SUBJECT : TH-4

INTERNET OF THINGS

POONAM PANDA
[PTGF, E & TC]

Th.4(ii)-INTERNET Of THINGS

(Elective)

Name of the Course: Diploma in **Electronics & Communication** Engineering			
Course code:		Semester	6th
Total Period:	60	Examination	3 hrs
Theory periods:	4P / week	Class Test:	20
Tutorial:		End SemesterExamination:	80
Maximum marks:	100		

A. RATIONALE:

Internet of Things and develop skills required to build real-life IoT based projects. The Internet of things describes the network of physical objects—things‖—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet. The goal behind the Internet of things is to have devices that self report in real-time, improving **efficiency** and bringing important information to the surface more quickly than a system depending on human intervention.Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security and environmental monitoring all are examples of **internet of things** applications for smart cities

B. OBJECTIVE:

After completion of this subject the student will be able to know:

1. Understand internet of Things and its hardware and software components
2. Interface I/O devices, sensors & communication modules
3. Remotely monitor data and control devices
4. Develop real life IoT based projects

C. Topic wise distribution ofperiods:

Sl. No.	Topics	Period
1	Introduction to IoT	08
2	Elements of IoT	10
3	IoT Application Development	14
4	Smart Technology	10
5	Smart TVs: Viewing in a Connected World	08
6	IoT Case Studies	10
	Total:	**60**

D. COURSECONTENTS:

1. Introduction to IoT

- 1.1 What isIoT.
- 1.2 Architectural Overview,
- 1.3 Design principles and neededcapabilities,
- 1.4 IoT Applications, Sensing,Actuation,
- 1.5 Basics of Networking, M2M and IoTTechnology
- 1.6 Fundamentals- Devices andgateways,
- 1.7 Data management, Business processes inIoT,
- 1.8 Everything as aService(XaaS),
- 1.9 Role of Cloud in IoT, Security aspects inIoT.

2. Elements ofIoT

- 2.1 Hardware Components- Computing (Arduino,RaspberryPi),
- 2.2 Communication, Sensing, Actuation, I/Ointerfaces.
- 2.3 Software Components- Programming API's (using Python/Node.js/Arduino) forCommunication
- 2.4 Protocols-MQTT, ZigBee, Bluetooth, CoAP, UDP,TCP.

3. IoT ApplicationDevelopment

- 3.1 Solution framework for IoTapplications-
- 3.2 Implementation of Deviceintegration,
- 3.3 Data acquisition andintegration,

3.4 Device data storage- Unstructured data storage on cloud/localserver,
3.5 Authentication, authorization of devices.

4. Smart Technology

4.1 Understanding the IoT BigPicture
4.2 Building the Internet of Things
4.3 Understanding Smart Devices, BuildingBlocks
4.4 Understanding Network Connections
4.5 Understanding IPAddresses
4.6 Understanding cellular Network & MeshNetwork

5. Smart TVs: Viewing in a Connected World

5.1 What is Smart TV & itsuse
5.2 What is inside SmartTV
5.3 What a Smart TVdoes
5.4 Smart TV OperatingSystems
5.5 What is Smart TVSet-Top Devices
5.6 Integrating Smart TV in toIOT

6. IoT Case Studies

6.1 IoT case studies (anyone)
a. SmartHome
b. Smartcar
c. SmartCities
d. SmartDrones
6.2 Industrialautomation,

Syllabus coverage up to Internal assessment

Chapters: 1, 2, 3 and 4.

Learning Resources:

1. Vijay Madisetti, ArshdeepBahga, IoT Case Studies, "A Hands-on Approach", University Press
2. Michael Miller, Internet ofThings,Pearson
3. Dr. SRN Reddy, RachitThukral and Manasi Mishra, "Introduction to Internet of Things: Apractical Approach", ETILabs
4. Pethuru Raj and Anupama C. Raman, "The Internet of Things: Enabling Technologies, Platforms, and Use Cases", CRCPress
5. Jeeva Jose, "Internet of Things", Khanna Publishing House,Delhi
6. Adrian McEwen, "Designing the Internet of Things", Wiley
7. Raj Kamal, "Internet of Things: Architecture and Design", McGrawHill
8. Cuno Pfister, "Getting Started with the Internet of Things", O ReillyMedia

1.1 WHAT IS IOT

The **Internet of things** (**IoT**) describes the network of physical objects—"things" or objects—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet

