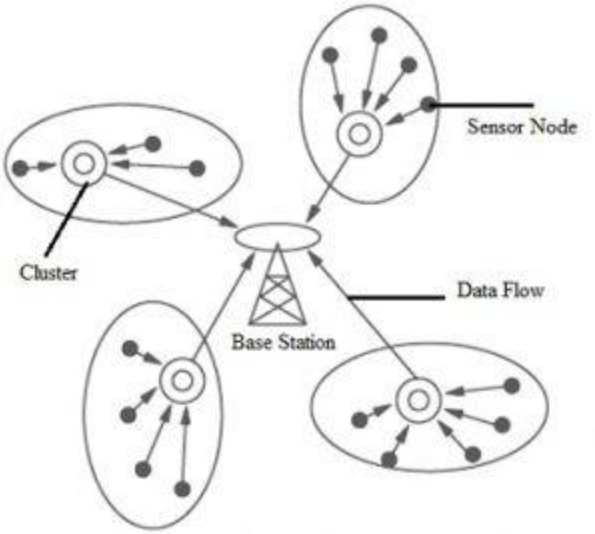
Physical Layer

The physical layer provides an edge for transferring a stream of bits above the physical medium. This layer is responsible for the selection of frequency, generation of a carrier frequency, signal detection, Modulation & data encryption. IEEE 802.15.4 is suggested as typical for low rate particular areas & wireless sensor networks with low cost, power consumption, density, the range of communication to improve the battery life. CSMA/CA is used to support star & peer to peer topology. There are several versions of IEEE 802.15.4.V.

The main benefits of using this kind of architecture in WSN is that every node involves simply in less-distance, low- power transmissions to the neighboring nodes due to which power utilization is low as compared with other kinds of sensor network architecture. This kind of network is scalable as well as includes a high fault tolerance.

Clustered Network Architecture

In this kind of architecture, separately sensor nodes add into groups known as clusters which depend on the "Leach Protocol" because it uses clusters. The term 'Leach Protocol' stands for "Low Energy Adaptive Clustering Hierarchy". The main properties of this protocol mainly include the following.



Clustered Network Architecture

- This is a two-tier hierarchy clustering architecture.
- This distributed algorithm is used to arrange the sensor nodes into groups, known as clusters.
- In every cluster which is formed separately, the head nodes of the cluster will create the TDMA (Time-division multiple access) plans.
- It uses the Data Fusion concept so that it will make the network energy efficient.

This kind of network architecture is extremely used due to the data fusion property. In every cluster, every node can interact through the head of the cluster to get the data. All the clusters will share their collected data toward the base station. The formation of a cluster, as well as its head selection in each cluster, is an independent as well as autonomous distributed method.

WSN NODE

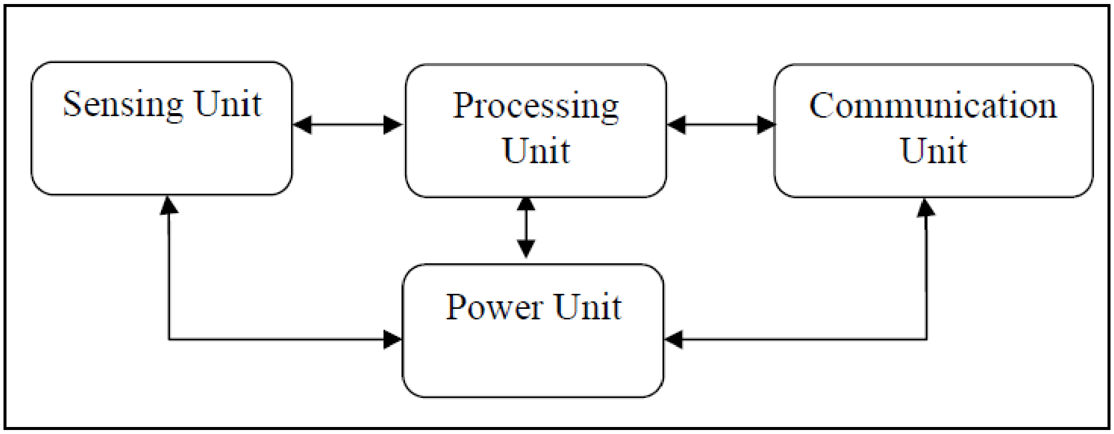


Figure 1.1 Basic Building Blocks of Sensor Node

The sensing unit of sensor nodes integrates different types of sensors like thermal sensors, magnetic sensors, vibration sensors, chemical sensors, bio sensors, and light sensors. The measured parameters from the external environment by sensing unit of sensor node are fed into the processing unit. The analog signal generated by the sensors are digitized by using Analog to Digital converter (ADC) and sent to controller for further processing.

