Introduction to Internet of Things (IoT)

Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a very few of the categorical examples where IoT is strongly established.

There are four main components used in IoT:

1. **Low-power embedded systems –**
   Less battery consumption, high performance are the inverse factors play a significant role during the design of electronic systems.
2. **Cloud computing –**
   Data collected through IoT devices is massive and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system.
3. **Availability of big data –**
   We know that IoT relies heavily on sensors, especially real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.
4. **Networking connection –**
   In order to communicate, internet connectivity is a must where each physical object is represented by an IP address. However, there are only a limited number of addresses available according to the IP naming. Due to the growing number of devices, this naming system will not be feasible anymore. Therefore, researchers are looking for another alternative naming system to represent each physical object.

There are two ways of building IoT:

1. Form a separate internetwork including only physical objects.
2. Make the Internet ever more expansive, but this requires hard-core technologies such as rigorous cloud computing and rapid big data storage (expensive).

In the near future, IoT will become broader and more complex in terms of scope. It will change the world in terms of "anytime, any place, anything in connectivity."

IoT Enablers –

- **RFIDs:** uses radio waves in order to electronically track the tags attached to each physical object.
- **Sensors:** devices that are able to detect changes in an environment (ex: motion detectors).
- **Nanotechnology:** as the name suggests, these are extremely small devices with dimensions usually less than a hundred nanometers.
- **Smart networks:** (ex: mesh topology).

Characteristics of IoT:

- Massively scalable and efficient
- IP-based addressing will no longer be suitable in the upcoming future.
- An abundance of physical objects is present that does not use IP, so IoT is made possible.

Dash

- Devices typically consume less power. When not in use, they should be automatically programmed to sleep.
- A device that is connected to another device right now may not be connected in another instant of time.
- Intermittent connectivity – IoT devices aren't always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not in use. Otherwise, connections might turn unreliable and thus prove to be inefficient.

As a quick note, IoT incorporates trillions of sensors, billions of smart systems, and millions of applications.

Application Domains of IoT:

IoT is currently found in four different popular domains:
1) Manufacturing/Industrial business - 40.2%
2) Healthcare - 30.3%
3) Security - 7.7%
4) Retail - 8.3%

Nowadays, many companies from different sectors or sectors are adopting this technology to simplify, improve, automate and control different processes. Next, we show some of the surprising practical applications of the IoT.

1. Wearables

Virtual glasses, fitness bands to monitor for example calorie expenditure and heart beats, or GPS tracking belts, are just some examples of wearable devices that we have been using for some time now. Companies such as Google, Apple, Samsung and others have developed and introduced the Internet of Things and the application thereof into our daily lives.

These are small and energy efficient devices, which are equipped with sensors, with the necessary hardware for measurements and readings, and with software to collect and organize data and information about users.

2. Health

The use of wearables or sensors connected to patients, allows doctors to monitor a patient's condition outside the hospital and in real-time. Through continuously monitoring certain metrics and automatic alerts on their vital signs, the Internet of Things helps to improve the care for patients and the prevention of lethal events in high-risk patients.

Another use is the integration of IoT technology into hospital beds, giving way to smart beds, equipped with special sensors to observe vital signs, blood pressure, oximeter and body temperature, among others.

3. Traffic monitoring

The Internet of things can be very useful in the management of vehicular traffic in large cities, contributing to the concept of smart cities.

When we use our mobile phones as sensors, which collect and share data from our vehicles through applications such as Waze or Google Maps, we are using the Internet of Things to inform us and at the same time contribute to traffic monitoring, showing the conditions of the different routes, and feeding and improving the information on the different routes to the same destination, distance, estimated time of arrival.

4. Fleet management

The installation of sensors in fleet vehicles helps to establish an effective interconnectivity between the vehicles and their managers as well as between the vehicles and their drivers. Both driver and manager/ owner can know all kinds of details about the status, operation and needs of the vehicle, just by accessing the software in charge of collecting, processing and organizing the data. Even, receive alarms in real time of maintenance incidents without having been detected by the driver.

Dash

The application of the Internet of Things to fleet management assists with geolocation (and with it the monitoring of routes and identification of the most efficient routes), performance analysis, telemetry control and fuel savings , the reduction of polluting emissions to the environment and can even provide valuable information to improve the driving of vehicles.

5. Agriculture

Smart farms are a fact. The quality of soil is crucial to produce good crops, and the Internet of Things offers farmers the possibility to access detailed knowledge and valuable information of their soil condition.

Through the implementation of IoT sensors, a significant amount of data can be obtained on the state and stages of the soil. Information such as soil moisture, level of acidity, the presence of certain nutrients, temperature and many other chemical characteristics, helps farmers control irrigation, make water use more efficient, specify the best times to start sowing, and even discover the presence of diseases in plants and soil.

6. Hospitality

The application of the IoT to the hotel industry brings with it interesting improvements in the quality of the service. With the implementation of electronic keys, which are sent directly to the mobile devices of each guest, it is possible to automate various interactions.

Thus, the location of the guests, the sending of offers or information on activities of interest, the realization of orders to the room or room service , the automatic charge of accounts to the room or the request of personal hygiene supplies, are activities that can be easily managed through integrated applications using the Internet of Things technology.

With the use of electronic keys, the check-out process is automated, disabling the operation of doors, offering information about the rooms immediately available, and even assigning housekeeping tasks to maintenance personnel.

7. Smart grid and energy saving

The progressive use of intelligent energy meters, or meters equipped with sensors, and the installation of sensors in different strategic points that go from the production plants to the different distribution points, allows better monitoring and control of the electrical network.

