Unit -5

Birth of IoT

The term “The Internet of Things” (IoT) was coined by **Kevin Ashton** in a presentation to Proctor & Gamble in 1999. He is a co-founder of MIT’s Auto-ID Lab. He pioneered RFID (used in bar code detector) for the supply-chain management domain. He also started Zensi, a company that makes energy sensing and monitoring technology.

A quote by Kevin Ashton:- *If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best.*

We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory.

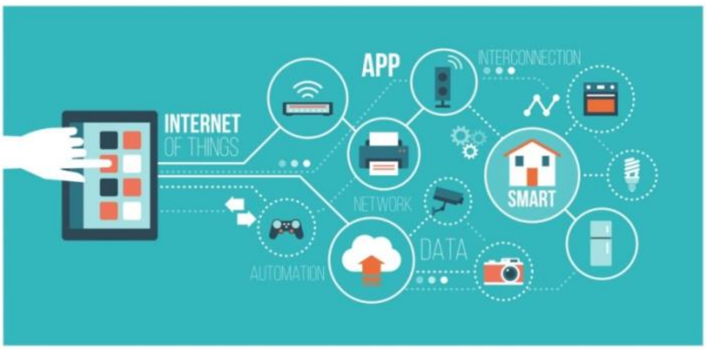
The above Kevin’s quote would have given you an idea about the ideologies behind the development of IoT. Let’s now try to further simplify this term and understand IoT fundamentally. After this, we will be moving forward and looking towards the benefits of IoT.

History of IoT

- 1970- The actual idea of connected devices was proposed
- 1990- John Romkey created a toaster which could be turned on/off over the Internet
- 1995- Siemens introduced the first cellular module built for M2M
- 1999- The term "Internet of Things" was used by Kevin Ashton during his work at P&G which became widely accepted
- 2004 - The term was mentioned in famous publications like the Guardian, Boston Globe, and Scientific American
- 2005-UN's International Telecommunications Union (ITU) published its first report on this topic.
- 2008- The Internet of Things was born
- 2011- Gartner, the market research company, include "The Internet of Things" technology in their research

Introduction to IoT

The ‘Thing’ in IoT can be any device with any kind of built-in-sensors with the ability to collect and transfer data over a network without manual intervention. The embedded technology in the object helps them to interact with internal states and the external environment, which in turn helps in decisions making process.



<u>What is IoT?</u>

IoT is a concept that connects all the devices to the internet and let them communicate with each other over the internet. IoT is a giant network of connected devices – all of which gather and share data about how they are used and the environments in which they are operated.

By doing so, each of your devices will be learning from the experience of other devices, as humans do. IoT is trying to expand the interdependence in human- i.e *interact*, *contribute* and c*ollaborate* to things. I know this sounds a bit complicated, let's understand this with an example.

A developer submits the application with a document containing the standards, logic, errors & exceptions handled by him to the tester. Again, if there are any issues Tester communicates it back to the Developer. It takes multiple iterations & in this manner a smart application is created.

Similarly, a room temperature sensor gathers the data and send it across the network, which is then used by multiple device sensors to adjust their temperatures accordingly. For example, refrigerator's sensor can gather the data regarding the outside temperature and accordingly adjust the refrigerator's temperature. Similarly, your air conditioners can also adjust its temperature accordingly. This is how devices can interact, contribute & collaborate.

Connecting multiple devices

Benefits of IoT

Since IoT allows devices to be controlled remotely across the internet, thus it created opportunities to directly connect & integrate the physical world to the computer-based systems using sensors and internet. The interconnection of these multiple embedded devices will be resulting in automation in nearly all fields and also enabling advanced applications. This is resulting in improved accuracy, efficiency and economic benefit with reduced human intervention. It encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. The major benefits of IoT are:

- ***Improved Customer Engagement*** – IoT improves customer experience by automating the action. For e.g. any issue in the car will be automatically detected by the sensors. The driver, as well as the manufacturer, will be notified about it. Till the time driver reaches the service station, the manufacturer will make sure that the faulty part is available at the service station.
- ***Technical Optimization*** – IoT has helped a lot in improving technologies and making them better. The manufacturer can collect data from different car sensors and analyze them to improve their design and make them much more efficient.
- ***Reduced Waste*** – Our current insights are superficial, but IoT provides real-time information leading to effective decision making & management of resources. For example, if a manufacturer finds fault in multiple engines, he can track the manufacturing plant of those engines and can rectify the issue with manufacturing belt.

Nowadays, we are surrounded by lots of IoT enabled devices which are continuously emitting data and communicating through multiple devices. Moving ahead, let’s discuss the required hardware for building an IoT application. We will also look at the IoT devices which we are using in our day to day life.

IoT Hardware

Now you would be wondering what is the required hardware for preparing an IoT solution. The answer to this question is, you’ll first require sensors that will sense the environment, then you require a remote dashboard to monitor your output and display it in a clearer & conceivable form. At last, you will require a device with the capability of serving & routing. The key task of the system would be detecting specific conditions and taking actions accordingly. One thing to keep in mind is securing the communication between the devices and the dashboard.

Some of the common sensors that you are surrounded by are accelerometers, temperature sensors, magnetometers, proximity sensors, gyroscopes, image sensors, acoustic sensors, light sensors, pressure sensors, gas RFID sensors, humidity sensors & micro flow sensors.

Nowadays we also have many wearable devices like smartwatches, shoes & 3D glasses. This is the best example of a smart solution. 3D glasses adjust television’s brightness and contrast according to your eye and your smartwatches keeps track of your daily activities and fitness.

But I feel the most important device which has tremendously contributed to IoT are the cell phones. Mobile apps have immensely contributed to revolutionizing the technology world. Cell phones are already encased with applications and sensors that reveals lots of information about its user. It has Geo-location information, it can sense and trace light condition, the orientation of your device and a lot more information. It also comes with multiple connectivity options like Wi-Fi, Bluetooth and cellular that helps them to communicate with other devices. Thus, due to these default qualities of cell phones, it is the core of the IoT ecosystem. Today, Smartphone can interact with smartwatch and fitness band to further ease and enhance the user experience.

IoT uses multiple technologies and protocols to communicate with devices based on the requirements. The major technologies & protocols are Bluetooth, wireless, NFC, RFID, radio protocols and WiFi-Direct.

IoT applications are flourishing across all industries & market. The IoT has a multitude of expansion over various industries. It spans over all groups of users, from those who are trying to reduce & conserve energy in their home to large organizations who want to improve their business operations. IoT has not only proved itself useful in optimizing critical applications in many organisations, but also have boosted the concept of advanced automation which we have imagined a decade before. Let’s understand the capabilities of IoT across different industries and look how they are revolutionizing them.

IoT Across Various Domains

Energy Applications: The energy rates have raised to a great instinct. Individuals and organisations, both are searching ways to reduce and control the consumption. IoT provides a way to not only monitor the energy usage at the appliance-level but also at the house-level, grid level or could be at the distribution level. Smart Meters & Smart Grid are used to monitor energy consumption. It also detects threats to the system performance and stability, which protect appliances from downtime and damages.

Healthcare Application: Smart watches and fitness devices have changed the frequency of health monitoring. People can monitor their own health at regular intervals. Not only this, now if a patient is coming to the hospital by ambulance, by the time he or she reaches the hospital his health report is diagnosed by doctors and the hospital quickly starts the treatment. The data gathered from multiple healthcare applications are now collected and used to analyze different disease and find its cure.

Education: IoT provides education aids which helps in fulfilling the gaps in the education industry. It not only improves the quality of education but also optimizes the cost and improves the management by taking into consideration students response and performance.

Government: Governments are trying to build smart cities using IoT solutions. IoT enhances armed force systems and services. It provides better security across the borders through inexpensive & high-performance devices. IoT helps government agencies to monitor data in real-time and improve their services like healthcare, transportation, education etc.

Air and Water Pollution: Through various sensors, we can detect the pollution in the air and water by frequent sampling. This helps in preventing substantial contamination and related disasters. IoT allows operations to minimize the human intervention in farming analysis and monitoring. Systems automatically detect changes in crops, soil, environment, and more.

Transportation: IoT has changed the transportation sector. Now, we have self-driving cars with sensors, traffic lights that can sense the traffic and switch automatically, parking assistance, giving us the location of free parking space etc. Also, various sensors in your vehicle indicate you about the current status of your vehicle, so that you don't face any issues while travelling.

Marketing your product: Using IoT, organizations can better analyze & respond to customer preferences by delivering relevant content and solutions. It helps in improving business strategies in the real-time.