The processing unit is the important core unit of the sensor node. The processor executes different tasks and controls the functionality of other components. The required services for the processing unit are pre-programmed and loaded into the processor of sensor nodes. The energy utilization rate of the processor varies depending upon the functionality of the nodes. The variation in the performance of the processor is identified by the evaluating factors like processing speed, data rate, memory and peripherals supported by the processors.

The computations are performed in the processing unit and the acquired result is transmitted to the base station through the communication unit. In communication unit, a common transceiver act as a communication unit and it is mainly used to transmit and receive the information among the nodes and base station and vice versa. There are four states in the communication unit: transmit, receive, idle and sleep. In general the functionality of the sensor node is shown in Figure.

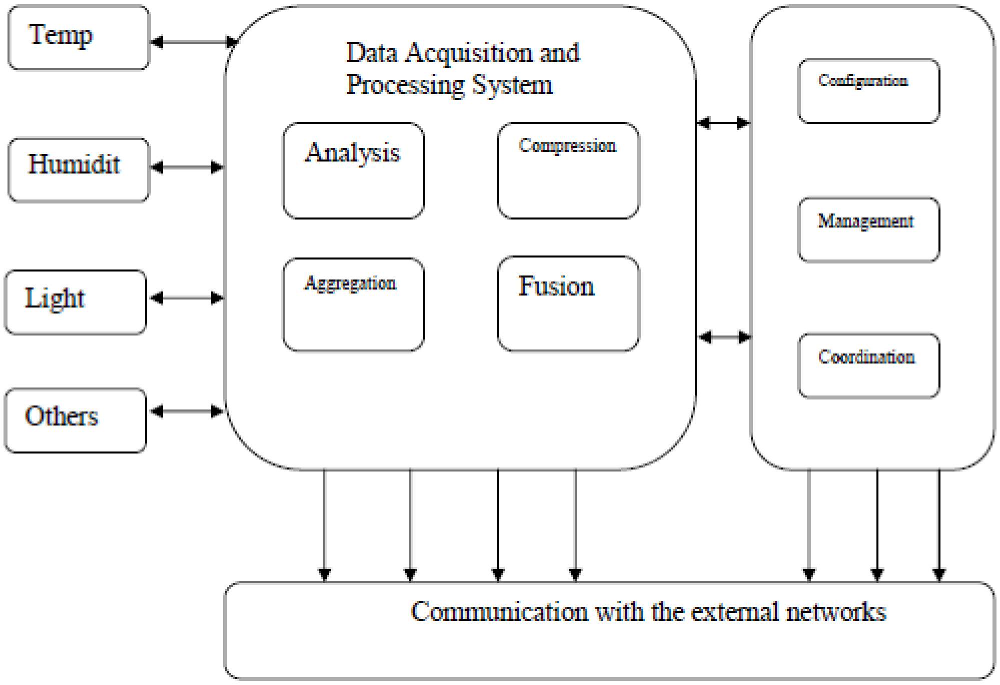


Figure 1.2 Functionality of A Sensor Node

The major characteristics of the sensor node used to evaluate the performance of WSN
Are

1. Fault tolerance: Each node in the network is prone to unanticipated failure. Fault tolerance is the capability to maintain sensor network functionalities without any break due to sensor node failures.
2. Mobility of nodes: In order to increase the communication efficiency, the nodes can move anywhere within the sensor field based on the type of applications.
3. Dynamic network topology: Connection between sensor nodes follows some standard topology. The WSN should have the capability to work in the dynamic topology.
4. Communication failures: If any node in the WSN fails to exchange data with other nodes, it should be informed without delay to the base station or gateway node.
5. Heterogeneity of nodes: The sensor nodes deployed in the WSN may be of various types and need to work in a cooperative fashion.
6. Scalability: The number of sensor nodes in a sensor network can be in the order of hundreds or even thousands. Hence, WSN designed for sensor networks is supposed to be highly scalable.
7. Independency: The WSN should have the capability to work without any central control point.
8. Programmability: The option for reprogramming or reconfiguring should be available for the WSN to become adaptive for any dynamic changes in the network.
9. Utilization of sensors: The sensors should be utilized in a way that produces the maximum performance with less energy.

10. Impracticality of public key cryptosystems: The limited computation and power resources of sensor nodes often make it undesirable to use public key algorithms.