By establishing a bidirectional communication between the service provider company and the end user, information of enormous value can be obtained for the detection of faults, decision making and repair thereof.

It also allows offering valuable information to the end user about their consumption patterns and about the best ways to reduce or adjust their energy expenditure.

8. Water supply

A sensor, either incorporated or adjusted externally to water meters, connected to the Internet and accompanied by the necessary software , helps to collect, process and analyze data, which allows understanding the behaviour of consumers, detecting faults in the supply service, report results and offer courses of action to the company that provides the service.

Likewise, it offers final consumers the possibility of tracking their own consumption information, through a web page and in real time, even receiving automatic alerts in case of detecting consumption out of range to their average consumption record, which could indicate the presence of a leak.

9. Maintenance management

One of the areas where the application of IoT technology is most extensive is precisely maintenance management. Through the combination of sensors and software specialized in CMMS/ EAM maintenance management, a multifunctional tool is obtained whose use can be applied to a multiplicity of disciplines and practices, with the purpose of extending the useful life of physical assets, while guaranteeing asset reliability and availability.

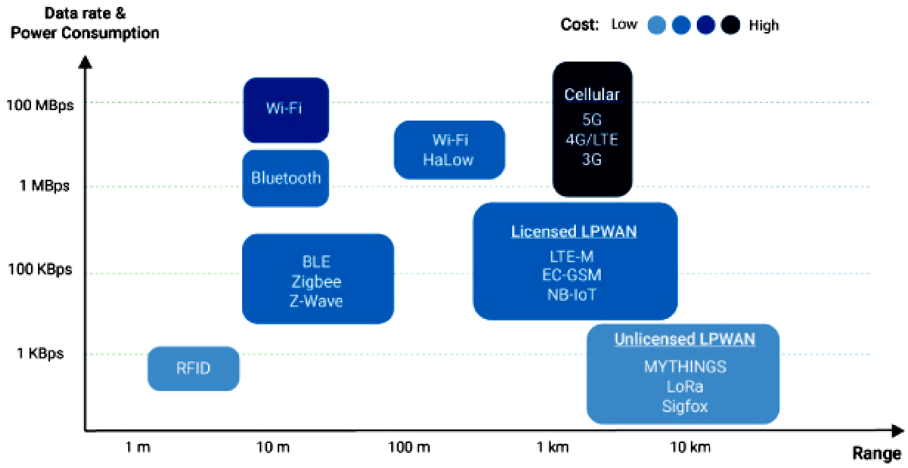
When the characteristics of the software in charge of processing and arranging the data collected by the sensors are designed to specifically address the maintenance management needs of physical assets, their application is almost unlimited.

Dash

The real-time monitoring of physical assets allows determining when a measurement is out of range and it is necessary to perform condition-based maintenance (CBM), or even applying Artificial Intelligence (AI) algorithms such as Machine Learning or Deep Learning to predict the failure before it happens.

IoT Categories

The Internet of Things (IoT) starts with connectivity, but since IoT is a widely diverse and multifaceted realm, you certainly cannot find a one-size-fits-all communication solution. Continuing our discussion on mesh and star topologies, in this article we'll walk through the six most common types of IoT wireless technologies. Each solution has its strengths and weaknesses in various network criteria and is therefore best-suited for different IoT use cases.



1. LPWANs

Low Power Wide Area Networks (LPWANs) are the new phenomenon in IoT. By providing long-range communication on small, inexpensive batteries that last for years, this family of technologies is purpose-built to support large-scale IoT networks sprawling over vast industrial and commercial campuses.

LPWANs can literally connect all types of IoT sensors – facilitating numerous applications from asset tracking, environmental monitoring and facility management to occupancy detection and consumables monitoring. Nevertheless, LPWANs can only send small blocks of data at a low rate, and therefore are better suited for use cases that don't require high bandwidth and are not time-sensitive.

Also, not all LPWANs are created equal. Today, there exist technologies operating in both the licensed (NB-IoT, LTE-M) and unlicensed (e.g. MYTHINGS, LoRa, Sigfox etc.) spectrum with varying degrees of performance in key network factors. For example, while power consumption is a major issue for cellular-based, licensed LPWANs; Quality-of-Service and scalability are main considerations when adopting unlicensed technologies. Standardization is another important factor to think of if you want to ensure reliability, security, and interoperability in the long run.

2. Cellular (3G/4G/5G)

Well-established in the consumer mobile market, cellular networks offer reliable broadband communication supporting various voice calls and video streaming applications. On the downside, they impose very high operational costs and power requirements.

Dash

While cellular networks are not viable for the majority of IoT applications powered by battery-operated sensor networks, they fit well in specific use cases such as connected cars or fleet management in transportation and logistics. For example, in-car infotainment, traffic routing, advanced driver assistance systems (ADAS) alongside fleet telematics and tracking services can all rely on the ubiquitous and high bandwidth cellular connectivity.

Cellular next-gen 5G with high-speed mobility support and ultra-low latency is positioned to be the future of autonomous vehicles and augmented reality. 5G is also expected to enable real-time video surveillance for public safety, real-time mobile delivery of medical data sets for connected health, and several time-sensitive industrial automation applications in the future.

3. Zigbee and Other Mesh Protocols

Zigbee is a short-range, low-power, wireless standard (IEEE 802.15.4), commonly deployed in mesh topology to extend coverage by relaying sensor data over multiple sensor nodes. Compared to LPWAN, Zigbee provides higher data rates, but at the same time, much less power-efficiency due to mesh configuration.