Now that we are aware of the powerful IoT solutions that have been astoundingly impacting various domains, let's take a deep dive and understand Raspberry Pi, which is commonly used to prepare IoT solutions. After understanding Raspberry Pi we will be creating an IoT application.

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."

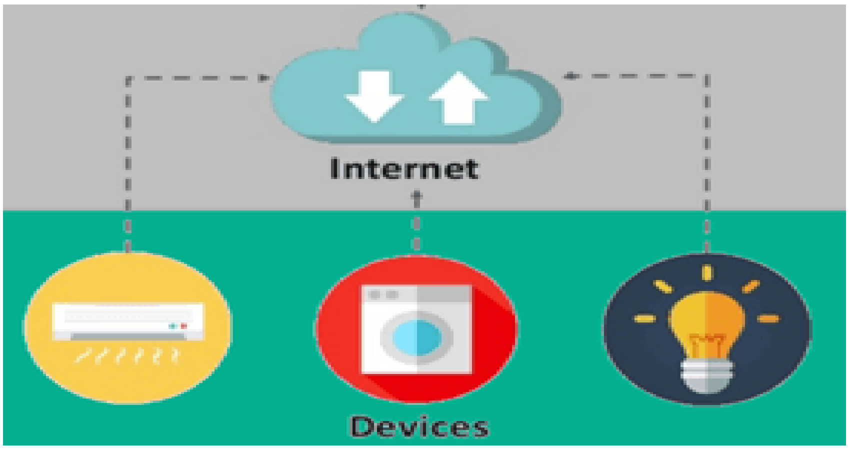
IoT Enablers –

- 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.
- 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.

How IoT works?



- The entire IoT process starts with the devices themselves like smartphones, smartwatches, electronic appliances like TV, Washing Machine which helps you to communicate with the IoT platform.
- Now in this IoT tutorial, we will learn about four fundamental components of an IoT system:
- **1) Sensors/Devices:** Sensors or devices are a key component that helps you to collect live data from the surrounding environment. All this data may have various levels of complexities. It could be a simple temperature monitoring sensor, or it may be in the form of the video feed.
- A device may have various types of sensors which performs multiple tasks **apart** from sensing. Example, A mobile phone is a device which has multiple sensors like GPS, camera but your smartphone is not able to sense these things.
- **2) Connectivity:** All the collected data is sent to a cloud infrastructure. The sensors should be connected to the cloud using various mediums of communications. These

communication mediums include mobile or satellite networks, Bluetooth, WI-FI, WAN, etc.

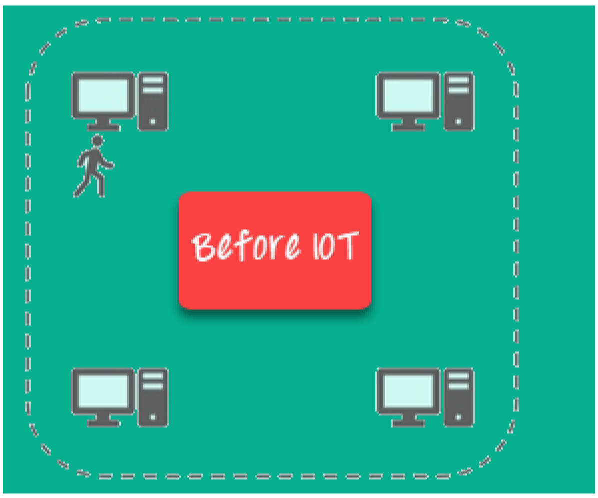
- **3) Data Processing:** Once that data is collected, and it gets to the cloud, the software performs processing on the gathered data. This process can be just checking the temperature, reading on devices like AC or heaters. However, it can sometimes also be very complex like identifying objects, using computer vision on video.
- **4)User Interface:** The information needs to be available to the end-user in some way which can be achieved by triggering alarms on their phones or sending them notification through email or text message. The user sometimes might need an interface which actively checks their IoT system. For example, the user has a camera installed in his home. He wants to access video recording and all the feeds with the help of a web server.
- However, it's not always one-way communication. Depending on the IoT application and complexity of the system, the user may also be able to perform an action which may create cascading effects.
- For example, if a user detects any changes in the temperature of the refrigerator, with the help of IoT technology the user should able to adjust the temperature with the help of their mobile phone.

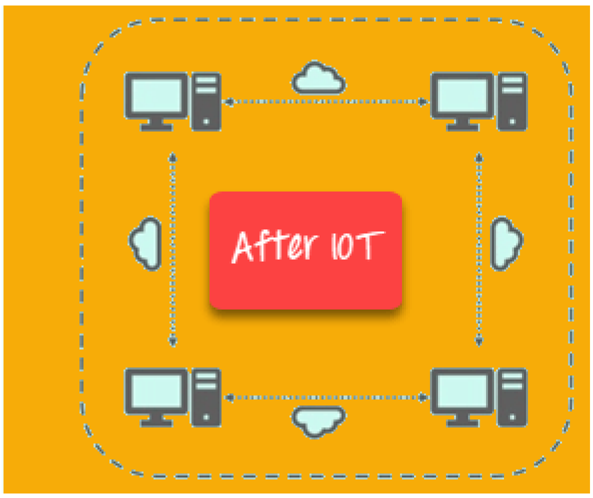
Challenges of Internet of Things (IoT)

At present IoT is faced with many challenges, such as:

- Insufficient testing and updating
- Concern regarding data security and privacy
- Software complexity
- Data volumes and interpretation
- Integration with AI and automation
- Devices require a constant power supply which is difficult
- Interaction and short-range communication

Advantages of IoT





Key benefits of IoT technology are as follows:

- **Technical Optimization:** IoT technology helps a lot in improving technologies and making them better. Example, with IoT, a manufacturer is able to collect data from various car sensors. The manufacturer analyzes them to improve its design and make them more efficient.
- **Improved Data Collection:** Traditional data collection has its limitations and its design for passive use. IoT facilitates immediate action on data.

- **Reduced Waste:** IoT offers real-time information leading to effective decision making & management of resources. For example, if a manufacturer finds an issue in multiple car engines, he can track the manufacturing plan of those engines and solves this issue with the manufacturing belt.
- **Improved Customer Engagement:** IoT allows you to improve customer experience by detecting problems and improving the process.

Disadvantages IoT

- **Security:** IoT technology creates an ecosystem of connected devices. However, during this process, the system may offer little authentication control despite sufficient security measures.
- **Privacy:** The use of IoT, exposes a substantial amount of personal data, in extreme detail, without the user's active participation. This creates lots of privacy issues.
- **Flexibility:** There is a huge concern regarding the flexibility of an IoT system. It is mainly regarding integrating with another system as there are many diverse systems involved in the process.
- **Complexity:** The design of the IoT system is also quite complicated. Moreover, it's deployment and maintenance also not very easy.
- **Compliance:** IoT has its own set of rules and regulations. However, because of its complexity, the task of compliance is quite challenging.

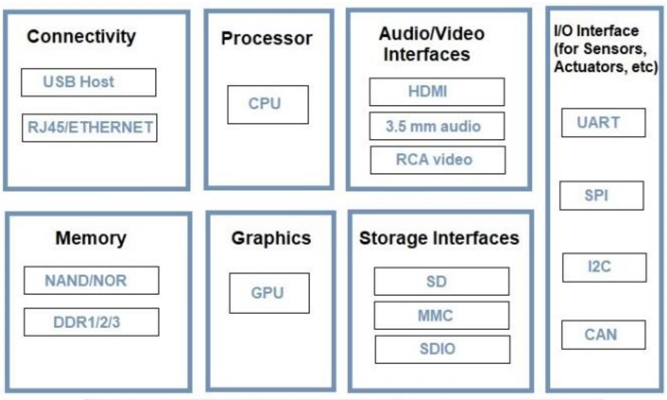
Physical and Logical Design of IoT

Physical 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.