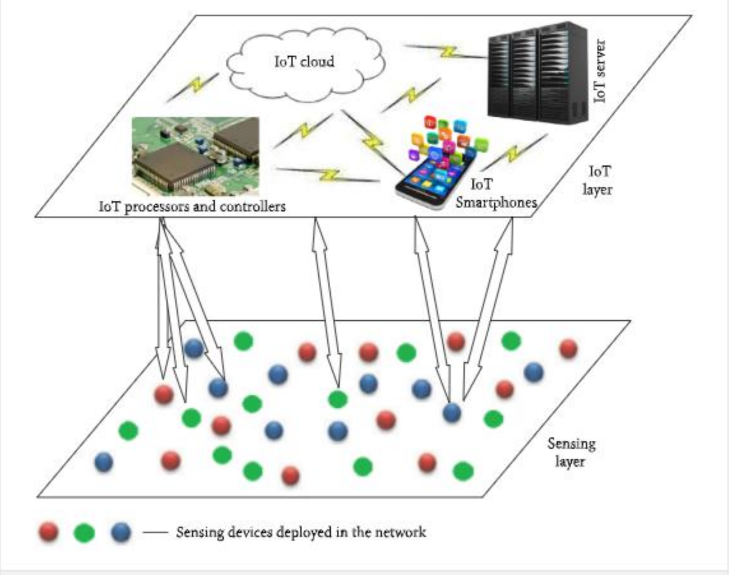
11. Lack of aprior knowledge of post-deployment configuration: If a sensor network is deployed via random distribution, the protocols will not be aware of the communication status between each nodes after deployment.

Clustering Principles in an Internet of Things

Two-layer IoT architectural framework, which represents a system model for clustering algorithms, is described. The sensor network is mainly used for acquiring the data from the surrounding environment depending upon the applications. IoT network consists of many sensing devices that are not necessarily to be connected to the Internet. In this view, it is preferred to have a framework that differentiates between IP-enabled devices and non-IP-enabled devices, that is, IoT devices and simple sensing nodes without IP capability. This kind of framework provides a layered architecture and is efficient in terms of communication for exchanging the data, which is validated through simulations described later in this paper.

Generally, in wireless sensor network, the nodes that are more than one hop away from the base station or access point consume energy rapidly. In IoT framework, if sensor motes or nodes are static to acquire the data which should be accessible anytime and anywhere, the multihop communication should be handled carefully for optimizing network resources for prolonging the lifetime of an application deployed for a specific task. It is preferred that IoT devices that have more energy and higher end processors as compared to underlying ordinary sensor nodes should be available to underlying sensor nodes for communication for at most two hops. The IoT devices may have mobility and this provides further flexibility to underlying static nodes for communication, so that many such static nodes in the network may be covered by mobile IoT devices. Thus, ordinary nodes may communicate through local group leader called cluster head (CH) to IoT device and the data acquired through ordinary sensor node may now be accessible anywhere and anytime. For dynamic scenario, the mobility may be incorporated in few IoT nodes whenever it is necessary. In this view, a two-layered IoT architectural framework is introduced.

The architectural framework for IoT applications consists of two layers, namely, IoT layer and sensing layer. Sensing layer is deployed with devices that are either IP-enabled or ID-enabled, depending on the requirement of the application. In this layer, deployed devices include sensors, actuators, and RFID devices. An IoT layer device comprises IP-enabled devices with IoT protocol stack which is significant in nature, because the IoT protocol stack has been introduced to operate in energy-constrained environment at any layer in the network hierarchy, that is, at data link using IEEE 802.15.4e networking using 6LowPAN,application layer using CoAP which results in a huge difference in developing the clustering approach in IoT as compared to that in WSN. These IoT devices are expected to have longer battery life and storage with the ability to perform real-time processing and communication, as compared to the functionalities provided by ordinary nodes. These features of IoT devices are also necessary for availability of the data or information acquired anywhere and anytime. An important job of mobile IoT nodes is to monitor and collect the information from CHs in the sensing layer. The two-layered IoT framework is shown in Figure .


IoT cloud
IoT server
IoT processors and controllers
IoT Smartphones
IoT layer
Sensing layer
Sensing devices deployed in the network

Two-layered hierarchical IoT architectural framework.

