UNIT-III (CO3)

IoT definition, Characteristics, IoT conceptual and architectural framework, Components of IoT ecosystems, Physical and logical design of IoT, IoT enablers, Modern day IoT applications, M2M communications, IoT vs M2M, IoT vs WoT, IoT reference architecture, IoT Network configurations, IoT LAN, IoT WAN, IoT Node, IoT Gateway, IoT Proxy, Review of Basic Microcontrollers and interfacing.

IoT Definition

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Characteristics:

There are the following characteristics of IoT as follows:

Connectivity

Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connectivity should be guaranteed at all times Without connection, nothing make sense.

Intelligence

The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

Scalability

The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

IoT conceptual and architectural framework

technology has a wide variety of applications and use of Internet of Things is growing so faster. Depending upon different application areas of Internet of Things, it works accordingly as per it has been designed/developed. But it has not a standard defined architecture of working which is strictly followed universally. The architecture of IoT depends upon its functionality and implementation in different sectors. Still, there is a basic process flow based on which IoT is built.

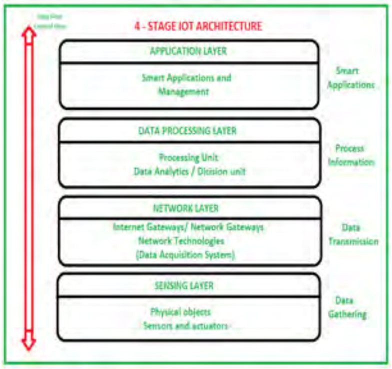

Figure 3.1: Stage of IOT Architecture

Components of IoT ecosystems

1. Sensing and embedding components

This is the first tier of an IoT ecosystem and it forms the backbone of the entire Internet of Things network. Data is indispensable for IoT and sensors are an important factor to ensure the accuracy and credibility of data. This essential layer consists of physical, micro appliances, embedded in an IoT device, which are responsible for collecting data or controlling a mechanism.

Sensors

Sensors work to gather minute data from the surrounding environment. They are sometimes also known as 'detectors' as the primary function of sensors is to detect even the slightest changes in the surrounding environment. This allows an IoT device to capture relevant data for real-time or post-processing.
Depending on the type of sensor, this small piece of hardware can measure absolutely anything. This can be smoke, motion or even blood pressure. While advanced sensors can measure a range of complexities, some IoT devices have multiple sensors bundled to be able to collect a range of data or perform multiple functions. Our smartphones for example have GPS, fingerprint, camera, tilt, motion and numerous other sensors, all bundled in one.
Smart AC'S or thermostats are able to sense room temperature and humidity levels at the same time. Depending on the device and use-case, different applications require different types of sensors.
Sensors are integral to achieve automation based on certain triggers. Considering the example of smart ACs, a person utilizing an automated mode function may set room temperature preferences between 73 and 77degrees Fahrenheit. As soon as a room temperature higher than 77 degrees is detected the device will transmit a command to the air conditioning unit to operate at specified settings. As soon as a room is cooler than 73 degrees the change in temperature will be detected and a signal will be transmitted to the AC to turn off.
In the image below, an IoT-enabled smart AC controller is used to make a conventional air conditioner smart. It consists of a sensor which detects room temperature conditions along with a transmitter to send signals and receive a response. The entire IOT ecosystem is in play to guide automated actions.

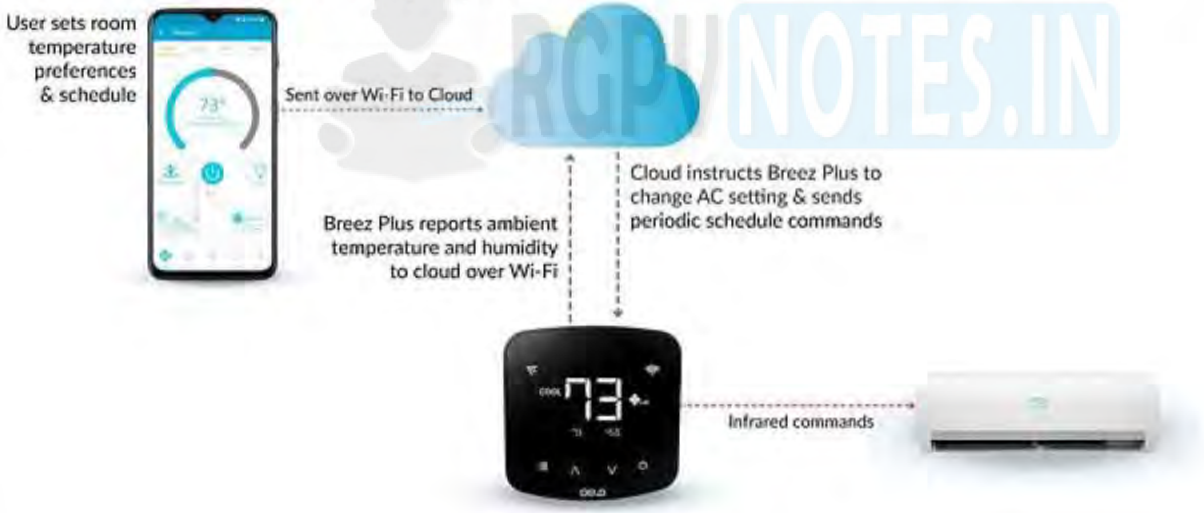
User sets room temperature preferences & schedule
73°
Sent over Wi-Fi to Cloud
Cloud instructs Breez Plus to change AC setting & sends periodic schedule commands
Breez Plus reports ambient temperature and humidity to cloud over Wi-Fi
COOL
73
Infrared commands