Generic Block Diagram of IoT Devices

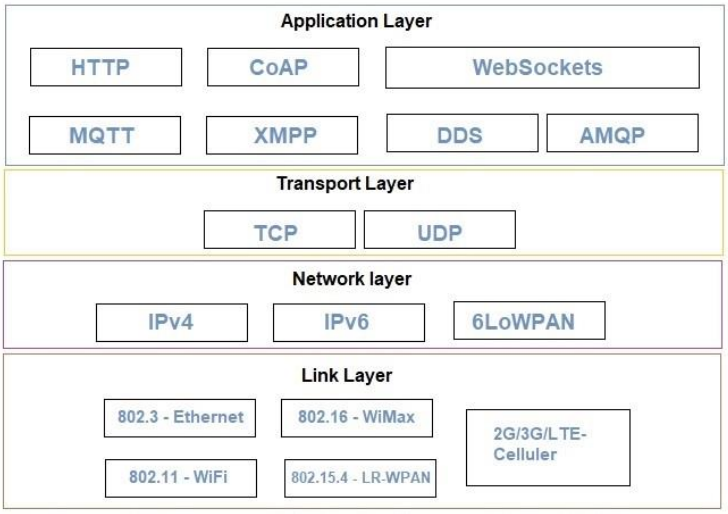
For example, Temperature data generated by a Temperature Sensor in Home or other place, when processed can help in determining temperature and take action according to users.

Above picture, shows a generic block diagram of IoT device. It may consist of several interfaces for connections to other devices. IoT Device has I/O interface for Sensors, Similarly for Internet connectivity, Storage and Audio/Video.

IoT Device collect data from on-board or attached Sensors and Sensed data communicated either to other device or Cloud based sever. Today many cloud servers available for especially IoT System. These Platfrom known as IoT Platform. Actually these cloud especially design for IoT purpose. So here we can analysis and processed data easily.

How it works ? For example if relay switch connected to an IoT device can turn On/Off an appliance on the commands sent to the IoT device over the Internet.

IoT Protocols
IoT protcols help to establish Communication between IoT Device (Node Device) and Cloud based Server over the Internet. It help to sent commands to IoT Device and received data from an IoT device over the Internet. An image is given below. By this image you can understand which protocols used.



Link Layer
Link layer protocols determine how data is physically sent over the network’s physical layer or medium (Coxial calbe or other or radio wave). Link Layer determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached (eg. coxial cable).

Here we explain some Link Layer Protocols:

802.3 – Ethernet : Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s by IEEE 802.3 standard. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.
For more information visit Tutorialspoint https://www.tutorialspoint.com/ieee-802-3-and-ethernet) (Source)
802.11 – WiFi : IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 60 GHz frequency bands.
For more info visit wikipedia https://en.wikipedia.org/wiki/IEEE_802.11 (Source)
802.16 – Wi-Max : The standard for WiMAX technology is a standard for Wireless Metropolitan Area Networks (WMANs) that has been developed by working group number 16 of IEEE 802, specializing in point-to-multipoint broadband wireless access. Initially 802.16a was developed and launched, but now it has been further refined. 802.16d or 802.16-2004 was released as a refined version of the 802.16a standard aimed at fixed applications. Another

version of the standard, 802.16e or 802.16-2005 was also released and aimed at the roaming and mobile markets.
For more information visit this https://www.electronics-notes.com/articles/connectivity/wimax/what-is-wimax-802-16-technology-basics.php (Source)
802.15.4 -LR-WPAN : A collection of standards for Low-rate wireless personal area network. The IEEE's 802.15.4 standard defines the MAC and PHY layer used by, but not limited to, networking specifications such as Zigbee®, 6LoWPAN, Thread, WiSUN and MiWi™ protocols. The standards provide low-cost and low-speed communication for power constrained devices.
2G/3G/4G- Mobile Communication : These are different types of telecommunication generations. IoT devices are based on these standards can communicate over the celluer networks.

Network Layer
Responsible for sending of IP datagrams from the source network to the destination network. Network layer performs the host addressing and packet routing. We used IPv4 and IPv6 for Host identification. IPv4 and IPv6 are hierarchical IP addrssing schemes.

IPv4 :
An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.
Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was standardized in 1998. IPv6 deployment has been ongoing since the mid-2000s.
For for more detail https://en.wikipedia.org/wiki/IP_address (Source)

IPv6 : Internet Protocol version 6 (**IPv6**) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4. In December 1998, IPv6 became a Draft Standard for the IETF, who subsequently ratified it as an Internet Standard on 14 July 2017. IPv6 uses a 128-bit address, theoretically allowing 2^{128}, or approximately 3.4×10^{38} addresses. *Source – wikipedia*
for more detail https://en.wikipedia.org/wiki/IPv6

6LoWPAN : 6LoWPAN is an acronym of *IPv6 over Low-Power Wireless Personal Area Networks*.6LoWPAN is the name of a concluded working group in the Internet area of the IETF. 6LoWPAN is a somewhat contorted acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN, therefore, allows for the smallest devices with limited processing ability to transmit information wirelessly using an internet protocol. 6LoWPAN can communicate with 802.15.4 devices as well as other types of devices on an IP network link like WiFi.
For more deatils visit this https://iotbyhvm.ooo/6lowpan-zigbee/

Transport Layer
This layer provides functions such as error control, segmentation, flow control and congestion control. So this layer protocols provide end-to-end message transfer capability independent of the underlying network.

TCP : TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to

each other. Together, TCP and IP are the basic rules defining the Internet. The Internet Engineering Task Force (IETF) defines TCP in the Request for Comment (RFC) standards document number 793.
Source – For more detail : https://searchnetworking.techtarget.com/definition/TCP

UDP : User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer. Read more here *https://www.geeksforgeeks.org/user-datagram-protocol-udp/*

Application Layer
Application layer protocols define how the applications interface with the lower layer protocols to send over ther network.

HTTP : *Hypertext Transfer Protocol (HTTP)* is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes. HTTP follows a classical client-server model, with a client opening a connection to make a request, then waiting until it receives a response. HTTP is a stateless protocol, meaning that the server does not keep any data (state) between two requests. Though often based on a TCP/IP layer, it can be used on any reliable transport layer, that is, a protocol that doesn't lose messages silently like UDP does. RUDP — the reliable update of UDP — is a suitable alternative.
CoAP : CoAP-Constrained Application Protocol is a specialized Internet Application Protocol for constrained devices, as defined in RFC 7252. It enables devices to communicate over the Internet. It is defined as Contrained Application Protocol, and is a protocol intended to be used in very simple hardware. The protocol is especially targeted for constrained hardware such as 8-bits microcontrollers, low power sensors and similar devices that can't run on HTTP or TLS. It is a simplification of the HTTP protocol running on UDP, that helps save bandwidth. It is designed for use between devices on the same constrained network (e.g., low-power, lossy networks), between devices and general nodes on the Internet, and between devices on different constrained networks both joined by an internet. CoAP is also being used via other mechanisms, such as SMS on mobile communication networks.
Read more … https://iotbyhvm.ooo/what-is-coap-protocol/

WebSocket : The WebSocket Protocol enables two-way communication between a client running untrusted code in a controlled environment to a remote host that has opted-in to communications from that code. The security model used for this is the origin-based security model commonly used by web browsers. The protocol consists of an opening handshake followed by basic message framing, layered over TCP. The goal of this technology is to provide a mechanism for browser-based applications that need two-way communication with servers that does not rely on opening multiple HTTP connections (e.g., using XMLHttpRequest or <iframe>s and long polling).

MQTT :
MQTT is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport and useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium. For example, it has been used in sensors communicating to a broker via satellite link, over occasional dial-up connections with healthcare providers, and in a range of home automation and small device scenarios.

MQTT protocol runs on top of the TCP/IP networking stack. When clients connect and publish/subscribe, MQTT has different message types that help with the handshaking of that process. The MQTT header is two bytes and first byte is constant. In the first byte, you specify the type of message being sent as well as the QoS level, retain, and DUP (duplication) flags. The second byte is the remaining length field.

Read my article for more information https://iotbyhvm.ooo/mqtt/
XMPP : Extensible Messaging and Presence Protocol (**XMPP**) is a communication protocol for message-oriented middleware based on XML (Extensible Markup Language). It enables the near-real-time exchange of structured yet extensible data between any two or more network entities. Originally named **Jabber**, the protocol was developed by the eponymous open-source community in 1999 for near real-time instant messaging (IM), presence information, and contact list maintenance. Designed to be extensible, the protocol has been used also for publish-subscribe systems, signalling for VoIP, video, file transfer, gaming, the Internet of Things (IoT) applications such as the smart grid, and social networking services.

DDS : The Data Distribution Service (DDS™) is a middleware protocol and API standard for data-centric connectivity from the Object Management Group® (OMG®). It integrates the components of a system together, providing low-latency data connectivity, extreme reliability, and a scalable architecture that business and mission-critical Internet of Things (IoT) applications need.
In a distributed system, middleware is the software layer that lies between the operating system and applications. It enables the various components of a system to more easily communicate and share data. It simplifies the development of distributed systems by letting software developers focus on the specific purpose of their applications rather than the mechanics of passing information between applications and systems.