Communication between the devices in the IoT layer and sensing layer consists of different possibilities. As shown in Figure 1, one CH may communicate with one IoT node; two CHs may communicate with one IoT node; and one CH may communicate with two IoT nodes, depending on whether the IoT node is within its range of transmission or not. Although every node in sensing layer may not be in the range of other nodes, still all the sensing nodes are capable of understanding the scenario of entire network through communicating and collaborating with IoT nodes. Assuming that thousands of devices are scattered in the real-time network and are going to take part in accomplishing the given task, communication and connectivity should be addressed in an energy-efficient way. In this regard, the proposed clustering mechanisms for our two-layer architecture are more suitable for any real-time IoT-based application. From this discussion, it is clear that the IoT network may generate a huge amount of data over the time, and thus accessing the same anytime and anywhere is a challenging task. In such a scenario, it is important to have an IoT-based cloud environment that facilitates storing and processing the sensing information in the cloud, where IoT nodes perform real-time processing to accomplish a given task and forward the data to corresponding static IoT nodes or IoT cloud. IoT cloud is connected to IoT servers and IoT nodes are located physically anywhere. IoT server is basically an IoT node that is responsible for high level data processing that helps to make appropriate decisions. Similarly, IoT smartphone is also an IoT node that can be used to access the acquired information and to control the applications remotely. Likewise, IoT processors and controllers are also considered as IoT nodes for small scale card sized computers or embedded processors. For simplicity, the IP-based processors, controllers, and vehicles may be called IoT microcomputers, IoT controllers, and IoT vehicles, respectively. Also, they can be used as parameters on IoT cloud and can be utilized for various applications. Based on applications, the device mobility also plays an important role in IoT environment. Few of these devices may be static and others may be mobile. For instance, IoT cloud and IoT server can be considered as a static node, whereas IoT smartphones, IoT vehicles, IoT microcomputers, and IoT controllers can be considered as mobile nodes. This implies that these IoT nodes are portable and their positions vary at different times. This IoT-layered framework is used for developing the clustering algorithms.

Software Agents for Object Representation

For a long time, Intelligent Software Agent is an interesting research field and seen as a technology that has many potential to solve a variety of issues. The paradigm has its notable application in distributed systems. Nowadays, with every achievement and milestone in technology, software agents represent a leading solution to solve issues related to complexity and diversity of modern systems. Wooldridge [18] defines a software agent as a computer system that is able to interact with its environment and capable of making autonomous decision on behalf of its owner to meet its given objectives (see Figure i). Another definition for software agent is a software entity that works autonomously and continuously in a specific environment inhabited by other software entities.

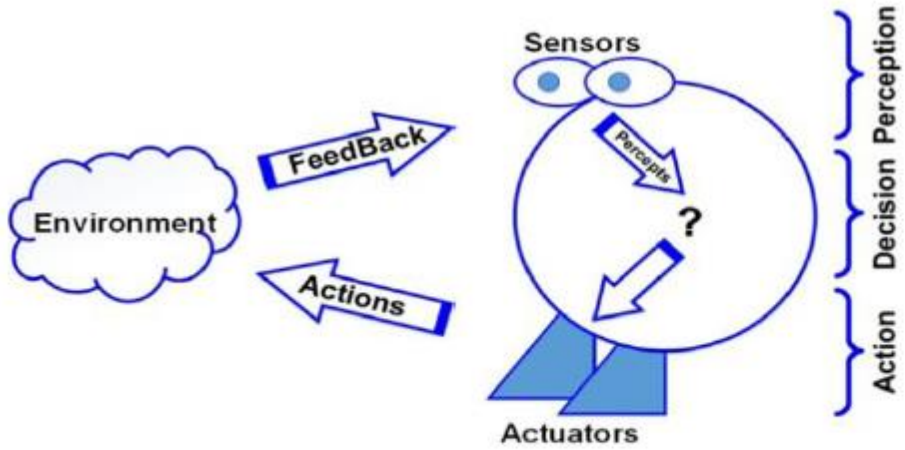


Figure i. Simple representation of software agent and environment

we can derive some distinct properties about software agents. Firstly, software agents are notable for being flexible and intelligent, so that it can cope with any environmental changes and respond to it without asking, to some extent, for its owner’s interference and guidance. In addition, software agents have the authority to do what they see suitable in any way to achieve their objectives and goals. Therefore, to achieve the given goals, software agents work autonomously and continuously in their environment, that enables them to learn from experience and form some kind of knowledge base. Finally, software agents are not alone in an environment, thus entailing their ability to interact, negotiate and cooperate with other agents and software entities in that environment. All these properties can be summarized to three distinguished characteristics: Reactivity, Pro-activeness and Social ability

1. Reactivity: Software agents have the ability to sense the surrounding environment and interact with it in manners that serve their objectives.
2. Pro-activeness: Software agents have the ability to change their behavior to be goal-directed by starting the first request or contact (take the initiative) in order to achieve their objectives and goals.
3. Social ability: Software agents have the ability to be social and interact with other agents to achieve their objectives.