Figure 3.2: IOT Ecosystem

Thanks to advancements in technology, today's sensors are minute, smart and cheap! The selection of sensors depends on the purpose you wish to achieve. You may want the sensor to be able to detect motion, temperature, pressure, smoke or any other such trigger. The choice of sensors also depends on their accuracy, reliability of results, the range at which they should work, resolution and level of intelligence which in other words means their ability to deal with noise and interference.

Actuators

Actuators work opposite to that of sensors. While sensors, sense; actuators act. They receive a signal or a command and, on its basis, they cause an action. They are as crucial as sensors as once the sensors have detected a change in the environment, an actuator is required to make something happen based on the trigger.

2. Connectivity

IoT is a network involving devices, sensors, cloud and actuators and all these needs to interconnect with one another to be able to decipher data and consequently perform an action. Connectivity forms the second piece of the puzzle in the complex world of the IoT ecosystem.

Protocols

Once the data has been collected by the sensors, it requires a medium for transport. In other words, a communication channel is necessary between sensors and the cloud. IoT protocols are responsible for transferring data in the online world and this transmission can only be possible if two devices are safely connected. IoT standards and protocols involve an invisible language allowing physical objects to communicate with one another.

IoT gateways

Incoming, raw data from the sensors must pass through gateways to reach the cloud. Gateways translate network protocols ensuring seamless communication of all devices within the network. Essentially this makes the gateways a crucial communication point and is responsible for easy management of data traffic.

Moreover, gateways offer security by protecting the system from unauthorized access and malicious attacks. It can also be considered as a security layer as the data flowing through it protected by the latest encryption practices.

Gateways can also pre-process data from the sensors before sending it to the cloud

3. IoT cloud

Once the data has been collected and it has travelled to the cloud, it needs to be processed. The cloud is where the “smart stuff” takes place! This high-performance facility majorly ties the components to the IoT ecosystem together. It handles the data, stores it and makes decisions to make or break a deal. All of this is performed for colossal amounts of data in just under milliseconds – the time is critical for IoT, as especially in critical concerns such as health and safety, latency cannot be compromised.

While the main purpose of IoT solutions is to provide and act on real-time information, there needs to be a component that is able to handle enormous amounts of data to cater to the time-sensitive nature of the IoT model. This is where cloud systems come into play. They form the brain of the IoT ecosystem as they are typically responsible for processing, commanding or taking analytics into account for the collected data. Devices, protocols, gateway and storage are combined for efficient real-time data analysis.

4. IoT analytics and data management

Data may be a small word but it holds immense power that can pose a huge effect on any business. IoT Analytics is used to make sense of the vast amounts of analog data. This for example can include the determination of key performance indicators in a certain application where one may be interested in viewing errors or irregularities in real-time.

Once identified an immediate action would be required to prevent any undesirable scenarios. To put it differently, analytics involves converting raw data into useful insights that later are interpreted or analyzed to drive decision making.

Smart analytics is useful in multiple scenarios. The basic role is to analyse a situation and formulate a decision based on this. This can be basic such as analysing if a room’s temperature falls in an acceptable range, or complex if for example a car is just about to crash. Data analytics helps determine vital business insights. Deep learning models can be used for predictive analysis. Various learnings can be derived from the data to predict trends, plan ahead and make useful business decisions.

Analytics requires storage power and intelligent computation to be able to make sense of any data. Tasks such as this can be hosted on the cloud, depending on the IoT architecture.

5. End-user devices and user interface

The user interface is the visible component that is easily accessible and in control of the IoT user. This is where a user can control the system and set their preferences. The more user-friendly this component of the IoT ecosystem is, the easier is a user’s interaction.

A user may interact with the system via the device itself, or this interaction can be conducted remotely via smartphones, tablets, and laptops. Smart home systems such as Amazon Alexa or Google Home etc. also allow users to communicate with their “things”.

Design is a major consideration in today’s fast-paced world and one IoT device can set itself apart from a competitor on the basis of a strong design. Touch interfaces, use of colors, font, voice, and more are some of the factors that come to play here. While an attractive design is necessary, the interface should be user-friendly enough to avoid any difficulties for the user.