Source – https://www.dds-foundation.org/what-is-dds-3/
AMQP : The AMQP – IoT protocols consist of a hard and fast of components that route and save messages within a broker carrier, with a set of policies for wiring the components together. The AMQP protocol enables patron programs to talk to the dealer and engage with the AMQP model. AMQP has the following three additives, which might link into processing chains in the server to create the favored capability.

- **Exchange:** Receives messages from publisher primarily based programs and routes them to 'message queues'.
- **Message Queue:** Stores messages until they may thoroughly process via the eating client software.
- **Binding:** States the connection between the message queue and the change.

Logical Design of IoT
In this article we discuss Logical design of Internet of things. Logical design of IoT system refers to an abstract representation of the entities & processes without going into the low-level specifies of the implementation. For understanding Logical Design of IoT, we describes given below terms.

- IoT Functional Blocks
- IoT Communication Models
- IoT Communication APIs

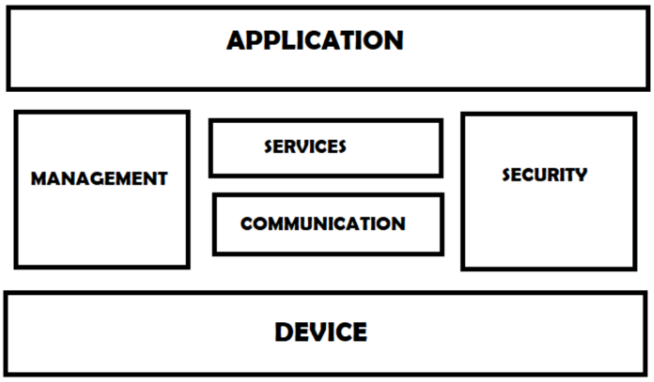
IoT Functional Blocks
An IoT system comprises of a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication and management.

functional blocks are:

Device: An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.

Communication: Handles the communication for the IoT system.
Services: services for device monitoring, device control service, data publishing services and services for device discovery.
Management: this blocks provides various functions to govern the IoT system.
Security: this block secures the IoT system and by providing functions such as authentication , authorization, message and content integrity, and data security.

Application: This is an interface that the users can use to control and monitor various aspects of the IoT system. Application also allow users to view the system status and view or analyze the processed data.



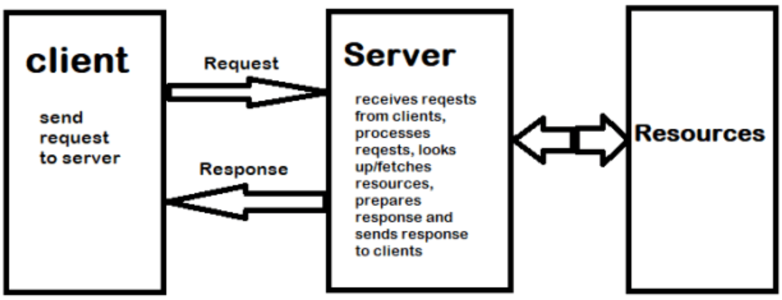
IoT Communication Models

Request-Response Model

Request-response model is communication model in which the client sends requests to the server and the server responds to the requests. When the server receives a request, it decides how to respond, fetches the data, retrieves resource representation, prepares the response, and then sends the response to the client. Request-response is a stateless communication model and each request-response pair is independent of others.

HTTP works as a request-response protocol between a client and server. A web browser may be the client, and an application on a computer that hosts a web site may be the server.

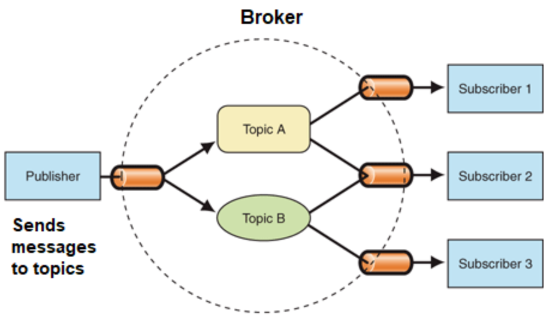
Example: A client (browser) submits an HTTP request to the server; then the server returns a response to the client. The response contains status information about the request and may also contain the requested content.



Request-Response Communication Model

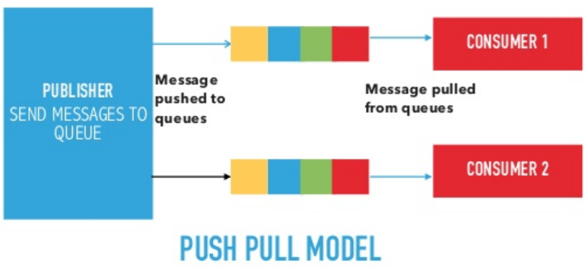
Publish-Subscribe Model

Publish-Subscribe is a communication model that involves publishers, brokers and consumers. Publishers are the source of data. Publishers send the data to the topics which are managed by the broker. Publishers are not aware of the consumers. Consumers subscribe to the topics which are managed by the broker. When the broker receive data for a topic from the publisher, it sends the data to all the subscribed consumers.



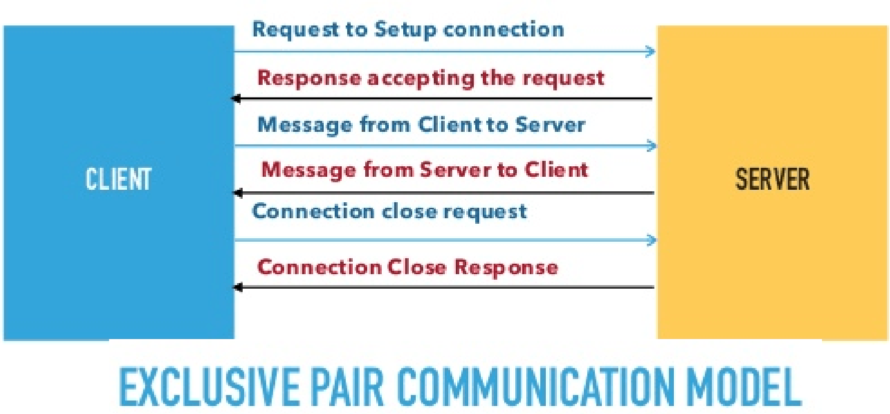
Push-Pull Model

Push-Pull is a communication model in which the data producers push the data to queues and the consumers Pull the data from the Queues. Producers do not need to be aware of the consumers. Queues help in decoupling the messaging between the Producers and Consumers. Queues also act as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate rate at which the consumer pull data.



Exclusive Pair Model

Exclusive Pair is a bidirectional, fully duplex communication model that uses a persistent connection between the client and server. Connection is setup it remains open until the client sends a request to close the connection. Client and server can send messages to each other after connection setup. Exclusive pair is stateful communication model and the server is aware of all the open connections.