Software agents enjoy many other characteristics, which include mobility, interactive, adaptive, coordinative, cooperative, negotiation, etc. Software agents enjoy a wide range of other characteristics, making it impossible for any researchers to include all of these in a single type. At BT labs, they reduce these characteristics to three important attributes only, which any basic software agent architecture could have as shown in Figure (ii)

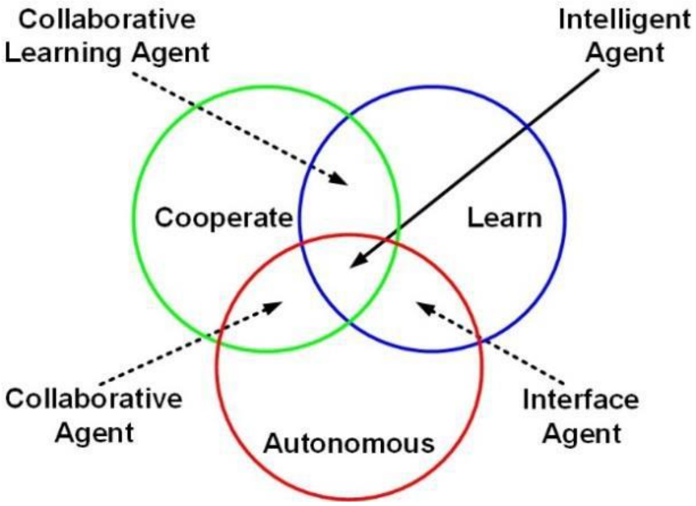


Figure (ii). Software agents general architecture

From these attributes they derived many types of software agents, which are as follows-

1. Collaborative Agents

This type of software agent is characterized by its autonomy and cooperation with other agents to achieve the tasks of its owners. In addition, in order to achieve its delegated goal, this agent type is able to negotiate with other agents to reach an acceptable agreement. The characteristics of collaborative software agents include autonomy, social ability, responsiveness and pro-activeness.

2. Interface Agents

This type of software agent is characterized by its autonomy, learning capability and working with users in the same work environment. An interface software agent represents a personal agent (autonomous personal assistant) that helps its owner by observing, monitoring and learning the actions. It then suggests new methods and better ways for doing the actions in the application. The agent, while collaborating with the user may not need to use an agent communication language as with other agents. Moreover, its collaboration with other agents is limited to asking for advice only and not for negotiation like collaborating agents.

3. Mobile Agents

A mobile agent is a software agent that is characterized by mobile capability, i.e. it is capable of transporting itself from one location to another. In addition, it is autonomous, cooperative and capable of travelling through computer networks to interact with foreign hosts and gather information on behalf of its owner and then returns to its owner after performing its delegated tasks. This type of software agent has a unique feature represented by its capability of exchanging information with other agents without giving all its information.

4. Information Agents

The main purpose for information agents is to help its owner to manage, manipulate and collect information from many distributed resources. It is identified by what it does unlike collaborative and interface agents. It is also characterized by its autonomous actions and mobility.

5. Reactive Agents

Reactive agents are featured by their simplicity and basic interaction with other agents. The agent is visioned as a collection of modules that function autonomously to perform a particular task. It also characterized by dynamic interaction with its environment, which leads to undesired complexity. Reactive agents are categorized as a low-level nature that is close to raw sensor data.

6. Hybrid and Heterogeneous Agents Hybrid agents are formed by combining two or more type of software agents in one single entity. This type of agents is used for an improved version of the software agent, which has the strength of the combined types, to meet the need of the designer's goals. Heterogeneous agents are similar to hybrid agents and are formed for the same purpose of improving the strong points or to reduce the weak points in the combined types. However, heterogeneous agents may include hybrid agents as well.

Data Synchronization

Data Synchronization is the process of establishing consistency and consolidation of data between different devices. It is fundamental to most IT solutions, especially in IoT and Mobile. Data Synchronization entails the continuous harmonization of data over time and typically is a complex, non-trivial process. Even corporates struggle with its implementation and had to roll back Data Sync solutions due to technical challenges.

Data Synchronization challenges include asynchrony, conflicts, slow bandwidth, flaky networks, third-party applications, and file systems that have different semantics.