Because of their physical short-range (< 100m), Zigbee and similar mesh protocols (e.g. Z-Wave, Thread etc.) are best-suited for medium-range IoT applications with an even distribution of nodes in close proximity. Typically, Zigbee is a perfect complement to Wi-Fi for various home automation use cases like smart lighting, HVAC controls, security and energy management, etc. – leveraging home sensor networks.

Until the emergence of LPWAN, mesh networks have also been implemented in industrial contexts, supporting several remote monitoring solutions. Nevertheless, they are far from ideal for many industrial facilities that are geographically dispersed, and their theoretical scalability is often inhibited by increasingly complex network setup and management.

4. Bluetooth and BLE

Defined in the category of Wireless Personal Area Networks, Bluetooth is a short-range communication technology well-positioned in the consumer marketplace. Bluetooth Classic was originally intended for point-to-point or point-to-multipoint (up to seven slave nodes) data exchange among consumer devices. Optimized for power consumption, Bluetooth Low-Energy was later introduced to address small-scale Consumer IoT applications.

BLE-enabled devices are mostly used in conjunction with electronic devices, typically smartphones that serve as a hub for transferring data to the cloud. Nowadays, BLE is widely integrated into fitness and medical wearables (e.g. smart watches, glucose meters, pulse oximeters, etc.) as well as Smart Home devices (e.g. door locks) – whereby data is conveniently communicated to and visualized on smartphones.

The release of Bluetooth Mesh specification in 2017 aims to enable a more scalable deployment of BLE devices, particularly in retail contexts. Providing versatile indoor localization features, BLE beacon networks have been used to unlock new service innovations like in-store navigation, personalized promotions, and content delivery.

5. Wi-Fi

There is virtually no need to explain Wi-Fi, given its critical role in providing high-throughput data transfer for both enterprise and home environments. However, in the IoT space, its major limitations in coverage, scalability and power consumption make the technology much less prevalent.

Imposing high energy requirements, Wi-Fi is often not a feasible solution for large networks of battery-operated IoT sensors, especially in industrial IoT and smart building scenarios. Instead, it more pertains to connecting devices that can be conveniently connected to a power outlet like smart home gadgets and appliances, digital signages or security cameras.

Wi-Fi 6 – the newest Wi-Fi generation – brings in greatly enhanced network bandwidth (i.e. <9.6 Gbps) to improve data throughput per user in congested environments. With this, the

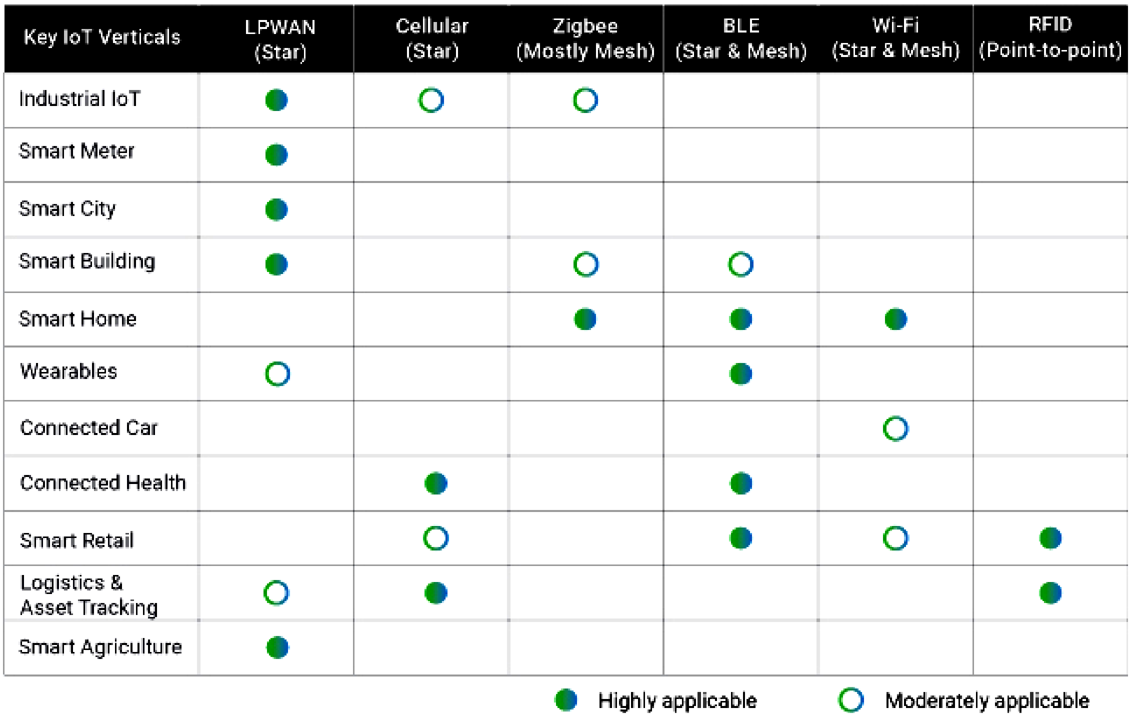
Dash

standard is poised to level up public Wi-Fi infrastructure and transform customer experience with new digital mobile services in retail and mass entertainment sectors. Also, in-car networks for infotainment and on-board diagnostics are expected to be the most game-changing use case for Wi-Fi 6. Yet, the development will likely take some more time.