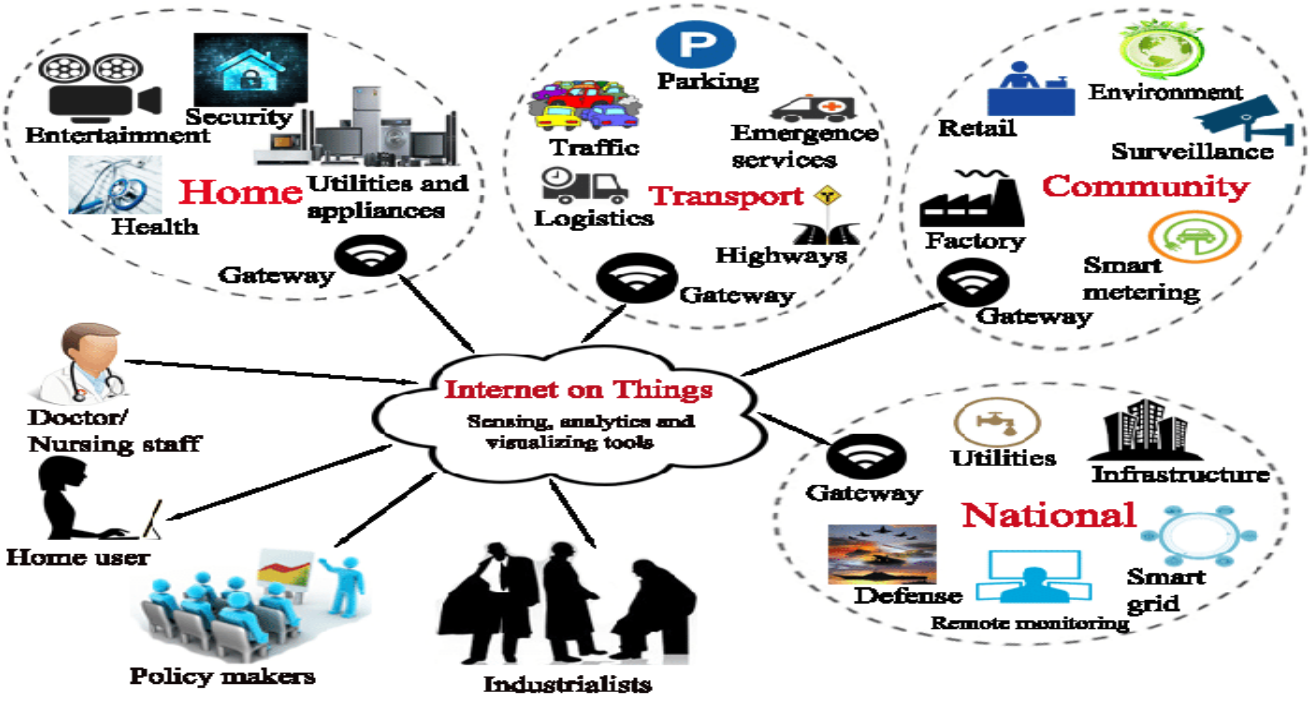
Things have evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smart phones and smart speakers. IoT can also be used in healthcare systems.

Definition:

A dynamic global n/w infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into information n/w, often communicate data associated with users and their environments.

Characteristics:

1. **Dynamic & Self Adapting**: IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, users context or sensed environment.
   Eg: the surveillance system is adapting itself based on context and changing conditions.
2. **Self-Configuring:** allowing a large number of devices to work together to provide certain functionality.
3. **Inter Operable Communication Protocols:** support a number of interoperable communication protocols and can communicate with other devices and also with infrastructure.
4. **Unique Identity:** Each IoT device has a unique identity and a unique identifier(IP address).
5. **Integrated into Information Network:** that allow them to communicate and exchange data with



other devices and systems

1.2 ARCHITECTURAL OVERVIEW

- **What is the Internet of Things? -** The concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices. The IoT is a giant network of connected things and people – all of which collect and share data about the way they are used and about the environment around them.
- **How does it work?** Devices and objects with built in sensors are connected to an Internet of Things platform, which integrates data from the different devices and applies analytics to share the most valuable information with applications built to address specific needs.
- **These powerful IoT platforms** can pinpoint exactly what information is useful and what can safely be ignored. This information can be used to detect patterns, make recommendations, and detect possible problems before they occur.
- **For example,** if a car manufacturing business, might want to know which optional components (leather seats or alloy wheels, for example) are the most popular. Using Internet of Things technology,it is possible to:
  - **Use sensors** to detect which areas in a showroom are the most popular, and where customers linger longest;
  - **Drill down** into the available sales data to identify which components are selling fastest;
  - **Automatically** align sales data with supply, so that popular items don't go out of stock.
- **The information** picked up by connected devices enables to make smart decisions about which components to stock up on, based on real-time information, which helps save time and money.
- **With the insight** provided by advanced analytics comes the power to make processes more efficient. Smart objects and systems mean you can automate certain tasks, particularly when these are repetitive, mundane, time-consuming or even dangerous.

1.3 DESIGN PRINCIPLES AND NEEDED CAPABILITIES

In the near future, our everyday lives will be more and more filled with intelligent, connected objects. They will appear in our homes, in our working environments and in the cities, we live in as well as travel with us everywhere we go in the form of wearable, smart clothing and things we cannot even imagine right now. This development is called the internet of things, IoT.

IoT solutions consist of multiple elements: physical devices like sensors, actuators and interactive devices, the network connecting these devices, the data gathered from these devices and analyzed to create a meaningful experience and last but definitely not least, the physical context in which user interacts with the solution.

Design principles

1. Do your research

When designing IoT-enabled products, designers might make the mistake of forgetting why

customers value these products in the first place. That's why it's a good idea to think about the value an IoT offering should deliver at the initial phase of your design.

When getting into IoT design, you're not building products anymore. You're building services and experiences that improve people's lives. That's why in-depth qualitative research is the key to figuring out how you can do that.

Assume the perspective of your customers to understand what they need and how your IoT implementation can solve their pain points. Research your target audience deeply to see what their existing experiences are and what they wish was different about them.

2. Concentrate on value

Early adopters are eager to try out new technologies. But the rest of your customer base might be reluctant to put a new solution to use. They may not feel confident with it and are likely to be cautious about using it.

If you want your IoT solution to become widely adopted, you need to focus on the actual tangible value it's going to deliver to your target audience.

What is the real end-user value of your solution? What might be the barriers to adopting new technology? How can your solution address them specifically?

Note that the features the early tech adopters might find valuable might turn out to be completely uninteresting for the majority of users. That's why you need to carefully plan which features to include and in what order, always concentrating on the actual value they provide.

3. Don't forget about the bigger picture

One characteristic trait of IoT solutions is that they typically include multiple devices that come with different capabilities and consist of both digital and physical touch points. Your solution might also be delivered to users in cooperation with service providers.

That's why it's not enough to design a single touch point well. Instead, you need to take the bigger picture into account and treat your IoT system holistically.

Delineate the role of every device and service. Develop a conceptual model of how users will perceive and understand the system. All the parts of your system need to work seamlessly together. Only then you'll be able to create a meaningful experience for your end-users.