Data Synchronization versus Data Replication in Databases

Data replication is the process of storing the same data in several locations to prevent data loss and improve data availability and accessibility. Typically, data replication means that all data is fully mirrored / backed up / replicated on another instance (device/server). This way, all data is stored at least twice. Replication typically works in one direction only (unidirectional); there is no additional logic to it and no possibility of conflicts.

In contrast, Data Synchronization typically relates to a subset of the data (selection) and works in two directions (bi-directional). This adds a layer of complexity, because now conflicts can arise. Of course, if you select all data for synchronisation into one direction, it will yield the same result as replication. However, replication cannot replace synchronization.

Why do you need to keep data in synchronization?

Think about it – if clocks were not in sync, everyone would live on a different time. While I can see an upside to this, it would result in much inefficiency as you could not rely on schedules. When business data is not in sync (up-to-date everywhere), it harms the efficiency of the organization due to:

- Isolated data silos
- Conflicting data / information states
- Duplicate data / double effort
- Outdated information states / incorrect data

In the end, the members of such an organization would not be able to communicate and collaborate efficiently with each other. They would instead be spending a lot of time on unnecessary work and “conflict resolution”. On top, management would miss an accurate overview and data-driven insights to prioritize and steer the company. The underlying mechanism that keeps data up-to-date across devices is a technical process called data synchronization (Sync). And while we expect these processes to “just work”, someone needs to implement and maintain them, which is a non-trivial task.
Growing data masses and shifts in data privacy requirements call for sensible usage of network bandwidth and the cloud. Edge computing with selective data synchronization is an effective way to manage which data is sent to the cloud, and which data stays on the device. Keeping data on the edge and synchronizing selective data sets effectively, reduces the data volume that is transferred via the network and stored in the cloud. Accordingly, this means lower mobile networking and cloud costs. On top, it also enables higher data security and data privacy, because it makes it easy to store personal and private data with the user. When data stays with the user, data ownership is clear too.

Identity Management System : Identity Management System manages identities individually and their privileges, roles, authorization, and authentication inside or outside the system boundaries to increase performance and security and to decrease delay, cost and repetitive operations. Identity Management System is a set of procedures organized manually and computerized. The Identity Management System aim is the identification and management of system resource utilization and the support of data integrity and privacy. Additionally, Identity Management System is responsible for generating certificates, managing attributes and roles, controlling accesses and authentication. Identity Management System includes a collection of decentralized software resources and several network protocols. Furthermore, the interface of Identity Management System with business components and Identity Management System procedures conforms to human resources, legislation and ethical procedures of businesses. Figure 1 presents the Identity Management System architecture where things such as simple devices (for example, sensors) and complex devices (for example, smartphones or mainframes) are shown. Each thing belongs to a specific user-space. and collaborates with other things despite their heterogeneity. Additionally, there are multiple services that require information gathered from internal or external sensors to be used in scenarios such as e-Health, enterprise etc.