IoT Communication APIs

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

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

REST-based Communication APIs

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

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

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

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

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

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

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

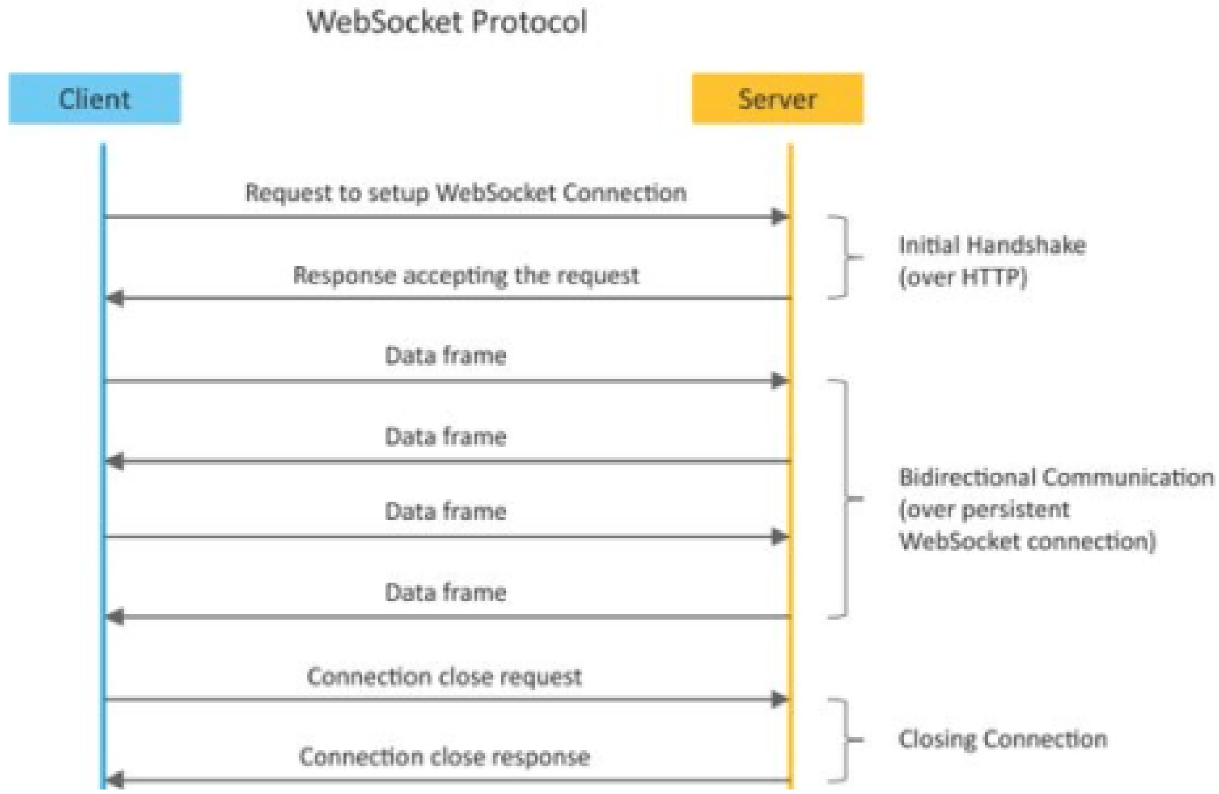
A RESTful web service is a " Web API " implemented using HTTP and REST principles. REST is most popular IoT Communication APIs.

Uniform Resource Identifier (URI)	**GET**	**PUT**	**PATCH**	**POST**	**DELETE**
Collection, such as https://api.example.com/resources/	*List* the URIs and perhaps other details of the collection's members.	*Replace* the entire collection with another collection.	Not generally used	*Create* a new entry in the collection. The new entry's URI is assigned automatically and is usually	*Delete* the entire collection.

				returned by the operation.	
Element, such as https://api.example.com/resources/item5	*Retrieve* a representation of the addressed member of the collection, expressed in an appropriate Internet media type.	*Replace* the addressed member of the collection, or if it does not exist, create it.	*Update* the addressed member of the collection.	Not generally used. Treat the addressed member as a collection in its own right and create a new entry within it.	*Delete* the addressed member of the collection.
HTTP methods					

WebSocket based communication API

Websocket APIs allow bi-directional, full duplex communication between clients and servers. Websocket APIs follow the exclusive pair communication model. Unlike request-response model such as REST, the WebSocket APIs allow full duplex communication and do not require new coonection to be setup for each message to be sent. Websocket communication begins with a connection setup request sent by the client to the server. The request (called websocket handshake) is sent over HTTP and the server interprets it is an upgrade request. If the server supports websocket protocol, the server responds to the websocket handshake response. After the connection setup client and server can send data/mesages to each other in full duplex mode. Websocket API reduce the network traffic and letency as there is no overhead for connection setup and termination requests for each message. Websocket suitable for IoT applications that have low latency or high throughput requirements. So Web socket is most suitable IoT Communication APIs for IoT System.



IoT functional blocks
An IoT system is comprised of a number of functional blocks to facilitate various utilities to the system such as, sensing, identification, actuation, communication, and management (Sebastian and Ray, 2015a). Fig. 1. presents these functional blocks as described below.

- Device: An IoT system is based on devices that provide sensing, actuation, control, and monitoring activities. IoT devices can exchange data with other connected devices and application, or collect data from other devices and process the data either locally or send the data to centralized servers or cloud based applications back-ends for processing the data, or perform some tasks locally and other tasks within IoT infrastructure based on temporal and space constraints (i.e. memory, processing capabilities, communication latencies, and speeds, and deadlines). An IoT device may consist of several interfaces for communications to other devices, both wired and wireless. These include (i) I/O interfaces for sensors, (ii) interfaces for Internet connectivity, (iii) memory and storage interfaces, and (iv) audio/video interfaces. IoT devices can also be of varied types, for instance, wearable sensors, smart watches, LED lights, automobiles and industrial machines. Almost all IoT devices generate data in some form of the other which when processed by data analytics systems generate leads to useful information to guide further actions locally or remotely, For instance, sensor data generated by a soil moisture monitoring device in a garden, when processed can help in determining the optimum watering schedules

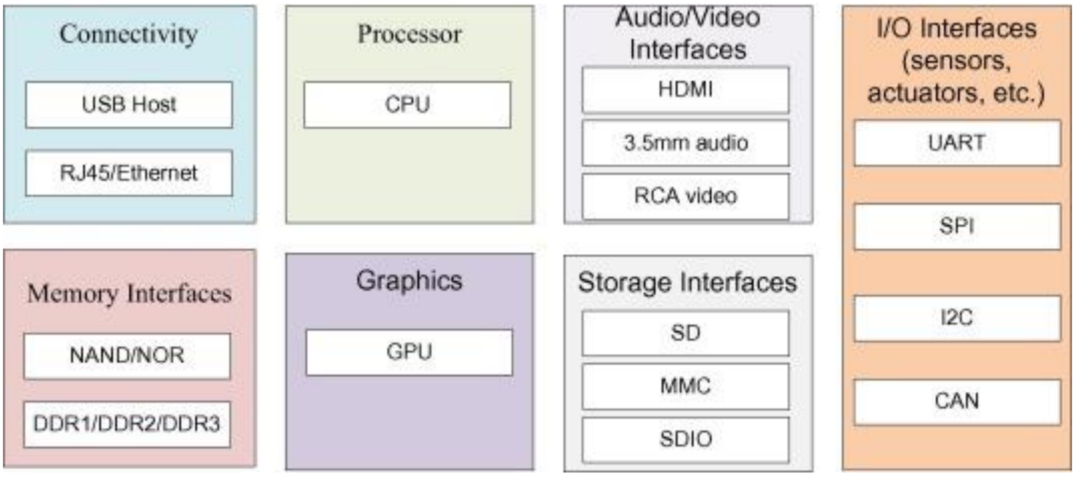
- Communication: The communication block performs the communication between devices and remote servers. IoT communication protocols generally work in data link layer, network layer, transport layer, and application layer.

- Services: An IoT system serves various types of functions such as services for device modeling, device control, data publishing, data analytics, and device discovery.

- Management: Management block provides different functions to govern an IoT system to seek the underlying governance of IoT system.

- Security: Security functional block secures the IoT system by providing functions such as, authentication, authorization, privacy, message integrity, content integrity, and data security.

- Application: Application layer is the most important in terms of users as it acts as an interface that provides necessary modules to control, and monitor various aspects of the IoT system. Applications allow users to visualize, and analyze the system status at present stage of action, sometimes prediction of futuristic prospects.



IoT home automation – Smart homes and Internet of Things

Before proceeding any further, let's take a closer look at IoT. 'Internet of Things' is an umbrella term used for all technologies that enable the connection of a device to the Internet.

Such systems depend on the collection of data. The data is then used for monitoring, controlling and transferring information to other devices via the internet. This allows specific actions to be automatically activated whenever certain situations arise. In a simple example, consider a smart kettle. The kettle can be programmed to automatically turn off once it reaches a specific temperature. It might also send a notification to the user on the same.

Now apply the same concept to the entire home and all the devices present. That is a smart home powered by IoT. Instead of manually going up to the device and taking action, those actions can be taken at the press of a button. **These days, most smart IoT home automation devices allow you to control them via an app or even via voice commands.**

Now imagine if you did not even need to undertake such actions. In other words, the smart home will know when to take certain actions and automatically take them. This is where the future of home automation and IoT lies.

Here are some possible scenarios that we may see in future.

Lighting

These days, smart lighting is all the rage. They can be scheduled to turn on/off and change their intensity. However, in future, it is possible for this to be taken a step further. With IoT enabled across the home, the lights can respond to other actions you take.

For example, the lights can respond to your home cinema. They can turn off or dim whenever you start watching a movie. Going further, they may even react to the type of movie. For example, they can turn off completely if the lights sense that you are watching a horror movie, giving you the proper atmosphere.

Doors

In the future, doors can become smarter as well. Imagine them opening only when you enter or close. This may be made possible via a smart device or facial recognition. This can be taken to the next step by getting the rest of the house take actions in tandem with your entry.

For example, the lights can turn on as soon you as enter through the door. Alternatively, if you are leaving, they can turn off.