4. Remember about the security

Don't forget that IoT solutions aren't purely digital. They're located in the real-world context, and the consequences of their actions might be serious if something goes wrong. At the same time, building trust in IoT solutions should be one of your main design drivers.

Make sure that every interaction with your product builds consumer trust rather than breaking it. In practice, it means that you should understand all the possible error situations that may be related to the context of its use. Then try to design your product in a way to prevent them. If error situations occur, make sure that the user is informed appropriately and provided with help.

Also, consider data security and privacy as a key aspect of your implementation. Users need to feel that their data is safe, and objects located in their workspaces or home can't be hacked. That's why quality assurance and testing the system in the real-world context are so important.

5. Build with the context in mind

And speaking of context, it pays to remember that IoT solutions are located at the intersection of the physical and digital world. The commands you give through digital interfaces produce real-world effects. Unlike digital commands, these actions may not be easily undone.

In a real-world context, many unexpected things may happen. That's why you need to make sure that the design of your solution enables users to feel safe and in control at all times.

The context itself is a crucial consideration during IoT design. Depending on the physical context of your solution, you might have different goals in mind. For example, you might want to minimize user distraction or design devices that will be resistant to the changing weather conditions.

The social context is an important factor, as well. Don't forget that the devices you design for workspaces or homes will be used by multiple users.

6. Make good use of prototypes

IoT solutions are often difficult to upgrade. Once the user places the connected object somewhere, it might be hard to replace it with a new version – especially if the user would have to pay for the upgrade.

Even the software within the object might be hard to update because of security and privacy reasons. Make sure that your design practices help to avoid costly hardware iterations. Get your solution right from the start. From the design perspective, it means that prototyping and rapid iteration will become critical in the early stages of the project.

Needed capabilities

1. Connectivity

It starts with how a device or sensor connects to the internet and a cloud platform. There are many options to choose from Wi-Fi through a hub or gateway, 2G, or 3G cellular networks. Once you have connectivity in place, now you can get the device or sensor talking to your cloud IoT platform. Ensure you find a service provider that can send data through clean API's that are easy to implement and install. This will ensure you can get quickly setup and start capturing your data within minutes.

2. Control

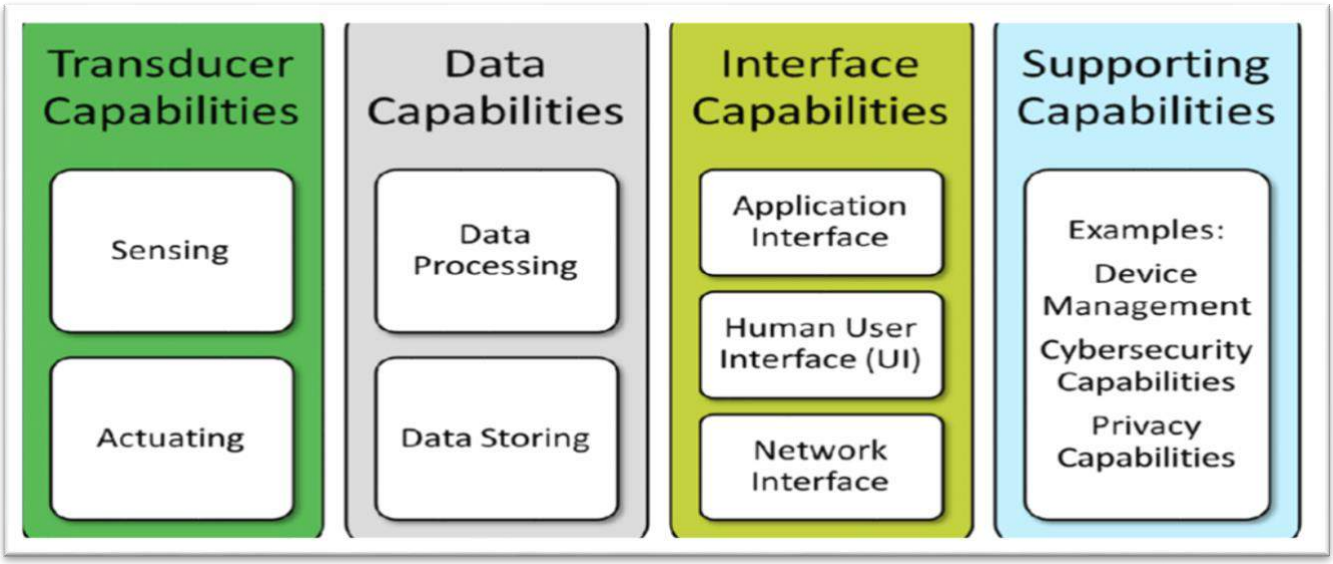
The next capability necessary when evaluating an IoT data platform is control of the device. There are a number of different scenarios for control including controlling a device through an application, device-to-device communication, or control from the cloud (based on an event, rule or some other pre-determined condition). For example, if you have a water leak detector, it can automatically send a command to the device which could be an appliance or part of the core infrastructure to turn off the water valve. Here, using two-way communication, a signal can be sent from the detector to the device via the cloud to shut off the water. Lastly, you can program the device from an app (or website) to shut off at a certain time or schedule based on a pre-programmed rule.

3. Device Management

Device management is also a major consideration. To keep devices and sensors up to date and functional, a strong device management solution is a core component of an IoT cloud platform. There are a few main capabilities a device management platform provides, including the ability for manufacturers to send software or firmware updates OTA (over-the-air), factory provisioning, as well as an out-of-box experience (OOBE).OOBE is part of a core experience that is often left to the last minute or completely glossed over. It's the first experience that an end user, be it a consumer, installer or technician has when interacting with a device for the first time.