6. RFID

Radio Frequency Identification (RFID) uses radio waves to transmit small amounts of data from an RFID tag to a reader within a very short distance. Till now, the technology has facilitated a major revolution in retail and logistics.

By attaching an RFID tag to all sorts of products and equipment, businesses can track their inventory and assets in real-time allowing for better stock and production planning as well as optimized supply chain management. Alongside increasing IoT adoption, RFID continues to be entrenched in the retail sector, enabling new IoT applications like smart shelves, self-checkout, and smart mirrors.



Key IoT Verticals	LPWAN (Star)	Cellular (Star)	Zigbee (Mostly Mesh)	BLE (Star & Mesh)	Wi-Fi (Star & Mesh)	RFID (Point-to-point)
Industrial IoT	●	○	○			
Smart Meter	●					
Smart City	●					
Smart Building	●		○	○		
Smart Home			●	●	●	
Wearables	○			●		
Connected Car					○	
Connected Health		●		●		
Smart Retail		○		●	○	●
Logistics & Asset Tracking	○	●				●
Smart Agriculture	●					

● Highly applicable ○ Moderately applicable

IoT Enablers

Based on several discussions on the topic of IoT with operators, there are some key enablers for IoT which are imperative to achieve success in this new area. For each of the areas of IoT, the requirement will be different from various contributors. For example, a use case may require low latency for decision making whereas another would require high throughput for live video streaming.

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 upto 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.

IoT Connectivity Layers

These Elements of IoT define the fundamentals of almost every IoT system on the globe. Still, they are divided into multiple architecture layers to further refine the overall IoT network.
These IoT layers are :

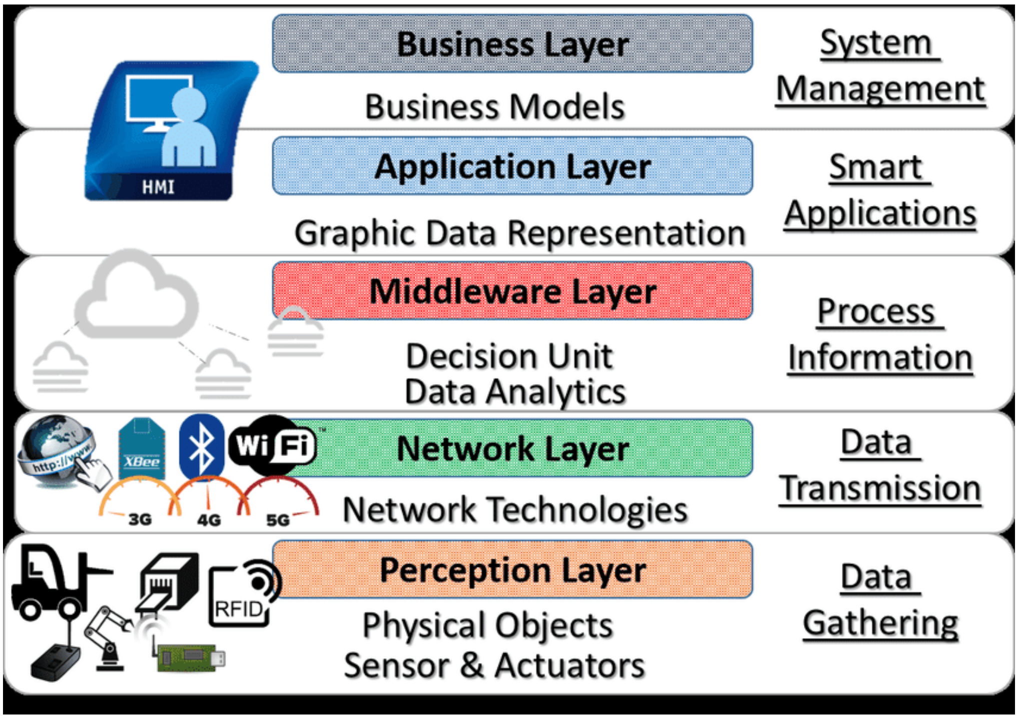
- **Perception Layer** that manages smart devices across the system.
- **Connectivity/Transport Layer** allows transferring data from the cloud to devices and vice-versa, different aspects of gateways and networks.
- **Processing Layer** that controls and manages IoT levels for streamlining data across the system.
- **Application Layer** that aids in the procedures of analytics, device control, and reporting to end-users.

With continuous changes in the IT environment, many organizations have added three additional layers to their infrastructure. Here is an IoT Block diagram showing the various stages of IoT architecture layers.

- **Business layer** that derives information and decision-making analysis from data.
- **Security Layer** that covers all aspects of protecting the whole **IoT architecture**

Dash

- **Edge Computing Layer** that works at an edge or near the device information collection.



1. Perception Layer

These IoT layers form the components of the internet physical design of IoT, acting as a medium between the digital and real world. In the IoT architecture layers, this perception layer has the main function of transforming analog signals into the digital form and vice versa. These come in a different multitude of shape and sizes with:

- **Sensors:** They are very small devices or systems built to understand and detect the change in their environment and further streamline information to their system. Generally, these sensors are quite small and take even less power to perform their task. Sensors have the unique ability to detect physical parameters such as humidity or temperature, then transforming them into electronic signals.
- **Actuators:** These represent a part of the machine that allows an electrical signal to be transformed into physical actions. These Actuators play a crucial role as components of IoT networks.
- **Machine and Devices:** They are the main devices that have actuators and sensors.