Windows

Windows can become smarter as well. Imagine them automatically open the shutters when the sun rises and close at sunset. You may even be able to program them to close automatically when it rains. Consider the previous example of a home movie. Your curtains can lower whenever you are watching a movie.

Thermostat

These days, you can control your home thermostat remotely via apps. In the future, you may not even need to do that. The thermostat will be able to recognise if you are nearing your home. It will then check the room and external temperature and set the right one for you. It may even recognise when you are taking certain actions and adjust accordingly such as when you are showering or exercising

.

Gardens

Even your gardens can become smarter in the future with IoT. You will be able to place IoT sensors in the garden. If these sensors detect dryness in the soil, they can trigger the irrigation system. Robotic lawnmowers can be automatically deployed if the grass exceeds a certain height.

Home routines

It is already possible for much of the home to be connected with smart devices. There are smart sockets that automatically turn on/off devices. Smart alarms can play music when you wake up or even tell you the news. Voice assistants can even run entire routines where the lights, home appliances, thermostat, alarms and other devices are controlled.

Going forward, this will be extended throughout the home. Consider the morning routine. The shutters will open right before you wake up to help you get rid of that grogginess. Even before you wake up, the coffee maker will start getting your morning cup ready. The bathroom will get the water heated for your shower. Your stereo will start playing some morning tunes as you have your morning cup. Your TV will also turn on and show you your preferred news channel. Of course, the thermostat will adjust to a comfortable temperature.

Of course, all of these are not going to happen overnight. There are a few barriers to widespread adoption of IoT-enabled smart homes, the primary of which is cost. Privacy is another major concern. Then there are the current technological limitations that create difficulties in a seamless connection between multipole IoT devices.

IoT Applications

- IoT solutions are widely used in numerous companies across industries. Some most common IoT applications are given below:

Application type	**Description**
Smart Thermostats	Helps you to save resource on heating bills by knowing your usage patterns.
Connected Cars	IoT helps automobile companies handle billing, parking, insurance, and other related stuff automatically.
Activity Trackers	Helps you to capture heart rate pattern, calorie expenditure, activity levels, and skin temperature on your wrist.
Smart Outlets	Remotely turn any device on or off. It also allows you to track a device's energy level and get custom notifications directly into your smartphone.

Parking Sensors	IoT technology helps users to identify the real-time availability of parking spaces on their phone.
Connect Health	The concept of a connected health care system facilitates real-time health monitoring and patient care. It helps in improved medical decision-making based on patient data.
Smart City	Smart city offers all types of use cases which include traffic management to water distribution, waste management, etc.
Smart home	Smart home encapsulates the connectivity inside your homes. It includes smoke detectors, home appliances, light bulbs, windows, door locks, etc.
Smart supply chain	Helps you in real time tracking of goods while they are on the road, or getting suppliers to exchange inventory information.

Industry Application of IOTs

1. ABB: Smart robotics

Power and robotics firm ABB is one of the most visible to embrace the concept of predictive maintenance, using connected sensors to monitor its robots' maintenance needs — across five continents — and trigger repair before parts break. Also related to IoT is the company's collaborative robotics. Its YuMi model, which was designed to collaborate alongside humans, can accept input via Ethernet and industrial protocols like Profibus and DeviceNet.

2. Airbus: Factory of the Future

To say that assembling a commercial jetliner is an elaborate affair would be an understatement. Such craft have millions of components and tens of thousands of assembly steps, and the cost of mistakes during the process can be enormous. To tackle the complexity, Airbus has launched a digital manufacturing initiative known as Factory of the Future to streamline operations and bolster production capacity. The company has integrated sensors to tools and machines on the shop floor and given workers wearable technology — including industrial smart glasses — designed to reduce errors and bolster safety in the workplace. In one procedure, known as cabin-seat marking, the wearables enabled a 500% improvement in productivity while nearly eliminating errors.

3. Amazon: Reinventing warehousing

The online retail giant doesn't often get called an IIoT company, but, to be sure, the company is an innovator when it comes to warehousing and logistics. As MIT Technology Review has put it:

Amazon is "testing the limits of automation and human-machine collaboration." While the company's ambitions to use drones for delivery has won considerable media attention, the firm’s fulfillment warehouses make use of armies of Wi-Fi-connected Kiva robots. The basic idea behind the Kiva technology, which Amazon acquired for $775 million in 2012, is that it makes more sense to have robots locate shelves of products and bring them to workers rather than have employees go to the shelves to hunt for products. In 2014, the robots helped the company cut its operating costs by 20%, according to Dave Clark, a senior vice president at Amazon.

4. Boeing: Using IoT to drive manufacturing efficiency

Aviation pioneer William Boeing quipped that it “behooves no one to dismiss any novel idea with the statement, ‘It can’t be done.’” The multinational aviation company founded in Boeing’s name apparently still subscribes to that ethos. It is now working toward the long-term goal of making its service offerings more important than its products while being the most valuable information provider in aviation. The company has already made significant strides in transforming its business. Boeing and its Tapestry Solutions subsidiary have aggressively deployed IoT technology to drive efficiency throughout factories and supply chains. The company is also steadily increasing the volumes of connected sensors embedded into its planes.

5. Bosch: Track and trace innovator

In 2015, Bosch launched what would be the Industrial Internet Consortium’s first test bed. The primary inspiration behind the so-called Track and Trace program is that workers would spend a sizable amount of their time hunting down tools. So the company added sensors to its tools to track them, starting with a cordless nutrunner. As the resolution of the tracking becomes more precise, Bosch plans to use the system to guide assembly operations.

6. Caterpillar: An IoT pioneer

Heavy-equipment maker Caterpillar has long been an IoT projects pioneer. Recently, the company, which now often goes by “Cat,” has been showing off the fruits of its investments in IoT technology. For instance, consider how it is using IoT and augmented reality (AR) applications to give machine operators an at-a-glance view of everything from fuel levels to when air filters need replacing. If an old filter expires, the company can send basic instructions for how to replace it via an AR app. The company’s marine asset intelligence division is also an innovator. Last year, Forbes ran an article explaining how the company used sensor-driven analytics to save a bundle of money on boats and shipping vessels.

[Industrial oT World highlights the intersection of IoT and industry, showcasing examples of how IoT transforms business across manufacturing, supply chain and operations. Get your tickets and free passes now.]

7. Fanuc: Helping to minimize downtime in factories

Robotics maker Fanuc is serious about reducing downtime in industrial facilities. Using sensors within its robotics in tandem with cloud-based analytics, the company can predict when failure of a component such as a robotic system or process equipment is imminent. While predictive maintenance is a familiar concept, Fanuc has embraced it more aggressively than most. Last year, GM awarded Fanuc’s Zero Downtime (ZDT) system its Supplier of the Year Innovation Award.

8. Gehring: A pioneer in connected manufacturing

Gehring Technologies, a 91-year-old company that makes machines for honing metal, was early to embrace IIoT technology. Now, the company enables its customers to see live data on how Gehring's machines work before they place an order. It does so by using digital technology, beaming real-time information from a new machine to a customer to ensure that it meets the customer's requirements for precision and efficiency. Gehring uses the same cloud-based real-time tracking to reduce downtime and optimize its own manufacturing productivity through monitoring its connected manufacturing systems, visualizing and analyzing data from its machine tools in the cloud.

9. Hitachi: An integrated IIoT approach

The Japanese company stands out from other industrial companies in terms of its integration and experience across operational and information technology. While most other industrial conglomerates leverage partnerships to fill in the gaps in their IoT knowledge, Hitachi is more independent. The company has more than 16,000 employees focused on the technology in some capacity. While it offers an IoT platform known as Lumada, Hitachi also makes a plethora of products leveraging connected technology, including trains, which the company is beginning to sell as a service. Hitachi has also developed an IoT-enhanced production model that it claims has slashed production lead times by half within its Omika Works division, which manufactures infrastructure for electricity, traffic, steel manufacturing and other industries.