4. Actionable Data

The last capability you should consider in a IoT data platform is how you can query the data in a manner that is clear and meaningful. It's one thing to get all your data in place, but the value of the data is only realized when it's turned into information that can help solve a problem. We want organizations to focus on their core competency, like making great appliances or services that deliver value to their customers, rather than focusing on cloud infrastructure that makes it possible.



1.4 IOT APPLICATIONS, SENSING AND ACTUATION

IoT Applications

The IoT applications are addressing the societal needs and the advancements to enabling technologies such as nano-electronics and cyber-physical systems continue to be challenged by a variety of technical (i.e., scientific and engineering), institutional, and economical issues.

List of IOT Applications

1. Smart Home
2. Wearable
3. Smart City
4. Smart Grid
5. Industrial IoT
6. Connected Car
7. Connected Healthcare
8. Smart Retail
9. Smart Transportation and Mobility

10. Smart Agriculture/ Farming

1) Smart Home

Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicted Smart homes will become as common as smartphones. The cost of owning a house is the biggest expense in a homeowner's life. Smart Home products are promised to save time, energy and money.

2) Wearable

Wearable devices are installed with sensors and software which collect data and information about the users. This data is later pre-processed to extract essential insights about user. These devices broadly cover fitness, health and entertainment requirements. The pre-requisite from internet of things technology for wearable applications is to be highly energy efficient or ultra-low power and small sized.

3) Smart City

Smart cities use IoT devices such as connected sensors, lights, and meters to collect and analyze data. The cities then use this data to improve infrastructure, public utilities and services, and more.

Smart city devices work to make everyday tasks easier and more efficient, while relieving pain points related to public safety, traffic, and environmental issues.

4) Smart Grid

The basic idea behind the smart grids is to collect data in an automated fashion and analyze the behavior or electricity consumers and suppliers for improving efficiency as well as economics of electricity use. Smart Grids will also be able to detect sources of power outages more quickly and at individual household levels like nearby solar panel, making possible distributed energy system.

5) Industrial IoT

Industrial internet of things is empowering industrial engineering with sensors, software and big data analytics to create brilliant machines. IoT holds great potential for quality control and sustainability. Applications for tracking goods, real time information exchange about inventory among suppliers and retailers and automated delivery will increase the supply chain efficiency.

6) Connected Cars

A connected car is a vehicle which is able to optimise its own operation, maintenance as well as comfort of passengers using on-board sensors and internet connectivity.

Most large auto makers as well as some brave startups are working on connected car solutions. Major brands like Tesla, BMW, Apple, Google are working on bringing the next revolution in automobiles.

7) Connected Healthcare

It can be used for out-patient care by healthcare providers, letting them get ECG, heart rate, respiratory rate, skin temperature, body posture, fall detection, and activity readings remotely. This can alert doctors to potential health problems before they arise, or give them additional insights into which treatments will be most effective for their patients, even when their patients aren't in the office.

8) Smart Retail

Today, retail stores are constantly focusing on leveraging the emerging technologies like cloud, mobile, RFID, beacons, etc., to provide connected retail services and better shopping experience to customers. For example, store owners are integrating sensors in the key zones of retail stores and connecting them to cloud through a gateway that enables real-time data analysis related to products, sales, and customers from these sensors.

Interestingly, IoT in retail and connected technologies are taking the retail industry by storm. 96% retailers are ready to make changes required to implement the Internet of Things in their stores.

9) Smart Transportation and Mobility

Internet of Vehicles (IoV) connected with the concept of Internet of Energy (IoE) represent future trends for smart transportation.

IoT technology that includes vehicle monitoring and maintenance, real-time tracking of packages, environmental sensors in shipping containers, information-gathering on employees and tools, and a number of safety-enhancing features for vehicles and people.

***10)* Smart Agriculture/ Farming**

Farmers are using meaningful insights from the data to yield better return on investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertiliser are some simple uses of IoT.

Sensors and Actuators

Sensors and actuators have a number of similarities and dissimilarities in the functioning or processing. Here we have listed the differences between the actuator and a sensor.

- The main difference between an actuator and a sensor is that the sensor converts the physical gesture into electrical signals and do different works. Whereas, the actuator is responsible for the conversion of electrical signal to mechanical work.
- Sensors measure discrete as well as continuous process variables. On the other hand, actuators are used to impel the parameters of both discrete and continuous processes.
- Sensors are widely used to original electrical signals in different electrical application. On the other hand, actuators are very useful in the production of energy in the form of heat and motion.
- Sensors are used as an input device because of the reason it is placed at input dork of the machine. However, actuator are used as output device as it is mostly placed at output port of the machinery.
- Sensors are the one which acts as a brain because it provides information to do work.

Difference between Sensor and Actuator:

SENSOR	ACTUATOR
It converts physical characteristics into electrical signals.	It converts electrical signals into physical characteristics.
It takes input from environment.	It takes input from output conditioning unit of system.
It gives output to input conditioning unit of system.	It gives output to environment.
Sensor generated electrical signals.	Actuator generates heat or motion.
It is placed at input port of the system.	It is placed at output port of the system.
It is used to measure the physical quantity.	It is used to measure the continuous and discrete process parameters.
It gives information to the system about environment.	It accepts command to perform a function.

Example: Photo-voltaic cell which converts light energy into electrical energy.	Example: Stepper motor where electrical energy drives the motor.

Sensor

Sensor is a device used for the conversion of physical events or characteristics into the electrical signals. This is a hardware device that takes the input from environment and gives to the system by converting it.