In IoT architecture, there is no limitation of location or distance between two or more devices that can be spread across the globe.

2. Connectivity Layer

Here in the second Connectivity layer, communication takes centre stage between the physical layer of devices and IoT architecture. This communication takes place via two methods;

First directly by either TCP or UDP/IP stack;

Second, gateways act as a link between Local Area Network (LAN) and Wide Area Network (WAN), thus providing a path for information to pass through multiple protocols.

So, which one element is not IoT? Several network technologies are integrated across IoT systems that include:

- **WiFi**, the most popular and versatile technique used across data-driven technologies. WiFi modems are suitable for Smart homes, personal offices, and even corporate offices for seamless communication between LAN and WAN, respectively.
- **Ethernet** represents the hardware that supports fixed or permanent devices such as video cameras, gaming consoles, and security installations.

Dash

- **Bluetooth** is another widely used technology suited mainly for communication between devices within a short range. A perfect example would be headphones that can work on small power and simultaneously share fewer data over the network.
- **NFC (Near Field Communications)** allows communication between a very short distance of 4 inches or less.
- **LPWAN (Low Power Wide Area Network),** designed and built to match the IoT usage across long distances. These low-power WAN devices can last as much as 10+ years while consuming low power throughout. However, it can send signals to give precise information over a long periodic duration. These include devices for smart buildings, smart fields, smart cities, etc.
- **ZigBee** is another advanced wireless networking technology that consumes low power and can offer small data-sharing ability. One of the unique features of IoT is its capability to handle up to 65,000 nodes in its premises. ZigBee is built with the main focus for home automation and also has shown remarkable success for medical, scientific, and industrial protocols.
- **Cellular networks** are ideally suited for communication on a global scale with more trust and reliability. For IoT, there are two broad IoT levels of the cellular network as
- LTE-M is Long Term Evolution for Machines that provides a very high-speed exchange of data and smooth direct cloud communication.
- NB-IoT as Narrowband that offers small data exchange using low-frequency channels respectively.

There are also messaging protocols present in the IoT system that allows seamless data sharing. Here is a list of top protocols present in the IoT architecture layers as of now.

- **Data Distribution Service (DDS)** represents a machine-to-machine real-time messaging framework in IoT systems.
- **Advanced Message Queuing Protocol (AMQP)** provides server protocols for servers via peer-to-peer data exchange.
- **Constrained Application Protocol (CoAP)** defines the protocols for constrained devices that use low power and low memory, such as wireless sensors.
- **Message Queue Telemetry Transport (MQTT)** represents the messaging protocol standards for low-powered devices using TCP/IP for seamless data communication.

3. Edge Layer

In the early stages, with IoT networks gaining size and numbers, latency becomes one of the major hurdles. And when multiple devices tried connecting with the main center, it clogged the system delaying the procedure. Here edge computing offered a unique solution that accelerated the growth of IoT Systems overall.

Now with the edge IoT layers, systems can process and analyze the information close to the source as much as possible. Edge has now become the standard for the 5th Generation of mobile networks (5G), offering systems to connect with more devices at a lower latency than the prevailing 4G standards. All the procedures for the IoT networks take place at the edge. Thus saving time, resources and further resulting in real-time reactions and improved performance.

4. Processing Layer

IoT systems are designed to capture, store, and process data for further requirements in this layer. In the processing layer, there are two main stages.

- **Data Accumulation**

Every device is sending millions of data streams across the IoT network. Here data comes in various forms, speeds, and sizes. Separating the essential data from these large streams is a primary concern that professionals must prioritize in this layer. Unstructured data in raw form such as photos and video streams can be quite enormous and must be done efficiently to gather intelligence factors for the business. Professionals must have a thorough understanding of the business procedures to pinpoint data requirements precisely and help procure future benefits.

- **Data Abstraction**

Once the data accumulation stage is finished, selected data is taken out from the large data for application to optimize their business procedures. Here the data abstraction follows the path as:

- Collecting all the data from all IoT and non-IoT systems (CRM, ERP, & ERM)
- Using data virtualization to make data accessible from a single location
- Managing raw data in multiple forms

Interoperability among devices and architecture plays a crucial role in the processing layer. Once data accumulation and abstraction are complete, it is easy for data analysts to use business acumen in fetching intelligence factors.

5. Application Layer

In this layer, Data is further processed and analyzed to gather business intelligence. Here IoT systems get connected with middleware or software that can understand data more precisely. Some examples of the Application layer include:

- Business decision-making software's
- Device control and monitoring services
- Analytics solutions built with Machine learning and Artificial Intelligence
- Mobile Application for further interactions

Each IoT system is built with its particular goals and objectives to match with business specifications. At present, most of the IoT Applications are working at a varying complexity and operate a multitude of technology stacks performing specific tasks for businesses.

6. Business Layer

Once IoT data is procured, it is valuable only if it applies to business planning and strategy. Every business has specific goals and objectives that it wants to accomplish by gathering intelligence from data. Business owners and stakeholders use data from past and present data to plan precisely for the future.

Today Data analysis has become the new oil for industries to enhance their productivity. Businesses are competing to get more data into their business for analysis and decision-making. Here software, CRM, and business intelligence programs have gained a lot of popularity in industries for superior performance.

7. Security Layer

With modern challenges, security has become one of the main necessities of IT architecture. Data breach, tracking malicious software, and hacking are the main challenges with Security Layer in integrating IoT systems.