Physical and logical design of IoT

Physical Design of IoT refers to IoT Devices and IoT Protocols. Things are Node device which have unique identities and can perform remote sensing, actuating and monitoring capabilities. IoT Protocols helps Communication established between things and cloud-based server over the Internet

Things

Basically, Things refers to IoT Devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities. Things are is main part of IoT Application. IoT Devices can be various type, Sensing Devices, Smart Watches, Smart Electronics appliances, Wearable Sensors, Automobiles, and industrial machines. These devices generate data in some forms or the other which when processed by data analytics systems leads to useful information to guide further actions locally or remotely.

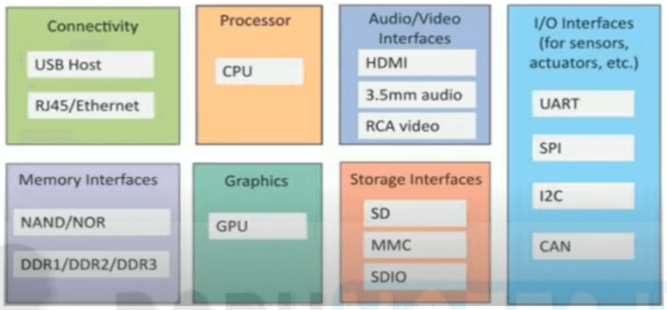

Figure 3.3: Things

Connectivity

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

Processor

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

Audio/Video Interfaces

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

Input/Output interface

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

Storage Interfaces

Things like SD, MMC, SDIO are used to store the data generated from an IoT device.
Other things like DDR, GPU are used to control the activity of an IoT system.

IoT Protocols

These protocols are used to establish communication between a node device and server over the internet. it helps to send commands to an IoT device and receive data from an IoT device over the internet. we use different types of protocols that present on both the server and client-side and these protocols are managed by network layers like application, transport, network, and link layer.

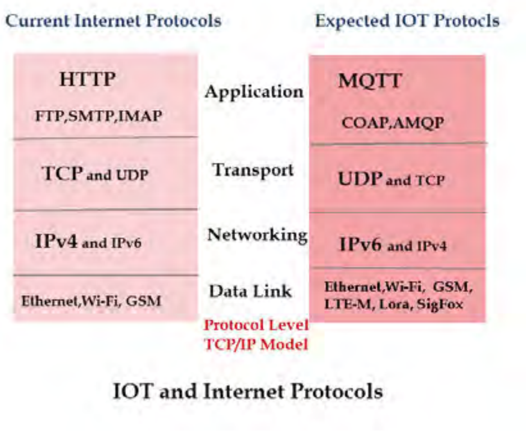

Figure 3.4: IoT Protocol

Application Layer protocol

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

HTTP

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

WebSocket

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

MQTT

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

Transport Layer

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

TCP

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

UDP

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

Network Layer

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

IPv4

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

IPv6

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

Link Layer

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

Ethernet

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

WiFi

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

Logical Design of IoT

The logical design of an IoT system refers to an abstract representation of entities and processes without going into the low-level specifies of implementation.

1. IoT Functional Blocks
2. IoT Communication Models
3. IoT Communication APIs

IoT Functional blocks

An IoT system consist number of functional blocks like Devices, services, communication, security, and application that provides the capability for sensing, actuation, identification, communication, and management.

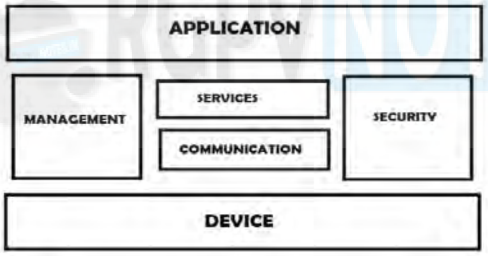

Figure 3.5: IoT Functional Block

These functional blocks consist of devices that provide monitoring control functions, handle communication between host and server, manage the transfer of data, secure the system using authentication and other functions, and interface to control and monitor various terms.

Application

It is an interface that provides a control system that use by users to view the status and analyse of system.

Management

This functional block provides various functions that are used to manage an IoT system.

Services

This functional block provides some services like monitoring and controlling a device and publishing and deleting the data and restore the system.

Communication

This block handles the communication between the client and cloud-based server and sends/receives the data using protocols.

Security

This block is used to secure an IoT system using some functions like authorization, data security, authentication, 2 step verification, etc.

Device

These devices are used to provide sensing and monitoring control functions that collect the data from the outer environment.

IoT Communication Models

There are several different types of models available in an IoT system that used to communicate between the system and server like the request-response model, publish-subscribe model, push-pull model, and exclusive pair model, etc.

Request-Response Communication Model

This model is a communication model in which a client sends the request for data to the server and the server responds according to the request. when a server receives a request it fetches the data, retrieves the resources and prepares the response, and then sends the data back to the client.

Publish-Subscribe Communication Model

In this communication model, we have a broker between publisher and consumer. here publishers are the source of data but they are not aware of consumers. they send the data managed by the brokers and when a consumer subscribes to a topic that managed by the broker and when the broker receives data from the publisher it sends the data to all the subscribed consumers.