10. John Deere: Self-driving tractors and more

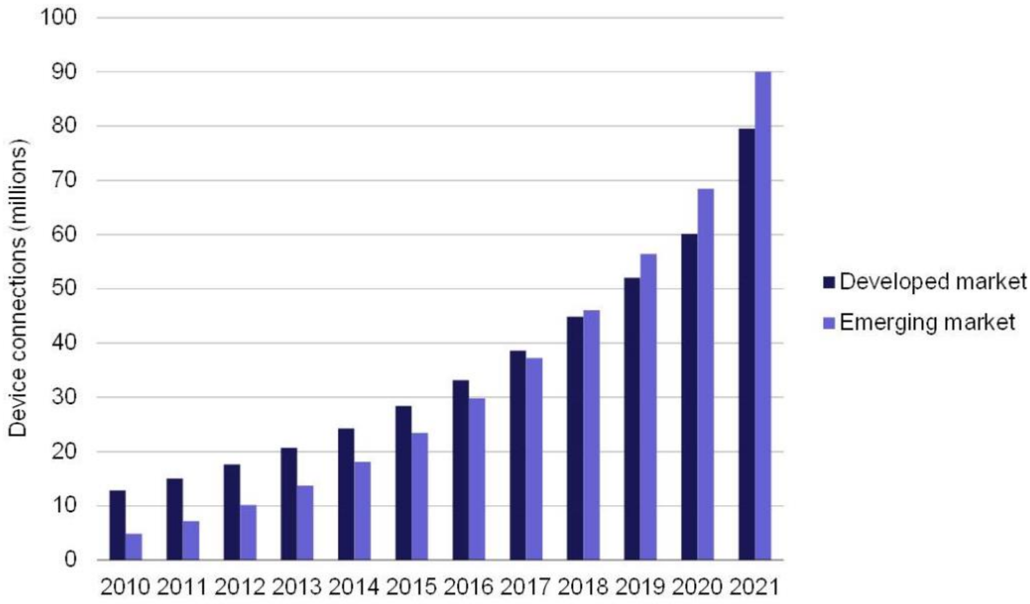
As the field of agriculture becomes more of a science and less of an art passed down the generational line, John Deere is responding by deploying Internet of Things technology — perhaps most notably with self-driving tractors. As The Washington Post wrote in 2015, Google didn't lead the self-driving vehicle revolution. John Deere did. The company also happens to be a pioneer in GPS technology. The most-advanced systems it uses in tractors are accurate to 2 centimetres. In addition, the company has deployed telematics technology for predictive maintenance applications.

Security and surveillance:-

Security and surveillance has become a common facet of business. There are dangers in the world: some are personal dangers, others are dangers or risks associated with assets. While there has been much recent debate about the appropriate use and amount of surveillance, it is fair to say that some amount of security and surveillance is necessary in today's world.

Security and surveillance solutions include everything from the most simple home monitoring systems and burglar alarms, to high-definition, motion-detecting cameras and retina scanning security solutions. Various forms of connectivity – both fixed-line and wireless – enable a basic type of M2M security solutions. However, when data from the solutions are aggregated and analyzed to predict behavior or thwart crimes, and we are able to access these data on common platforms and devices – including mobile devices – we have entered the world of the Internet of Things (IoT). I described this type of change from an M2M to an IoT world in a prior blog post entitled Progression from M2M to the Internet of Things: an introductory blog.

In 2012 there were 28 million security and surveillance IoT device connections worldwide growing to 170 million in 2021 at a compound-annual-growth-rate of 22%. See Figure 1. These include device connections in homes and businesses. Today, quite a large percentage of security and surveillance systems – especially those in homes – are unconnected. We anticipate an increase over the next ten years of the percentage of these kind of home systems that are connected.



Source: Analysys Mason, 2013

Figure 1: Security and surveillance IoT device connections, worldwide, 2010-2021

We also expect an increase in the number of connected security and surveillance systems in emerging geographic markets. As economic conditions continue to increase the overall wealth levels in emerging markets, we anticipate homes and businesses finding it necessary to better secure their environments. While we do not anticipate the overall adoption rate of connected security solutions in emerging markets to exceed that of developed markets, the overall size of the emerging markets make them very attractive for service providers and vendors of residential and commercial security and surveillance solutions.
Over the next ten years, we anticipate an **increased emphasis on four aspects of security and surveillance solutions** – and these four aspects highlight the changes we are seeing from an M2M to an IoT world:

- **IP enablement** – We anticipate increased reliance on IP as the transport medium for security and surveillance solutions. This increased reliance on a common protocol like IP will facilitate the introduction of new solutions and services including various home management solutions, video-based surveillance, facial recognition solutions and others, as well as help simplify the integration of various solutions. Using a common and readily available communications protocol will simplify deployments and lower overall costs for these solutions. In an IoT world, we anticipate reliance on IP as the underlying protocol.
- **Integration with other home and business automation systems** – We anticipate home and commercial security and surveillance solutions to be integrated with other systems including home energy management; security of uniquely-tagged, valuable residential and commercial assets; and building automation solutions. This bundling of solutions with a common user-interface will add simplicity to the customer experience and provide a richer set of information to customers. We anticipate suppliers of traditional residential and commercial alarm systems will be the most likely sellers of these types of integrated solutions.

- **Video** – Higher bandwidth speeds and standardized applications for things like facial recognition and sophisticated movement identification make video-based surveillance solutions more common in both homes and businesses.
- **Mobile device access** – Being able to use standard mobile devices including smartphones and tablets to access security and surveillance data – whether historical records or real-time activities – is something demanded by many residential and commercial buyers of security and surveillance solutions. The proliferation of mobile devices and active application developer communities makes offering mobile device integration much more feasible than several years ago.

We expect service providers and vendors of security and surveillance solutions to continue to offer innovative solutions that bundle together equipment, applications, mobile tools, connectivity, video, and customer support/monitoring services. We anticipate these service providers to make greater use of applications that model, predict and quickly notify monitoring facilities of possible security breaches. **This movement toward integrated offerings and applications signals a change from M2M to IoT.**

What Is Virtual Reality?

Virtual reality (VR) refers to a computer-generated simulation in which a person can interact within an artificial three-dimensional environment using electronic devices, such as special goggles with a screen or gloves fitted with sensors. In this simulated artificial environment, the user is able to have a realistic-feeling experience.

Augmented reality (AR) is different from VR, in that AR enhances the real world as it exists with graphical overlays and does not create a fully immersive experience.

KEY TAKEAWAYS

- Virtual reality (VR) creates an immersive artificial world that can seem quite real, via the use of technology.
- Through a virtual reality viewer, users can look up, down, or any which way, as if they were actually there.
- Virtual reality has many use-cases, including entertainment and gaming, or acting as a sales, educational, or training tool.

Understanding Virtual Reality

The concept of virtual reality is built on the natural combination of two words: the virtual and the real. The former means "nearly" or "conceptually," which leads to an experience that is near-reality through the use of technology. Software creates and serves up virtual worlds that are experienced by users who wear hardware devices such as goggles, headphones, and special gloves. Together, the user can view and interact with the virtual world as if from within.

To understand virtual reality, let's draw a parallel with real-world observations. We understand our surroundings through our senses and the perception mechanisms of our body. Senses include taste, touch, smell, sight, and hearing, as well as spatial awareness and balance. The inputs gathered by these senses are processed by our brains to make interpretations of the objective environment around us. Virtual reality attempts to create an illusory environment that can be presented to our senses with artificial information, making our minds believe it is (almost) a reality.

Virtual Reality Use Cases

The simplest example of VR is a three dimensional (3D) movie. Using special 3D glasses, one gets the immersive experience of being a part of the movie with on-spot presence. The leaf falling from a tree appears to float right in front of the viewer, or the shot of a speeding car going over a cliff makes the viewer feel the chasm's depth and may give some viewers the feeling of falling. Essentially, the light and sound effects of a 3D movie make our vision and hearing senses believe that it's all happening right in front of us, though nothing exists in physical reality.

Technological advances have enabled further enhancement beyond standard 3D glasses. One can now find VR headsets to explore even more. Aided by computer systems, one can now play "real" tennis (or other sports) right in their living room by holding sensor-fitted racquets for playing within a computer-controlled game simulation. The VR headset that players wear on their eyes gives the illusion of being on a tennis court. They move and try to strike depending upon the speed and direction of the incoming ball and strike it with the sensor-fitted racquets. The accuracy of the shot is assessed by the game-controlling computer, which is shown within the VR game accordingly—showing whether the ball was hit too hard and went out of bounds or was hit too soft and was stopped by the net.

Other uses of this VR technology involve training and simulation. For example, those wanting to get a driver's license can get a first-hand experience of road driving using a VR setup that involves handling car parts like the steering wheel, brake, and accelerator. It offers the benefit of experience without the possibility of causing an accident, so students can develop a certain level of expertise in driving before actually being on the road.

Sellers of real estate can also use VR-aided walkthroughs of a home or apartment to give a feel for a property without actually having to physically be at the location with a potential buyer.

Other developing uses are training astronauts for space travel, exploring the intricacies of miniature objects, and allowing medical students to practice surgery on computer-generated subjects.