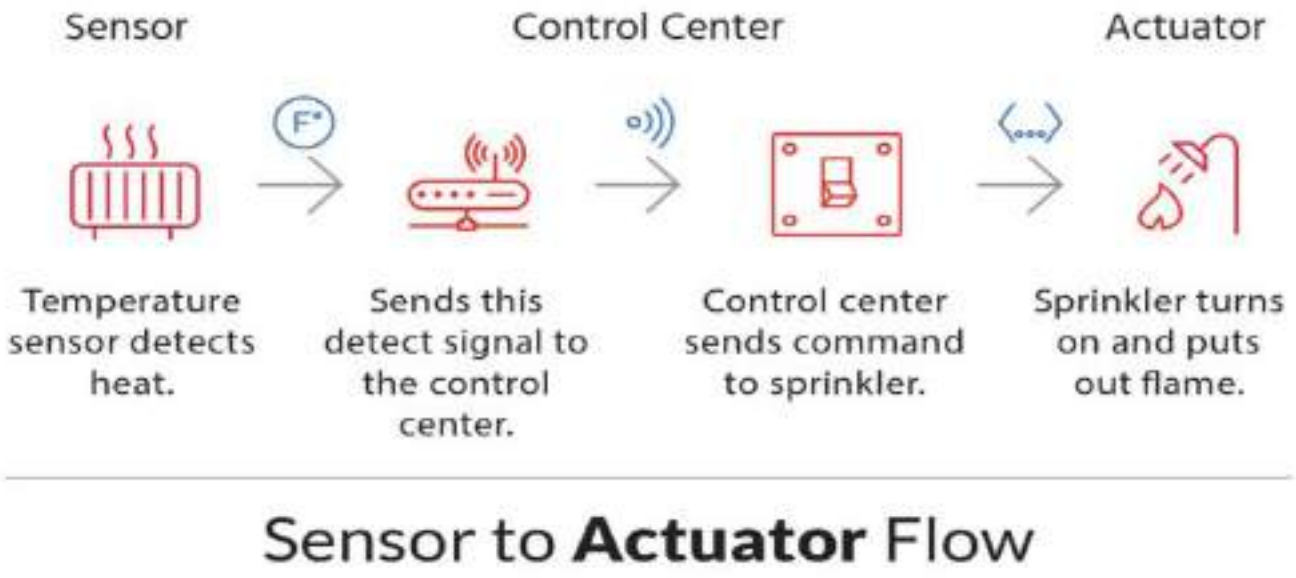
For example, a thermometer takes the temperature as physical characteristic and then converts it into electrical signals for the system.

Actuator

Actuator is a device that converts the electrical signals into the physical events or characteristics. It takes the input from the system and gives output to the environment.

For example, motors and heaters are some of the commonly used actuators.

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.



Types of sensors	Types of actuators
Humidity Sensors	Linear Actuators
Pressure Sensors	Rotary Actuators
Proximity Sensors	Hydraulic Actuators
Level Sensors	Pneumatic Actuators
Accelerometers	Electric Actuators

Gas Sensors	Thermal and Magnetic Actuators
Temperature sensor	Mechanical Actuators

1.5 BASICS OF NETWORKING, M2M AND IOTTECHNOLOGY

Basics of Networking

Today computer networks are everywhere. You will find them in homes, offices, factories, hospitals leisure centers etc.

Home and Office Networks

- The network you have at home uses the same networking technologies, protocols and services that are used in large corporate networks and on the Internet.
- The only real difference between an home network and a large corporate network is the size.
- A home network will have between 1 and 20 devices and a corporate network will have many thousands.
- If you are completely new to networking then the basic course will introduce you to the basic networking protocols used in small home/office networks and on the Internet.
- Setting Up and building a Home Network will introduce some basic networking component and show you how to build a home network and connect it to the Internet.

Networking Types

Networks can be **wired** or **wireless** with most networks being a mixture of both.

Wired vs Wireless Networks

- Early (pre-2008) networks were predominately wired.
- Today however most networks will use a mixture of wired and wireless network.
- Wired networks use Ethernet as the data link protocol. This is unlikely to change with the IOT, as IOT devices will be predominantly wireless.

Wired Networks- Advantages and Disadvantages

Advantages:

- Ethernet ports are found on almost all laptops/PCs and netbooks even on those 8 years old.
- Wired networks are faster than Wireless. Data rates were periodically increased from the original 10 megabits per second, to 1gigabits per second. Most home networks use 10-100Mbps.
- More secure than Wireless

Disadvantages:

- Need to Use cable which can be unsightly, difficult to run and expensive.
- Can't be used easily between buildings (planning etc.).
- **Note** a new technology that uses mains cable overcomes many of these disadvantages. powerline networking is common on home/small office networks
- Not supported on Mobile phones and tablets.

Wireless Networks – Advantages and Disadvantages

- Wireless networks use **Wi-fi** as the data link protocol. However other wireless options are being developed for the IOT (Internet of things).

Advantages:

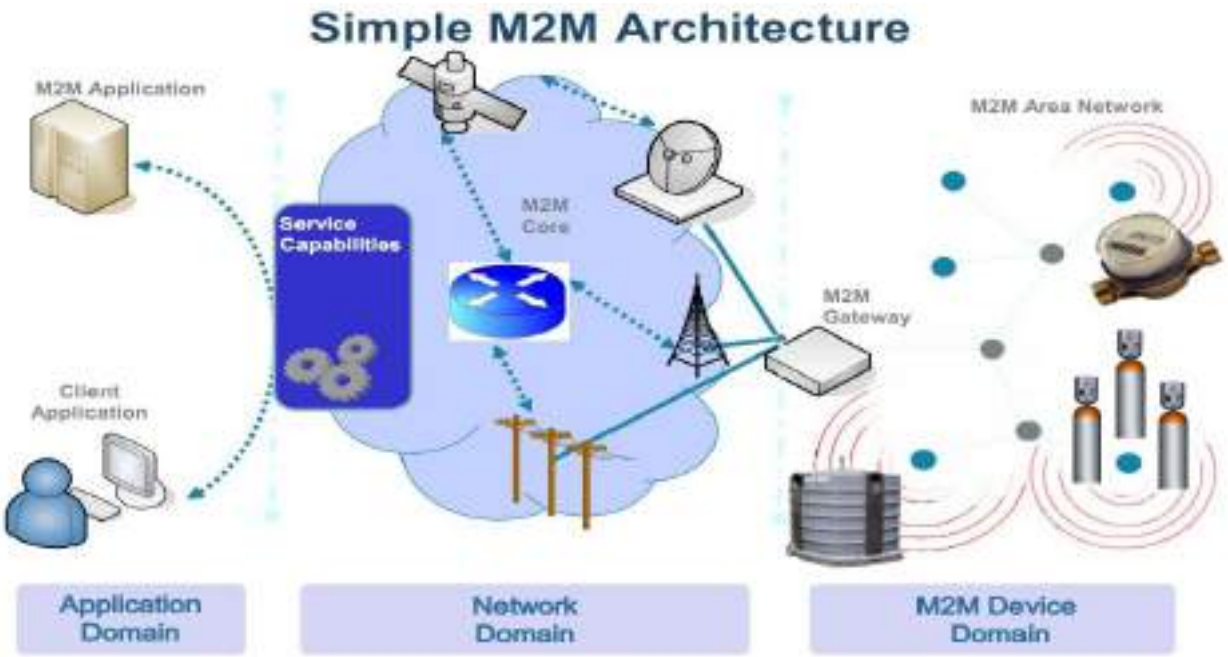
- Generally easier to set up.
- Can be used both on home and public networks
- No cables required.
- Can be used with mobile phones and tablets.

Disadvantages

- Generally Slower than wired networks.
- Limited by range.
- Open to eavesdropping.
- Not as secure depending on set up.

M2M

➔ Shows the end-to-end architecture of M2M systems comprises of M2M area networks, communication networks and application domain.



1. **Machine to machine** (**M2M**) is direct communication between devices using any communications channel, including wired and wireless.
2. Machine to machine communication can include industrial instrumentation, enabling a sensor or meter to communicate the information it records (such as temperature, inventory level, etc.) to application software that can use it (for example, adjusting an industrial process based on temperature or placing orders to replenish inventory).
3. Such communication was originally accomplished by having a remote network of machines relay information back to a central hub for analysis, which would then be rerouted into a system like a personal computer.

4. More recent machine to machine communication has changed into a system of networks that transmits data to personal appliances. The expansion of IP networks around the world has made machine to machine communication quicker and easier while using less power. These networks also allow new business opportunities for consumers and suppliers.
5. M2M is not a new technology, primarily because it doesn't actually require any wireless technologies or complex digital devices. A wired connection between two machines can still be considered an M2M connection, and indeed the very first iterations of this technology used phone lines to communicate.
6. However, in the modern world, M2M usually refers to machines that communicate using things like WiFi or mobile networks. In this article, we're going to take a look at what technology underpins M2M, and how it's applied in the real world.
7. M2M generally centers around the concept of telemetry. This is simply where sensors of varying types will collect information, and then relay it to a central point of some description. In the past, this central point may have been a person or a personal computer.
8. The data would be interpreted and then used. This is still often the case today. However, modern M2M systems allow for far more complexity, allowing machines to communicate with one another and make decisions quickly.

IoT Technology

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.

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.
- 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.
- Also recommended for you: IoT Connectivity - 4 Latest Standards That Will Shape 2020 and beyond.

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. smartwatches, 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.

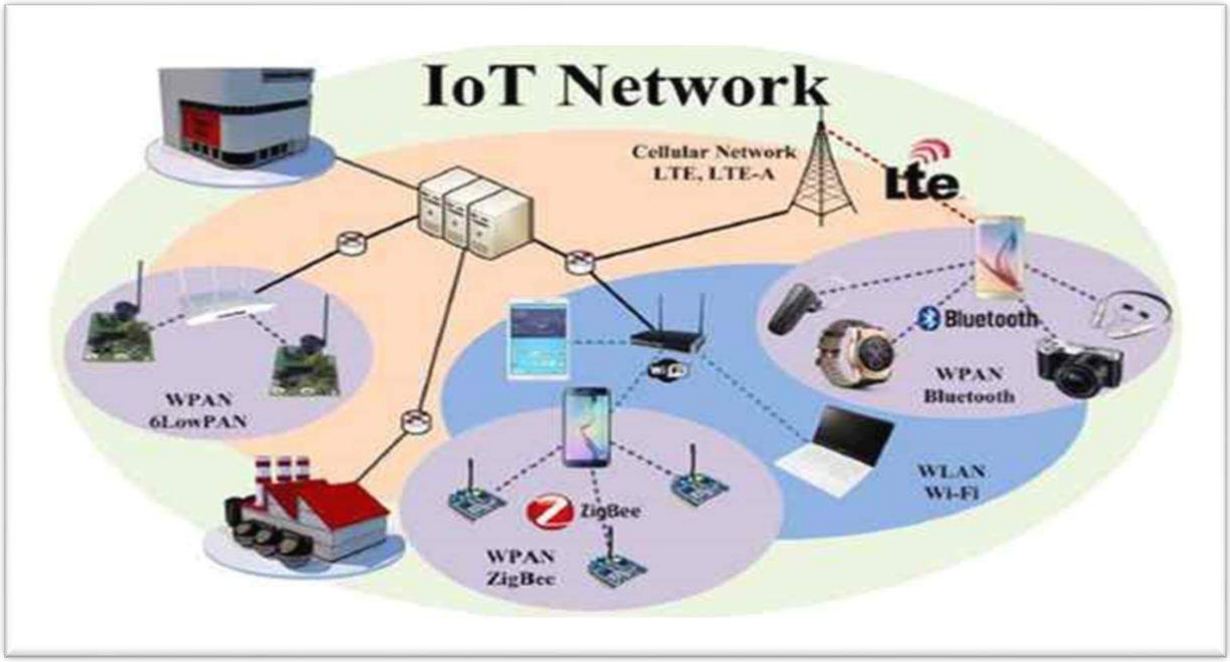
6. RFID

- 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.