- **Device Security**

The first point of security in the IoT layers starts with the devices themselves. Most of the manufacturers follow security guidelines to install in both firmware and hardware for IoT integration. Some of the essential measures are:

- Secure boot process to avoid any malicious code running on a device
- Using Trusted Platform Module (TPM) chips in combination with cryptographic keys for devices endpoint protections
- Extra physical layer to avoid direct access via the device
- Regular updates for security patches
- **Cloud Security**

Now Clouds are taking over from the traditional server for data storage and communication. Their data security is of paramount importance, especially for IoT systems. Mechanisms include multiple authorization factors and encryptions to avoid any data breach. Here the process of verifying any new device is an essential crux that must have strict regulations for device identity management.

- **Connection Security**

While transferring data across the network, it must be encrypted from an end-to-end point across the IoT system. Here messaging protocols such as DDS, AMQP, and MQTT are integrated to secure sensitive information from any breach. The use of TSL cryptographic protocol is recommended industry standard across IoT architecture for data communication.

IoT Baseline Technology

When devices were first introduced as "internet enabled," they were portrayed as convenient time savers. IoT devices have had varying levels of success, from internet refrigerators that became digital note boards to widely used webcams, home security devices, DVRs, thermostats and remote computer access systems.

As with all growing technology, the internet of things has attracted the attention of people who exploit it for their own purposes. Manufacturers, unfortunately, didn't pay much attention to IoT security when they began introducing their devices. Security experts warned of IoT vulnerabilities, and last fall, their fears were justified when a botnet of compromised IoT devices called Mirai unleashed a crippling DDoS attack against DNS provider Dyn.

One technique since the mid '90s – a boot baseline – can help with IoT security. The process is quite simple: Capture all the packets as that device powers on. Reviewing these packets gives us an understanding of what happens when an IoT device turns on and connects to the network, which can help with security investigations and in determining whether a device is infected.

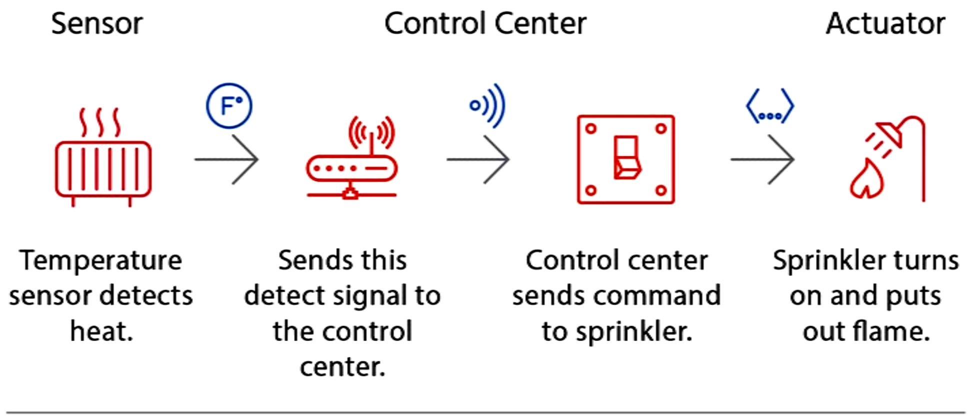
Some tips when performing a boot baseline trace are:

- For best results, start with equipment out of the box, or minimal configuration if you need to configure wireless settings.
- When capturing Ethernet-attached devices use taps, span ports or hubs.
- When capturing wireless devices, use the same technique as above, but target the Ethernet port on the access point

Sensors and Actuators in IoT

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

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


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

Sensor to **Actuator** Flow

Sensors

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

Actuators

Another type of transducer that you will encounter in many IoT systems is an actuator. In simple terms, an actuator operates in the reverse direction of a sensor. It takes an electrical input and turns it into physical action. For instance, an electric motor, a hydraulic system, and a pneumatic system are all different types of actuators.

Controller

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

IoT Variety is Key

There are many different types of sensors in an IoT system. Flow sensors, temperature sensors, voltage sensors, humidity sensors, and the list goes on. In addition, there are multiple ways to measure the same thing. For instance, a small propeller like the one you see on a weather station can measure airflow. However, this method would not work in a moving vehicle. As an alternative, vehicles can measure airflow by heating a small element and measuring the rate at which it cools.

Different applications call for different ways of measuring the same thing. At the same time, a single variable could trigger multiple actions. As a result, sensors and actuators in IoT must work together reliably.

The Importance of Accurate Sensors

Imagine that you are a bar owner and you want to measure the amount of beer coming out of one of your taps. One way you might do this is to install a sensor in line with the line that runs from the keg of beer to the tap. This sensor would most likely have a small impeller inside of it. When the beer ran through the sensor, it would cause the impeller to spin, just like the propeller on a weather station.

When the impeller spins, it will send a stream of electrical impulses to a computer. The computer will interpret the impulses to determine how much beer is flowing through. Sounds simple, right?

This is where sensors get interesting. If you look back at our description, you'll see that we never directly measured the amount of beer flowing through the sensor; we interpreted it from a stream of electrical impulses. That means that we must first figure out how to interpret it.

Sensor Calibration

To calibrate the sensor, we'd have to take a container with a known carrying capacity, say, a pint glass. Then we'd have to fill that container under a variety of conditions to determine what the electrical pulse signal looked like. Then, monitor the actuator that is responsible to turn on and off the flow on the other end.

For instance, the first pour off a new keg might tend to have more foam, which would read differently than a pour from the middle of the keg that was all beer. It's only through repeated trials and a lot of data that we gain confidence that we can interpret the data. Sensors and actuators in IoT can work together to automate processes, such as filling bottles.