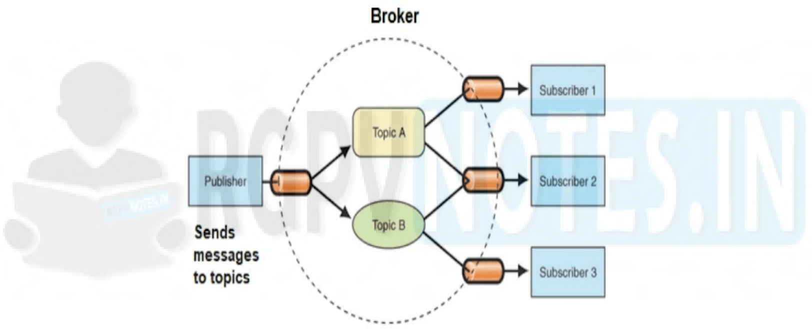

Figure 3.6: Publish subscribe communication model

Push-Pull Communication Model

It is a communication model in which the data push by the producers in a queue and the consumers pull the data from the queues. here also producers are not aware of the consumers.

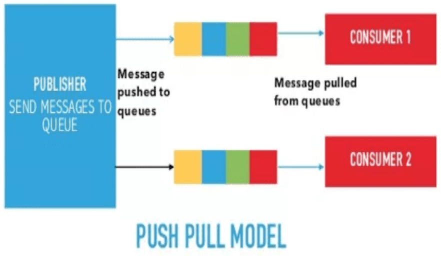

Figure 3.7: Push Pull Model

Exclusive Pair Communication Model

It is a bidirectional fully duplex communication model that uses a persistent connection between the client and server. here first set up a connection between the client and the server and remains open until the client sends a close connection request to the server.

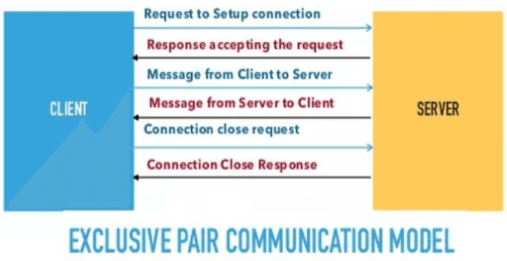
CLIENT
SERVER
Request to Setup connection
Response accepting the request
Message from Client to Server
Message from Server to Client
Connection close request
Connection Close Response
EXCLUSIVE PAIR COMMUNICATION MODEL

Figure 3.8: Exclusive Pair Communication Model

IoT communication APIs

These APIs like REST and WebSocket are used to communicate between the server and system in IoT.

REST-based communication APIs

Representational state transfer (REST) API uses a set of architectural principles that used to design web services. these APIs focus on the systems' resources that how resource states are transferred using the request-response communication model. this API uses some architectural constraints.

Client-server

Here the client is not aware of the storage of data because it is concerned about the server and similarly the server should not be concerned about the user interface because it is a concern of the client. and this separation is needed for independent development and updating of server and client. no matter how the client is using the response of the server and no matter how the server is using the request of the client.

Stateless

It means each request from the client to the server must contain all the necessary information to understand by the server. because if the server can't understand the request of the client, then it can't fetch the request data in a proper manner.

Cacheable

In response, if the cache constraints are given then a client can reuse that response in a later request. it improves the efficiency and scalability of the system without loading the extra data.
A RESTful web APIs is implemented using HTTP and REST principles.

WebSocket based communication API

This type of API allows bi-directional full-duplex communication between server and client using the exclusive pair communication model. this API uses full-duplex communication so it does not require a new connection setup every time when it requests new data. WebSocket API begins with a connection setup between the server and client and if the WebSocket is supported by the server then it responds back to the client with the successful response and after setup of a connection server and client can send data to each other in full-duplex mode.
this type of API reduces the traffic and latency of data and makes sure that each time when we request new data it cannot terminate the request.

IoT Enabler

System installers, repairers, craftsmen, electricians, plumbers, architects and do-it-yourselves who connect devices and systems to the Internet for personal use and for commercial and other business uses.
Below are the Top 5 enablers for Internet of things:
1. Selection of use cases with future growth: The most important enabler for IoT is careful selection of a use case today which has potential growth opportunities in the future. For example, a use case for agriculture may be based on adding sensors for extracting the information about the water and fertilizer level today, but in the long run there may be an evolution to send a drone with fertilizer if levels are observed to be low!
2. Technology Selection and Evolution: There are multiple options for IoT technologies available in the markets today, but what is important is to go with the mainstream 3GPP technologies for inter-working with advanced technologies like 5G in the future and at the same time providing the highest level of security. For example, like the case

of agriculture stated above, there could be a trigger to plow the field based on water levels by an unmanned ground vehicle (UGV) in the future based on 5G. Thus, is it very important to select technologies today which can support the evolution of the selected use cases to the next level.