What Technologies Have Made IoT Possible?

While the idea of IoT has been in existence for a long time, a collection of recent advances in a number of different technologies has made it practical.

- **Access to low-cost, low-power sensor technology.** Affordable and reliable sensors are making IoT technology possible for more manufacturers.
- **Connectivity.** A host of network protocols for the internet has made it easy to connect sensors to the cloud and to other "things" for efficient data transfer.
- **Cloud computing platforms.** The increase in the availability of cloud platforms enables both businesses and consumers to access the infrastructure they need to scale up without actually having to manage it all.
- **Machine learning and analytics.** With advances in machine learning and analytics, along with access to varied and vast amounts of data stored in the cloud, businesses can gather insights faster and more easily. The emergence of these allied technologies continues to push the boundaries of IoT and the data produced by IoT also feeds these technologies.
- **Conversational artificial intelligence (AI).** Advances in neural networks have brought natural-language processing (NLP) to IoT devices (such as digital personal assistants Alexa, Cortana, and Siri) and made them appealing, affordable, and viable for home use.



Differences between IoT and M2M

1) Communication Protocols:
   - Commonly uses M2M protocols include ZigBee, Bluetooth, ModBus, M-Bus, Wireless M-Bustec.
   - In IoT uses HTTP, CoAP, WebSocket,MQTT, XMPP, DDS, AMQP etc.,
2) Machines in M2M Vs Things inIoT:
   - Machines in M2M will be homogenous whereas Things in IoT will beheterogeneous.
3) Hardware Vs SoftwareEmphasis:
   - the emphasis of M2M is more on hardware with embedded modules, the emphasis of IoT is more on software.
4) Data Collection &Analysis
   - M2M data is collected in point solutions and often in on-premises storageinfrastructure.
   - The data in IoT is collected in the cloud (can be public, private or hybridcloud).
5) Applications
   - M2M data is collected in point solutions and can be accessed by on-premises applications such as diagnosis applications, service management applications, and on- premisis enterpriseapplications.
   - IoT data is collected in the cloud and can be accessed by cloud applications suchas analytics applications, enterprise applications, remote diagnosis and management applications,etc.

1.6 FUNDAMENTALS- DEVICES AND GATEWAYS

Devices

The sensing/actuating stage covers everything from legacy industrial devices to robotic camera systems, water level detectors, air quality sensors, accelerometers, and heart rate monitors. And the scope of the IoT is expanding rapidly, thanks in part to low-power wireless sensor network technologies and Power over Ethernet, which enable devices on a wired LAN to operate without the need for an A/C power source.

Physical devices and controllers that might control multiple devices. These are the thingsin the IoT, and they include a wide range of endpoint devices that send and receive information. Today, the list of devices is already extensive. It will become almost unlimited as more equipment is added to the IoT over time. Devices are diverse, and there are no rules about size, location, form factor, or origin. Some devices will be the size of a silicon chip. Some will be as large as vehicles. The IoT must support the entire range. Dozens or hundreds of equipment manufacturers will produce IoT devices.

Gateways

- Simply put, an IoT gateway is a physical device or virtual platform that connects sensors, IoT modules, and smart devices to the cloud.
- Gateways serve as a wireless access portal to give IoT devices access to the internet.
- On the surface, it may sound like a simple router, enabling communication between different protocols and devices.
- But IoT Gateways are sophisticated technology that does so much more, like edge-computing in particular.
- An IoT Gateway collects massive data from many connected devices and sensors in any given IoT ecosystem.

- The gateway pre-processes the data before passing it along to cloud platforms, where the heavy lifting of transforming data into meaningful intelligence is accomplished.
- IoT gateways also receive information from the cloud, sent back to devices to allow autonomous management of devices in the field.

"This means that all the information moving through an IoT ecosystem – from an IoT device to the cloud, or vice versa – goes through a connected IoT gateway."