The Importance of Accurate Calibration

With this correlation identified, a protocol can always assure the sensor is reading correctly. This process is calibration. Reputable manufacturers will deliver fully calibrated devices and provide instruction on how to re-calibrate to verify sensor accuracy.

The accuracy of sensed data is paramount, since you will make mission-critical decisions based on later analysis of the data, which will hold little value if the data is wrong.

IoT Components and Implementation

The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. Implementing this concept is not an easy task by any measure for many reasons including the complex nature of the different components of the ecosystem of IoT. To understand the gravity of this task, we will explain all the five components of IoT Implementation.

Components of IoT implementation

- Sensors
- Networks
- Standards
- Intelligent Analysis
- Intelligent Actions

Sensors

According to (IEEE) sensors can be defined as: An electronic device that produces electrical, optical, or digital data derived from a physical condition or event. Data produced from sensors is then electronically transformed, by another device, into information (output) that is useful in decision making done by "intelligent" devices or individuals (people).

Types of Sensors: Active Sensors & Passive Sensors

The selection of sensors greatly impacted by many factors, including:

- Purpose (Temperature, Motion, Bio…etc.)
- Accuracy
- Reliability
- Range
- Resolution
- Level of Intelligence (dealing with noise and interference)

The driving forces for using sensors in IoT today are new trends in technology that made sensors cheaper, smarter and smaller.

Challenges facing IoT sensors

- Power consumption

- Security
- Interoperability

Networks

The second step of this implantation is to transmit the signals collected by sensors over networks with all the different components of a typical network including routers, bridges in different topologies, including LAN, MAN and WAN. Connecting the different parts of networks to the sensors can be done by different technologies including Wi-Fi, Bluetooth, Low Power Wi-Fi , Wi-Max, regular Ethernet , Long Term Evolution (LTE) and the recent promising technology of Li-Fi (using light as a medium of communication between the different parts of a typical network including sensors).

The driving forces for wide spread network adoption in IoT can be summarized as follows

- High Data rate
- Low Prices of data usage
- Virtualization (X - Define Network trends)
- XaaS concept (SaaS, PaaS, and IaaS)
- IPv6 deployment

Challenges facing network implementation in IoT

- The enormous growth in number of connected devices
- Availability of networks coverage
- Security
- Power consumption

Standards

The third stage in the implementation process includes the sum of all activities of handling, processing and storing the data collected from the sensors. This aggregation increases the value of data by increasing, the scale, scope, and frequency of data available for analysis but aggregation only achieved through the use of various standards depending on the IoT application in used.

Types of Standards

Two types of standards relevant for the aggregation process; technology standards (including network protocols, communication protocols, and data-aggregation standards) and regulatory standards (related to security and privacy of data, among other issues).

Technology Standards

- Network Protocols (e.g.: Wi-Fi)
- Communications Protocols (e.g.: HTTP)
- Data aggregation standards (e.g.: Extraction, Transformation, Loading (ETL))

Regulatory Standards

Set and administrated by government agencies like FTC, for example Fair Information Practice Principles (FIPP) and US Health Insurance Portability and Accountability Act (HIPAA) just to mention few.

Challenges facing the adoptions of standards within IoT

- Standard for handling unstructured data: Structured data are stored in relational databases and queried through SQL. Unstructured data are stored in different types of noSQL databases without a standard querying approach.

- Security and privacy issues: There is a need for clear guidelines on the retention, use, and security of the data as well as metadata (the data that describe other data).
- Regulatory standards for data markets: Data brokers are companies that sell data collected from various sources. Even though data appear to be the currency of the IoT, there is lack of transparency about, who gets access to data and how those data are used to develop products or services and sold to advertisers and third parties.
- Technical skills to leverage newer aggregation tools: Companies that are keen on leveraging big-data tools often face a shortage of talent to plan, execute, and maintain systems.

Intelligent Analysis

The fourth stage in IoT implementation is extracting insight from data for analysis, Analysis is driven by cognitive technologies and the accompanying models that facilitate the use of cognitive technologies.

With advances in cognitive technologies' ability to process varied forms of information, vision and voice have also become usable. Below is a list of selected cognitive technologies that are experiencing increasing adoption and can be deployed for predictive and prescriptive analytics:

- Computer vision refers to computers' ability to identify objects, scenes, and activities in images
- Natural-language processingrefers to computers' ability to work with text the way humans do, extracting meaningfrom text or evengenerating text thatis readable.
- Speech recognition focuseson accurately transcribing human speech

Factors driving adoption intelligent analytics within the IoT

- Artificial intelligence modelscan be improved with large data sets that are more readilyavail- able than ever before, thanksto the lower storage costs.
- Growth in crowdsourcing and open- source analytics software: Cloud-based crowdsourcing services are leading to new algorithms and improvements in existing onesat an unprecedented rate.
- Real-time data processing and analysis: Analytics toolssuch as complexevent processing (CEP)enable processing and analysis of data on a real-time or a near-real-time basis, drivingtimely decision makingand action.

Challenges facing the adoptions of intelligent analytics within IoT

- Inaccurate analysis due to flaws in the data and/or model: A lack of data or presence of outliers may lead to false positives or false negatives, thus exposing various algorithmic limitations
- Legacy systems' abilityto analyze unstructured data: Legacy systems are well suited to handle structured data; unfortunately, most IoT/business interactions generate unstructured data
- Legacy systems' ability to manage real- time data: Traditional analytics software generally works on batch-oriented processing, whereinall the data are loaded in a batch and then analyzed.