3. Industry Partnerships: IoT has a vast landscape and it is essential for an enabler to have partnerships to facilitate development of long-term solutions, it is very unlikely for a IoT enabler to have it all in-house. Industry partnerships are required for different aspects, an enabler would require them for understanding the vertical (Like automobiles, education etc.) partnering for providing devices or associated hardware (like sensors, cameras etc.) and for providing IT systems and platforms for enabling IoT. It is assumed that the basic IoT connectivity would be always provided by a Mobile operator.

4. IT Transformation: When we talk about IoT, we are not talking about humans, so it will not make sense to send a connectivity bill to a sensor! Thus, it is essential that a IoT enabler has a IT system which can cater to the needs of IoT, mechanisms for flexibility and scalability for admitting billions of devices. There are also certain use cases where a system has to cater to requirements for multi country solutions like you cannot expect that your connected car stops working when you drive from Malaysia to Singapore.

5. Marketing with a Non-Mobile Mindset: The first and foremost requirement for IoT is to have a non-mobile mindset – we are no longer talking about mobile phones and humans we have a plethora of other devices which will be connected and provide solutions so a sensor will not walk up to a shop to enroll for connectivity! For any big enterprise investing in IoT it will be imperative to have a long-term view where the short-term vision solutions will not fly bring the futuristic thought the first!

Modern day IoT applications

- Smart Homes
- Smart City
- Self-driven Cars
- IoT Retail Shops
- Farming
- Wearables
- Smart Grids
- Industrial Internet

M2M Communication

Machine-to-machine, or M2M, is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans. Artificial intelligence (AI) and machine learning (ML) facilitate the communication between systems, allowing them to make their own autonomous choices.

M2M technology was first adopted in manufacturing and industrial settings, where other technologies, such as SCADA and remote monitoring, helped remotely manage and control data from equipment. M2M has since found applications in other sectors, such as healthcare, business and insurance. M2M is also the foundation for the internet of things (IoT).

M2M applications:

Utility Companies
Traffic Control
Telemedicine
Inventory Management
Banking

IoT vs M2M

Basis	IoT	M2M
Abbreviation	Internet of Things	Machine to Machine
Intelligence	Devices have objects that are responsible for decision making	Some degree of intelligence is observed in this
Connection type used	The connection is via Network and using various communication types.	The connection is a point to point
Communication protocol used	Internet protocols are used such as HTTP, FTP, and Telnet.	Traditional protocols and communication technology techniques are used
Data Sharing	Data is shared between other applications that are used to improve the end-user experience.	Data is shared with only the communicating parties.
Internet	Internet connection is required for communication	Devices are not dependent on the Internet.
Scope	A large number of devices yet scope is large.	Limited Scope for devices.
Business Type used	Business 2 Business(B2B) and Business 2 Consumer(B2C)	Business 2 Business (B2B)
Open API support	Supports Open API integrations.	There is no support for Open API's

Internet of Things vs Web of Things

- From the developer's perspective, the WoT enables access and control over IoT resources and applications using mainstream web technologies (such as HTML 5.0, JavaScript, Ajax, PHP, Ruby n Rails, etc.)
- The approach to building WoT is therefore based on rest API s, which enable both developers and deployers to benefit from the popularity and maturity of web technologies.
- Still, building the WoT has various scalability security etc. challenges especially as part of a roadmap towards a global WoT.
- While IoT is about creating a network of objects, things, people, system and applications, WoT tries to integrate them to Web.
- Technically speaking WoT can be thought as flavor/Option of an application layer added over the IoT‘s network layer.
- However, the scope of the Internet of things applications is broader and includes systems that not accessible through the web (eg. conventional WSN and RFID system)

Components of IoT

The fundamental components of IoT system are:

1. Sensors/Devices

First, sensors or devices help in collecting very minute data from the surrounding environment. All of this collected data can have various degrees of complexities ranging from a simple temperature monitoring sensor or a complex full video feed. A device can have multiple sensors that can bundle together to do more than just sense things. For example, our phone is a device that has multiple sensors such as GPS, accelerometer, camera but our phone does not simply sense things. The most rudimentary step will always remain to pick and collect data from the surrounding environment be it a standalone sensor or multiple device

2. Connectivity

Collected data is sent to a cloud infrastructure but it needs a medium for transport. The sensors can be connected to the cloud through various mediums of communication and transports such as cellular networks, satellite networks, Wi-Fi, Bluetooth, wide-area networks (WAN), low power wide area network and many more. Every option we choose has some specifications and trade-offs between power consumption, range, and bandwidth. So, choosing the best connectivity option in the IOT system is important.

3. Data Processing

Once the data is collected and it gets to the cloud, the software performs processing on the acquired data. This can range from something very simple, such as checking that the temperature reading on devices such as AC or heaters is within an acceptable range.