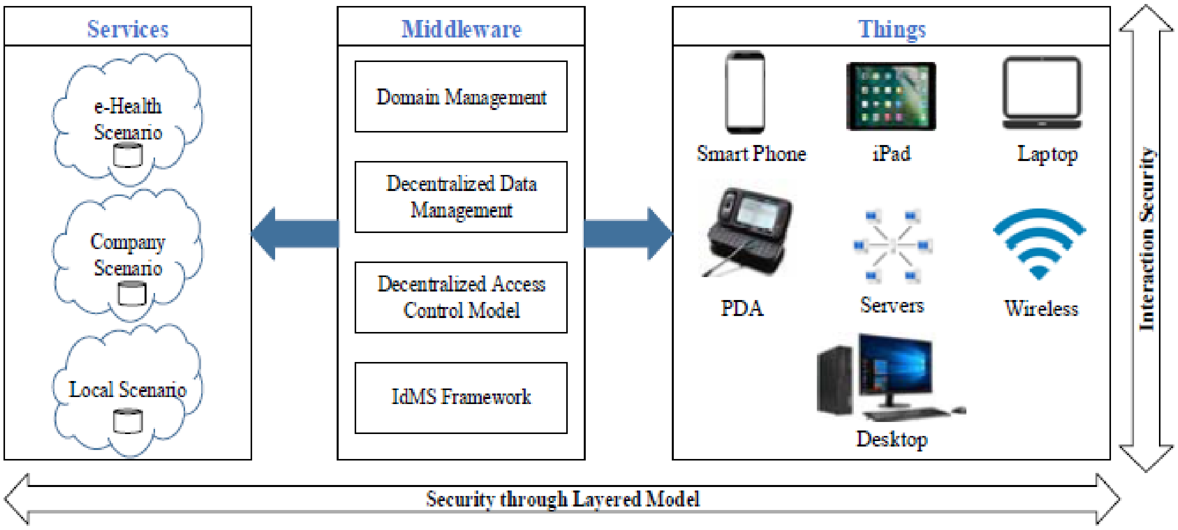
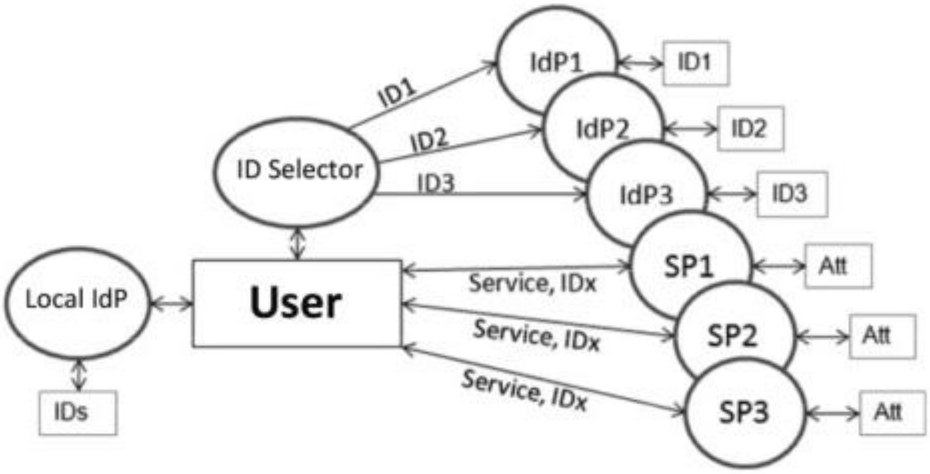


Figure 1. IdMS Framework

User-Centric Identity Management

Only the model presented in Figure allows the user to have complete control over their personal attributes. From their workstation, in either a local or remote fashion on the identity management site (IdP) of their choice, they have a portfolio of electronic identities and sometimes an identity selector. At the request of the services and SPs being accessed, they can select an identity and decide whether to issue certain attributes. U-Prove is a software solution of this type involving an IdP responsible for signing a token proving the validity of the user's attributes. Note that the SPs act individually in this model and can, albeit not without difficulty, offer collaborative services. SPs are increasingly inclined to propose authentication of user by leaving them to decide on the choice of IdP. This is, for example, the case with Yahoo who offers the possibility of authenticating users with their Facebook or Google account.



Identity management – user–centric model

Device centric identity management

Device-based identity utilizes security credentials on the device to authenticate with services and uses the identity provider to distribute the public key for the identity and maintains a list of attributes. It introduces a security token, which is sent to the users' device for authentication. Security credentials are stored in the device and are used to identify the service and authenticate the device requesting the service; thus, "each device maintains its own credentials for the user identity". The desired behavior is illustrated in Figure.

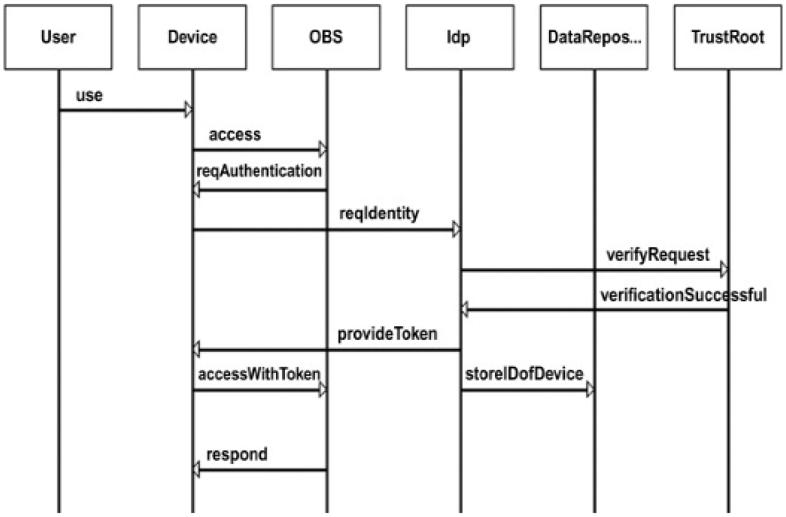


Figure . Device-based identity management model for a shopping system.