Intelligent Actions

Intelligent actions can be expressed as M2M and M2H interfaces for example with all the advancement in UI and UX technologies.

Factors driving adoption of intelligent actions within the IoT

- Lower machine prices
- Improved machine functionality
- Machines "influencing" human actions through behavioral-science rationale

Dash

- Deep Learning tools

Challenges facing the adoption of intelligent actions within IoT

- Machines' actions in unpredictable situations
- Information security and privacy
- Machine interoperability
- Mean-reverting human behaviors
- Slow adoption of new technologies

The Internet of Things (IoT) is an ecosystem of ever-increasing complexity, it's the next weave of innovation that will humanize every object in our life , which is the next level to automating every object in our life . Convergence of technologies will make IoT implementation much easier and faster, which in turn will improve many aspects of our life at home and at work and in between.

Challenges for the Internet of Things

The Internet of Things (IoT) has quickly become a huge part of how people live, communicate and do business. All around the world, web-enabled devices are turning our world into a more switched-on place to live.

There are many benefits to the increased adoption of IoT technology, says Kate Began, Polycase sales and marketing manager, from the ability to monitor cargo anywhere to playing your favourite music in the shower from a waterproof Bluetooth speaker. But there are still many challenges to widespread IoT adoption and to a secure, functioning global device network.

From security challenges to the perils of high customer expectations, these five factors are big concerns for the growth and development of the Internet of Things. Overcoming them will be the key to creating true lasting productivity and prosperity through these incredible technologies.

1. Security

Ask any security expert about the biggest headaches of the 21st century and they'll likely bring up IoT devices. The reason? In cybersecurity terms, IoT devices greatly expand the "attack surface," or the amount of potential areas for cybercriminals to penetrate a secure network.

Cybercriminals don't have to crack an IoT device's plastic enclosure to access sensitive materials. They can simply finesse their way in through one of the many security vulnerabilities that are found throughout the IoT. Many IoT devices have default passwords left unchanged, unpatched software and other major security vulnerabilities.

In 2017, a casino's data was compromised by hackers who accessed its network through an IoT thermostat in one of its fish tanks. Far worse, parents have reported strangers accessing their IoT baby monitors through the internet and using them to talk to their children.

Much of the burden of fixing this problem falls upon IoT device users. Many people still don't see IoT devices as potential security threats that have to be patched, updated and protected in much the same way that smartphones and computers do.

(In fact, many people still don't protect their phones or computers well enough, either.) But, as we'll discuss below, governments often haven't moved with sufficient speed to regulate these new technologies as they become available.

2. Regulation

Another common characteristic of technological innovations is that government regulation often takes a long time to catch up with the current state of technology. With the rapid evolution that's happening every day in IoT, the government is taking its time in catching up and businesses are often left without crucial information they need to make decisions.

Dash

The lack of strong IoT regulations is a big part of why the IoT remains a severe security risk, and the problem is likely to get worse as the potential attack surface expands to include ever more crucial devices. When medical devices, cars and children's toys are all connected to the Internet, it's not hard to imagine many potential disaster scenarios unfolding in the absence of sufficient regulation.

Quality control in IoT can be particularly tricky from a regulatory perspective. With huge numbers of IoT devices now being imported from countries like China that have different standards of quality and security, many experts are calling for strong and universal security standards for IoT technology.

3. Compatibility

New waves of technology often feature a large stable of competitors jockeying for market share, and IoT is certainly no exception. This can be good news, since competition creates increased choices for consumers, but it can also create frustrating compatibility issues.

Home mesh networks are one area where compatibility trouble is looming. Bluetooth has long been the compatibility standard for IoT devices. In fact, it was named after an ancient king, Harald Bluetooth, known for unifying warring tribes. But when it comes to home automation using mesh networking, several competitors have sprung up to challenge Bluetooth's mesh network offerings, including protocols such as Zigbee and Z-Wave. It could be years before the market settles enough to crown a single universal standard for home IoT.

Continued compatibility for IoT devices also depends upon users keeping their devices updated and patched, which, as we've just discussed, can be pretty difficult. When IoT devices that have to talk to each other are running different software versions, all kinds of performance issues and security vulnerabilities can result. That's a big part of why it's so important that IoT consumers keep their devices patched and up to date.

4. Bandwidth

Connectivity is a bigger challenge to the IoT than you might expect. As the size of the IoT market grows exponentially, some experts are concerned that bandwidth-intensive IoT applications such as video streaming will soon struggle for space on the IoT's current server-client model.

That's because the server-client model uses a centralised server to authenticate and direct traffic on IoT networks. However, as more and more devices begin to connect to these networks, they often struggle to bear the load.

Thus, it's important for IoT companies to carefully examine their IoT connectivity providers and to choose one with a strong record of service and innovation. Features like intelligent switching between mobile network operators (MNOs) are particularly useful for creating a more reliable and user-friendly IoT product for your customers.

5. Customer expectations

It's often said that it's better to under-promise and over-deliver. Many IoT manufacturers have learned this the hard way, with IoT start-ups failing often and leaving bewildered customers in their wake. When customer expectations and product reality don't match, the results can be system failures, orphaned technologies and lost productivity.

With such strong competition in the IoT market, customers whose expectations aren't met won't hesitate to go elsewhere. Businesses looking to enter this competitive and innovative sector should be prepared for a market that never sits still and customers who always want a smoother and more advanced experience.

Dash