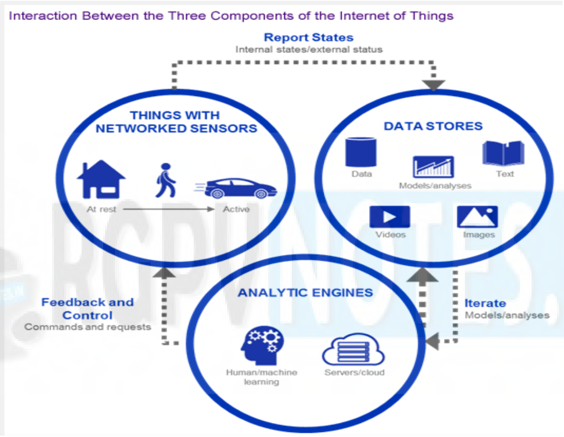

Figure 3.9: Components of the Internet of Things

4. User Interface

User sometimes might also have an interface through which they can actively check in on their IoT system. For example, a user has a camera installed in his house; he might want to check the video recordings and all the feeds through a web server. However, it’s not always this easy and a one-way street. Depending on the IoT application and complexity of the system, the user may also be able to perform an action that may backfire and affect the system. For example, if a user detects some changes in the refrigerator, the user can remotely adjust the temperature via their phone.

There are also cases where some actions perform automatically. By establishing and implementing some predefined rules, the entire IOT system can adjust the settings automatically and no human has to be physically present. Also, in case if any intruders are sensed, the system can generate an alert not only to the owner of the house but to the concerned authorities.

Functional Components of IoT

There are five key Functional components of IoT, things, gateways, mobile devices, the cloud and the enterprise as described below:

1. Things

Physical objects things that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. Things can also be self-sufficient and communicate to the internet for only centralized coordination and analysis.

2. Gateways

Gateways provide the application logic, store data and communicate with the internet for the things that are connected to it. Things don’t have to be as smart, because the gateway can provide these resources.

3. Smartphone's

Smart phones (or any mobile device) may house the application logic, store data and communicate with the internet on behalf of things that are connected to it. Things don't have to be as smart, because the smart phone provides these resources.

4. The Cloud

The cloud can act as the central connection hub, power analytics and provision data storage. Things don't have to be as smart, because the cloud will provide these resources.

5. The Enterprise

This architectural role is focused on keeping connected machines, application logic, and analytics and data storage on-premises that is, behind the enterprise firewall.

IoT Service oriented Architecture

A service-oriented architecture is an approach used to create an architecture based upon the use of services. Services (such as RESTful Web services) carry out some small function, such as producing data, validating a customer, or providing simple analytical services.

The service-oriented architecture is a widely used design pattern. It effectively combines individual units of software to provide higher level of functionality. The communication involves either simple data passing, or it could involve two or more services coordinating some activity. If a service-oriented architecture is to be effective, we need a clear understanding of the term service. A service is a function that is well defined, self-contained, and does not depend on the context or state of other services. SOA provides a strategic capability for integrating business processes, data, and organizational knowledge. SOA is governed by a well-defined set of frameworks. Service composition and service discovery are the two major elements of SOA.

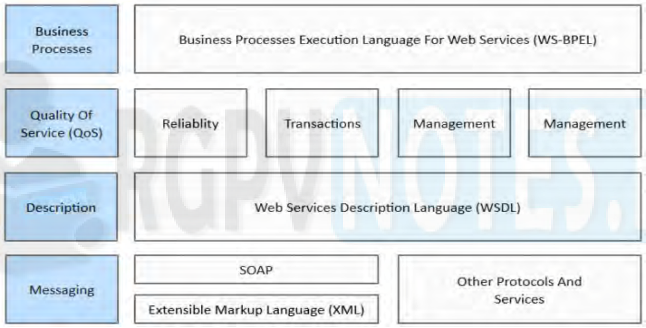
Business Processes
Business Processes Execution Language For Web Services (WS-BPEL)
Quality Of Service (QoS)
Reliablity
Transactions
Management
Management
Description
Web Services Description Language (WSDL)
Messaging
SOAP
Extensible Markup Language (XML)
Other Protocols And Services

Figure 3.10: Service-oriented Architecture (SOA)

IoT Challenges

The Internet of Things collects copious amounts of information that pass on as data. The general purpose of the technology is to make things "smarter" like appliances, every day and household items, industrial machinery and much more.

Here are some challenges presented by IoT:

1. Security

The most significant and arguably unsolvable challenge relates to security or, more specifically, cyber security as it pertains to information technology. It's not just the data connection that is vulnerable, but everything connected to the actual hardware.

Imagine a smart manufacturing unit equipped with IoT sensors. A property manager or maintenance associate can use a mobile device to check the device status, read incoming data or send commands. But what if a foreign attacker were to seize control of the machine using a known vulnerability or weak security measures to gain access.

2. Privacy

Most online connections are secured using a form of encryption. Means the data is locked behind a software key and cannot be decrypted translated without the appropriate authorization.