Application of VR:-

Entertainment

The potential of VR in entertainment is clear and huge as the entertainment industry is multi-billion dollars and consumers are always interested on its novelty. The VR video game world was popularized already by the Disney Movie Tron in 1982. Today the video games are explored in large and realism world through an avatar. In VR games, gamers can look in any direction or walk through the scene.

Hollywood movies offer increasing degrees of realism to make user feel like they are part of the scene. They let the user totally immerse in computer generated world with the help of HMD that supports a stereoscopic view of the scene accordingly to the user’s position and orientation enhanced by audio, haptic and sensory interfaces.

Education

In addition to creating social awareness, the first-person perspective could revolutionize education scenario we have today. Anything that is too dangerous, expensive, or impractical to do in reality, virtual reality is the solution. VR offers visualisation of geometric relationships in difficult concepts or data that are hard to interpret. If the real environment is costly or hazardous to health, VR is the best choice to understand and learn it. For example, flight simulation or fire fighting, nuclear power plant safety, medical procedures etc are the training in VR which are useful for education. Not just these common uses, VR education includes history, anthropology and foreign language acquisition. Students can explore the streets in 17th-century, on different era rather than just reading a book.

Health

VR technology can also help improve today's distributed health care system, in which doctors train to perform routine medical procedures in remote communities around the world. Doctors can immerse themselves in 3D organ models that were generated from medical scan data for better planning and preparation for a medical procedure. It can also be used to explaining the patient and his family so that they make more informed decisions. VR can also provide therapy to people suffering from mental illness.

Manufacturing

The manufacturing industry has used virtual reality to the models and designs it before implementing it.

Tourism and Advertisement

Virtual Reality has been used to create historical sites, which then enables users to experience it with comfort from your house. For instance you can even create the war that happened at and location and feel being in war. The advertisement and shopping experience would be even better with VR. In case of shopping experiences even Augmented Reality are used to get information of products

Smart Systems

Smart systems combine segments of human cognition with machine accuracy. Bringing applications ranging from manufacturing, construction, and healthcare to aerospace and ICT, they are dynamic and versatile. The increasing adoption of smart systems in all these sectors can be attributed to the fact that smart systems can alleviate pressing global challenges like waste, medical care, and man-induced climate change. For instance, a self-improving, smart manufacturing line can rectify mistakes and build processes based on real-time data to optimize resource consumption through an organic learning process. From artificial organs to drug dispensing devices that communicate with hospital networks remotely and autonomously, the healthcare sector is leading the adoption of smart systems. Smart devices in healthcare allowing chronic diseases to be monitored in real-time for well-informed, timely treatment are freely available in the market today. In fact, reports suggest that the healthcare and fitness sectors will account for over 50 percent of the smart devices shipped this year. Furthermore, smart systems also greatly reduce our impact on the environment. Smart cars that are virtually emission-free and smarter homes that are designed to minimize their ecological impact are examples of smart systems that progressively reduce environmental damage.

The reducing size and increasing power of sensors and other smart system components is paving the way for smart system integration – where a combination of various smart systems is deployed. This will increase the viability of the Internet of Things, where every object and person on the planet is connected to the Internet. The proliferation of smart systems will have a profound effect on talent acquisition and management too. As evidenced by history, when systems get smarter, people need to follow suit. By automating repetitive tasks such as reporting, data collection, and maintenance, these newly streamlined, multidimensional business processes will also mobilize the workforce into adding value. Aside from the ability to track every aspect of consumer and device behaviour, organizations can now eliminate waste, decrease costs through predictive maintenance, and focus on innovation through structural efficiency and robust processes.

Analytical ability, adaptability and predictive prowess are now as important to the business process as efficiency and productivity. Once organizations are able to extract valuable insights from the data they gather, the possibilities for personalized, data-focused decisions are limitless. Have you taken any steps to make your organization 'smarter'? Do let us know by using the comments section below.

Smart systems are emerging in multiple sectors driven by intensifying global competition and accompanying cost pressures, volatility in customer demand, concern for energy usage, and increased technology options. They, along with the potential for an even more broadly interconnected "Internet of Things", are also enabled by dramatic growth in information and sensor technologies. Smart Systems include the most discussed (and interrelated) cloud computing, smart manufacturing and smart grid, as well as healthcare, transportation (autonomous vehicles and smart highways), and emergency response.

In each case, the promise is:

- reduced costly down time enabled by systems that are self-diagnosing and self-correcting that offer predictive maintenance and redundancy switching before problems result in down time. Thus, smart grid addresses the need for energy cost reduction but also enhanced grid reliability;
- better informed planning with real-time modelling feedback along with qualification of materials, products and actions;
- increased flexibility and shortened system-wide response time to changing conditions; Potentially, support for modularity even in large, complex and traditionally customized units.

The systems should facilitate use of competing vendors and globally distributed production while ensuring consistent knowledge, data gathering and understanding across value chains.

The "Internet of Things" adds functionality to everyday objects. Refrigerators could monitor food condition and usage. Devices could coordinate energy usage and signal overloads. Industrial products could store information about their origin, destination (in transit), components, condition and use at varying stages of their lifecycle.

Challenges arise in transitioning from legacy processes, choosing migration paths from potential approaches (with more options emerging), and reconciling the needs and positions of diverse stakeholders. In many cases, there are significant initial costs which must be balanced with long term savings. The conversion to a national smart grid could cost trillions of dollars. System design can be difficult as IT developers and manufacturers, for example, operate in very different cultures and structures. Optimization across companies or even industries may force behavior changes and even reduce efficiency and performance for some users (e.g., optimal grid usage might push manufacturers to alter work schedules; and enabled pricing models and individual user informed control could challenge traditional power utility practices.)

Evolving standards will be essential in providing:

- common data formats and performance measures across devices, sensors and organizations;
- the basis for system designs supporting interoperability and modularity;
- potential consensus selection of development paths and transitions;
- vehicles for companies to balance their strategic and operational requirements with broader system demands;
- Enhanced confidence in investment decisions.

Embedded systems

Embedded systems are special-purpose computing systems embedded in application environments or in other computing systems and provide specialized support. The decreasing cost of processing power, combined with the decreasing cost of memory and the ability to design low-cost systems on chip, has led to the development and deployment of embedded computing systems in a wide range of application environments. Examples include network adapters for computing systems and mobile phones, control systems for air conditioning, industrial systems, and cars, and surveillance systems. Embedded systems for networking include two types of systems required for end-to-end service provision: infrastructure (core network) systems and end systems. The first category includes all systems required for the core network to operate, such as switches, bridges, and routers, while the second category includes systems visible to the end users, such as mobile phones and modems.

The importance of embedded systems is continuously increasing considering the breadth of application fields where they are used. For a long time, embedded systems have been used in many critical application domains, such as avionics and traffic management systems. Their broad use illustrates the importance of embedded systems, especially when considering the potential effects of their failure. For example, a failure of an automatic pilot system or a failure of a car braking system can lead to significant loss of life; failure of an electric power system may lead to loss of life or, if not to that, to loss of quality of life; and failure of a production control system in a factory may lead to a significant loss of revenue. Our dependence on embedded systems requires development and adoption of new architectural and design techniques in order to meet the necessary performance requirements and to achieve the required dependability using their limited resources in terms of processing, memory, and power.

The importance of embedded systems has led to the emergence of a strong industry that develops and uses them. Their criticality for services on all fronts and for technological and thus economic growth has led to significant efforts to address the challenges placed by embedded systems development and deployment. One important effort is the ARTEMIS initiative of the European Commission [1]. This program started with a Strategic Research Agenda (SRA) [8] and has grown to a significant activity, including a strong industrial association, named ARTEMISIA, which conducts research and development in the area of embedded systems. Figure 1-2, a figure from the ARTEMIS SRA [8], shows one view of the embedded systems area organized by research domains and application contexts. In Figure 1-2, horizontal bars constitute technological areas involved in embedded systems development and vertical bars indicate application contexts where embedded systems are used and are expected to penetrate applications in the future. Considering the differentiated requirements of embedded systems adoption in different application areas, Figure 1-2 groups in application contexts the services and applications that have common characteristics; different application contexts have significant differences among them. For example, the application context of private spaces includes systems and services for the home environment, the car, and private environments in general, where comfort and safety are the highest priority, while the context of industrial systems focuses on safety-critical systems for industry, avionics, and others.

Clearly, the organization and semantics of application contexts change as time progresses and new applications and services are developed. One can organize the vertical bars with different criteria, such as, for example, the industrial sectors involved in the development of embedded systems.