Business Model for Internet of Things:

“A business model describes the rationale of how an organization creates, delivers, and captures value.”

This definition illustrates the responsibility Product Managers have to deliver products that focus on value. In the IoT world, it’s very common to see products that simply add sensors to an existing product, display the data on a dashboard, and call it “value.” That should explain why companies are not getting traction in the market. The value is not really there.

IoT business model as having two parts:

1. Focuses on capturing and delivering value.
2. Leverages the unique characteristic of IoT products of having 24/7 connectivity to your customer’s environment to produce innovative and differentiated value.

Now that we have a definition, let’s look at seven of the top IoT business models (in no particular order).

1. Platform business model

The platform-based business model combines manufacturers and consumers in the marketplace to benefit both. The key to it is interoperability and interconnection of the devices and the business to generate revenue from related transactions.

Amazon and its Alexa voice recognition platform is a good example of this, as Amazon generates data through Alexa and then uses it to sell related products to consumers. Amazon charges third-party vendors and developers to create and release services on the platform, increasing its revenue and market reach.

2. Subscription model

Businesses can use the always-on connectivity of IoT devices to develop a recurring revenue business or subscription model. Like the as-a-service business model for technology, an IoT subscription model enables you to deliver continuous value to customers for a regular fee.

The IoT device breaks down the barrier between you and your customers, helping you foster an active relationship instead of a transactional one. Your device gathers more data about customers over time, giving you the chance to provide valuable features and products tailored to their unique needs.

3. Pay-per-usage model

Active sensors on your IoT devices mean you can regularly monitor your customer's environment to see how much they use your product or service. This gives you an opportunity to use a pay-per-usage business model where you charge them for the amount of time they actively interact with your product.

Many auto insurance companies are jumping into this model by offering a mileage-based insurance plan to customers. People don't pay for the IoT device installed on their car that tracks their driving usage and habits; they pay for the lower rates based on the data they generate on the device.

Rolls-Royce has been doing this for years with their TotalCare program, where airlines are charged on a fixed dollar per flying hour basis for the use of the engines on their planes. Rolls-Royce retains ownership of the engines and actively maintains them through IoT sensors that send telemetry in real-time to their monitoring sensors.

4. Asset-sharing model

Many industries have big expenditures when it comes to vital equipment. They want to be sure they're going to use the equipment enough to merit the expense. An asset-sharing business model for IoT could help with this by helping businesses sell their extra capacity back to the market. That way, each business pays a reduced price for the equipment and can still use it. Businesses could use this model on their own assets or as their main business by renting out large assets for sharing.

For consumers, this looks like car and scooter sharing companies such as Zipcar and Lime. For industrial firms in construction and mining, this means partnering with nearby businesses to share the cost of heavy machinery. IoT sensors would track the location and usage of the machines while also minimizing breakdowns by monitoring engine data in real-time. Each firm would have access to the data and could reserve time on the machines as needed.

5. Asset-tracking model

Connected devices in the supply chain help businesses identify, monitor and track assets in real time. It helps them protect in-field assets from loss or theft while monitoring for maintenance purposes. With the data generated by connected devices on these assets, businesses can check on their status regularly and know when to repair, fix or replace assets before they fail. This business model can also track the supply chain to identify inefficiencies, optimize workflows and increase visibility into usage.

Sierra Wireless helps global companies track their cold-chain cargo integrity with high-value IoT asset tracking platforms. Temperature-sensitive cargo such as food, produce and pharmaceuticals require precise temperature controls throughout the cold chain to maintain the integrity of the loads. As pressures mount for the refrigerated cargo industry as a whole, carriers can use these types of IoT sensors and online tracking platforms to ensure complete visibility of cargo, maintain adequate temperatures and take swift action on any identified issues.

6. Outcome-based model

The idea for this model is for customers to pay for the outcome of the IoT product, not the product itself. Many of the models discussed here are outcome-based, as they focus more on what customers gain from the device, rather than the device itself.

Self-monitoring products that can automatically reorder replacement parts or create a service request are good examples of this. Think of the HP printers that reorder ink cartridges automatically when you're nearly out of ink or the industrial company whose products automatically book a service call when they're not working optimally.

An innovative example of this is Propeller Health's digital health tool, Propeller. It enables those with asthma or chronic obstructive pulmonary disease manage their conditions in partnership with their clinicians and an IoT sensor attached to their inhalers. The sensors connect to the Propeller app on patients' smartphones and deliver insights on medication use, symptoms, triggers and environmental factors. Patients can share that data with their clinicians to inform their treatment plans and identify better outcomes.