Some of the more basic forms of encryption are easy to break, but they can still take a long time, slowing down any nefarious parties. Ultimately, it means that encrypted data is, and always will be, exponentially more secure than raw, unprotected data.

3. Resource Consumption

Electronics require energy to operate and IoT devices are no exception. They must actively transmit data 24/7, which means support from other technologies, including network adapters, gateways and more.

Beyond just electricity, data requires physical storage. Even with cloud and edge computing solutions, there is still a remote server connected to the network that is being used to house the digital content. Servers require an excessive amount of energy, as do data centers that require large-scale cooling systems to operate under heavy loads.

4. 6LoWPAN for IoT

6LoWPAN provides the upper layer system for use with low power wireless communications for IoT and M2M, originally intended for 802.15.4, it is now used with many other wireless standards. The 6LoWPAN system is used for a variety of applications including wireless sensor networks. This form of wireless sensor network sends data as packets and using IPv6 - providing the basis for the name - IPv6 over Low power Wireless Personal Area Networks.

IoT with IEEE 802.15.4

The Industrial Internet of Things is predicated on large-scale, distributed sensor/control networks that can run unattended for months to years with very low power consumption. The characteristic behaviour of this type of network entails very short bursts of message traffic over short distances using wireless technologies, often described as a low-rate, wireless personal area network (LR-WPAN). We keep the data frames short to lessen the possibility of radio interference forcing the need to retransmit. One such LR-WPAN approach uses the IEEE 802.15.4 standard. This describes a physical layer and media access control that are often used in the industrial control and automation applications referred to as Supervisory Control and Data Acquisition (SCADA).

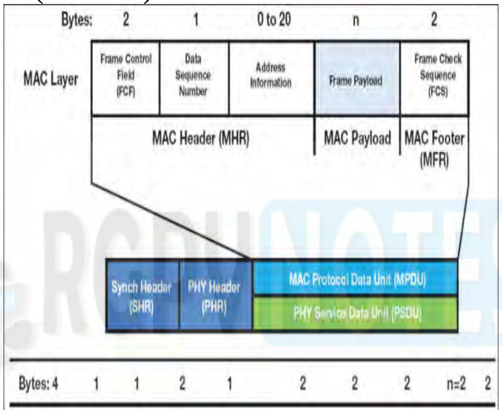

Figure 3.11: IEEE 802.15.4 Frame Format

ZigBee and its types

Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Hence, Zigbee is a low-power, low data rate, and close proximity (i.e., personal area) wireless ad hoc network.

The technology defined by the Zigbee specification is intended to be simpler and less expensive than other wireless personal area networks (WPANs), such as Bluetooth or more general wireless networking such as Wi-Fi. Applications include wireless light switches, home energy monitors, traffic management systems, and other consumer and industrial equipment that require short-range low-rate wireless data transfer.

Types of ZigBee devices

- ZigBee coordinator (ZC): The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is precisely one ZigBee coordinator in each network since it is the device that started the network originally (the ZigBee LightLink specification also allows operation without a ZigBee coordinator, making it more usable for off-the-shelf home products). It stores information about the network, including acting as the trust center and repository for security keys.
- ZigBee router (ZR): As well as running an application function, a router can act as an intermediate router, passing data on from other devices.
- ZigBee end device (ZED): Its functionality to talk to the parent node (either the coordinator or a router) it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory and thus can be less expensive to manufacture than a ZR or ZC.

RFID Features

The main features of RFID are as follows:

1. Able to Read and Write data without direct contact

The RF tag can contain up to several kilobytes of rich information. All of the data required for each process (process history, inspection history etc) can be freely stored, without the need for direct contact. This makes it possible to develop paperless sites, where the causes of production stop are reduced.

2. Highly pliable and reliable system configuration

With the technology to decentralize information, the load on higher systems is reduced. This means that system development costs can also be reduced, systems can be implemented significantly faster, and the system is much more flexible when making changes. Also, "the unification of items with their information" for each process and site can make it possible to manage production/processes and product quality without errors. And, with the latest information contained in RF tags, work can continue offline in emergencies, significantly shortening the time required to restore processes.

3. Adoption of space transmission technology and protocols

As opposed to barcodes which simply look for 1 or 0, advanced space transmission technologies and specialized protocols are employed for transmission through the air. 16 bits CRC is added to the information as it is transmitted. More than 18 bits Burst errors can be detected at a ratio of 00.9985%, providing a very high reliability in the transfer. Also, since there are no mechanical devices involved such as with the raster scan method for barcodes, the likelihood of malfunction and other problems is greatly reduced.

4. Electric and electromagnetic wave transmission

Unlike barcodes, since communication occurs by means of electric and electromagnetic waves, erroneous readings due to dirt, moisture, oil etc are cancelled out. Even if there is dust, moisture etc., or anything other than metal between the antenna and the RF tag, it will not affect transmission. And since the communication range is wide, there is no need for extreme positioning which can greatly reduce the time and cost of design.

5. Simultaneously access information of multiple RF tags

Some RFID systems are equipped with a function that allows you to simultaneously read the information of multiple RF tags existing within the transmissions area of the Reader/Writer.

RFID Working Principle

RFID belongs to a group of technologies referred to as Automatic Identification and Data Capture (AIDC). AIDC methods automatically identify objects, collect data about them, and enter those data directly into computer systems with little or no human intervention. RFID methods utilize radio waves to accomplish this. At a simple level, RFID systems consist of three components: An RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which is used to transmit data to the RFID reader (also called an interrogator).

The reader then converts the radio waves to a more usable form of data. Information collected from the tags is then transferred through a communications interface to a host computer system, where the data can be stored in a database and analyzed later.

RFID Applications

RFID technology is employed in many industries to perform such tasks as:

– Inventory management
– Asset tracking
– Personnel tracking
– Controlling access to restricted areas
– ID Badging
– Supply chain management
– Counterfeit prevention (e.g. in the pharmaceutical industry)

NFC (Near Field communication)

NFC has its origins in radio frequency identification (RFID) technology, which uses electromagnetic fields to encode and read information. Any NFC-enabled device has a small chip that is activated when it comes in close proximity to another NFC chip (10 centimeters or less). NFC therefore enables simple and safe two-way interactions between electronic devices.

There are two types of NFC devices: active and passive. Active NFC devices, such as smart phones, are capable of both sending and receiving information. Passive NFC devices can transmit information when read by active devices but cannot read information themselves.

Application of NFC technology as follows:

- Performing contactless transactions
- Connecting electronic devices with a single tap
- Sharing business cards
- Accessing information from a smart poster
- Downloading digital content
- Providing credentials for security systems

The benefits of NFC include easy connections, rapid transactions, and simple exchange of data. NFC serves as a complement to other popular wireless technologies such as Bluetooth, which has a wider range than NFC, but which also consumes more power.

Bluetooth

Bluetooth is also important for the rapidly growing Internet of Things, including smart homes and industrial applications. It is a low power, low range, high bandwidth connectivity option. When Bluetooth devices connect to each, it follows the parent-child model, meaning that one device is the parent and other devices are the children.

The parent transmits information to the child and the child listens for information from the parent. Invented by Ericsson in 1994, Bluetooth was intended to enable wireless headsets. Bluetooth has since expanded into a broad variety of applications including Bluetooth headsets, speakers, printers, video game controllers, and much more.

A Bluetooth parent can have up to 7 children, which is why your computer can be connected via Bluetooth to multiple devices at the same time. When devices are connected via Bluetooth, it's called a "piconet". Not only can a device be a parent in one piconet and a child in a different piconet at the same time, but the parent-child relationship can also switch.

A drawback of Bluetooth is lower bandwidth, but for many industrial applications this higher bandwidth simply isn't needed. Bluetooth is also useful in a smart home setting. Again, many devices in the smart home don't need high bandwidth connections and it's much easier to set up Bluetooth.

Wireless Sensor Network

A Wireless Sensor Network is one kind of wireless network includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes called motes. These networks certainly cover a huge number of spatially distributed, little, battery-operated, embedded devices that are networked to caringly collect, process, and transfer data to the operators, and it has controlled the capabilities of computing & processing.

The most common WSN architecture follows the OSI architecture Model. The architecture of the WSN includes five layers and three cross layers

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.

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.

Data Link Layer

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

Physical Layer

The physical layer provides an edge for transferring a stream of bits above physical medium. This layer is responsible for the selection of frequency, generation of a carrier frequency, signal detection, Modulation & data encryption.

Characteristics of Wireless Sensor Network

The characteristics of WSN include the following:

- The consumption of Power limits for nodes with batteries
- Capacity to handle with node failures
- Some mobility of nodes and heterogeneity of nodes
- Scalability to large scale of distribution
- Capability to ensure strict environmental conditions
- Simple to use
- Cross-layer design

Advantages of Wireless Sensor Networks

The advantages of WSN include the following:

- Network arrangements can be carried out without immovable infrastructure.
- Apt for the non-reachable places like mountains, over the sea, rural areas and deep forests.
- Flexible if there is a casual situation when an additional workstation is required.
- Execution pricing is inexpensive.
- It avoids plenty of wiring.
- It might provide accommodations for the new devices at any time.
- It can be opened by using a centralized monitoring.

Wireless Sensor Network Applications

Wireless sensor networks may comprise of numerous different types of sensors like low sampling rate, seismic, magnetic, thermal, visual, infrared, radar, and acoustic, which are clever to monitor a wide range of ambient situations. Sensor nodes are used for constant sensing, event ID, event detection & local control of actuators.

The applications of wireless sensor network mainly include:

- Military Applications
- Health Applications
- Environmental Applications
- Home Applications
- Commercial Applications
- Area monitoring
- Health care monitoring
- Environmental/Earth sensing
- Air pollution monitoring
- Forest fire detection
- Landslide detection
- Water quality monitoring
- Industrial monitoring