1.7 DATA MANAGEMENT AND BUSINESS PROCESSES IN IOT

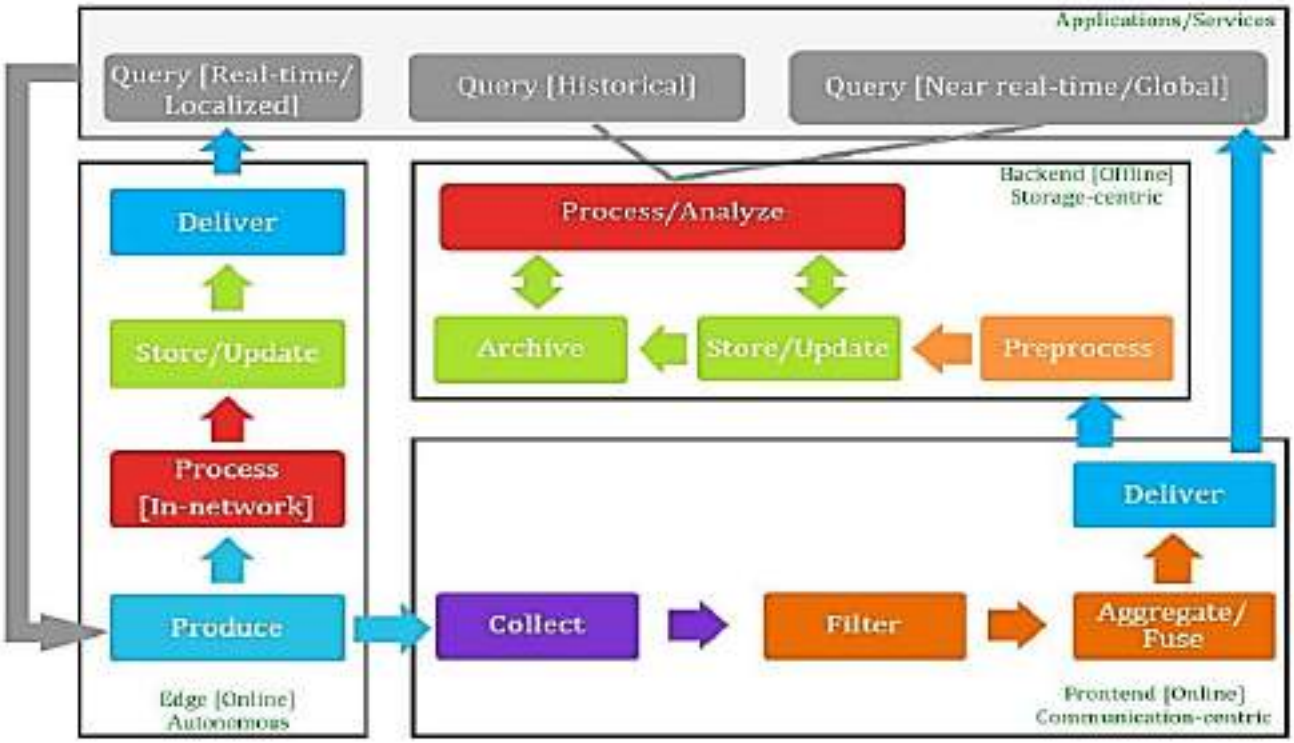
Data Management

Traditional data management systems handle the storage, retrieval, and update of elementary data items, records and files. In the context of IoT, data management systems must summarize data online while providing storage, logging, and auditing facilities for offline analysis. This expands the concept of data management from offline storage, query processing, and transaction management operations into online-offline communication/storage dual operations. We first define the data lifecycle within the context of IoT and then outline the energy consumption profile for each of the phases in order to have a better understanding of IoT data management.

IoT Data Lifecycle

The lifecycle of data within an IoT system—illustrated in Figure —proceeds from data production to aggregation, transfer, optional filtering and preprocessing, and finally to storage and archiving. Querying and analysis are the end points that initiate (request) and consume data production, but data production can be set to be "pushed" to the IoT consuming services. Production, collection, aggregation, filtering, and some basic querying and preliminary processing functionalities are considered online, communication-intensive operations. Intensive preprocessing, long-term storage and archival and in-depth processing/analysis are considered offline storage-intensive operations.

Storage operations aim at making data available on the long term for constant access/updates, while archival is concerned with read-only data. Since some IoT systems may generate, process, and store data in-network for real-time and localized services, with no need to propagate this data further up to concentration points in the system, "edges" that combine both processing and storage elements may exist as autonomous units in the cycle. In the following paragraphs, each of the elements in the IoT data lifecycle is explained



- ***Querying***: Data-intensive systems rely on querying as the core process to access and retrieve data. In the context of IoT, a query can be issued either to request real-time data to be collected for temporal monitoring purposes or to retrieve a certain view of the data stored within the system. The first case is typical when a (mostly localized) real-time request for data is needed. The second case represents more globalized views of data and in-depth analysis of trends and patterns.
- ***Production***: Data production involves sensing and transfer of data by the "Things" within the IoT framework and reporting this data to interested parties periodically (as in a subscribe/notify model), pushing it up the network to aggregation points and subsequently to database servers, or sending it as a response triggered by queries that request the data from sensors and smart objects. Data is usually time-stamped and possibly geo-stamped, and can be in the form of simple key-value pairs, or it may contain rich audio/image/video content, with varying degrees of complexity in-between.
- ***Collection****:* The sensors and smart objects within the IoT may store the data for a certain time interval or report it to governing components. Data may be collected at concentration points or gateways within the network where it is further filtered and processed, and possibly fused into compact forms for efficient transmission. Wireless communication technologies such as Zigbee, Wi-Fi and cellular are used by objects to send data to collection points.
- ***Aggregation****/Fusion*: Transmitting all the raw data out of the network in real-time is often prohibitively expensive given the increasing data streaming rates and the limited bandwidth. Aggregation and fusion techniques deploy summarization and merging operations in real-time to compress the volume of data to be stored and transmitted.
- ***Delivery***: As data is filtered, aggregated, and possibly processed either at the concentration points or at the autonomous virtual units within the IoT, the results of these processes may need to be sent further up the system, either as final responses, or for storage and in-depth analysis. Wired or wireless broadband communications may be used there to transfer data to permanent data stores.
- ***Preprocessing***: IoT data will come from different sources with varying formats and structures. Data may need to be preprocessed to handle missing data, remove redundancies and integrate data from

different sources into a unified scheme before being committed to storage. This preprocessing is a known procedure in data mining called data cleaning.

- ***Storage****/Update—Archiving*: This phase handles the efficient storage and organization of data as well as the continuous update of data with new information as it becomes available. Archiving refers to the offline long-term storage of data that is not immediately needed for the system's ongoing operations. The core of centralized storage is the deployment of storage structures that adapt to the various data types and the frequency of data capture.
- ***Processing****/Analysis*: This phase involves the ongoing retrieval and analysis operations performed and stored and archived data in order to gain insights into historical data and predict future trends, or to detect abnormalities in the data that may trigger further investigation or action. Task-specific preprocessing may be needed to filter and clean data before meaningful operations take place.

Business Processes in IoT

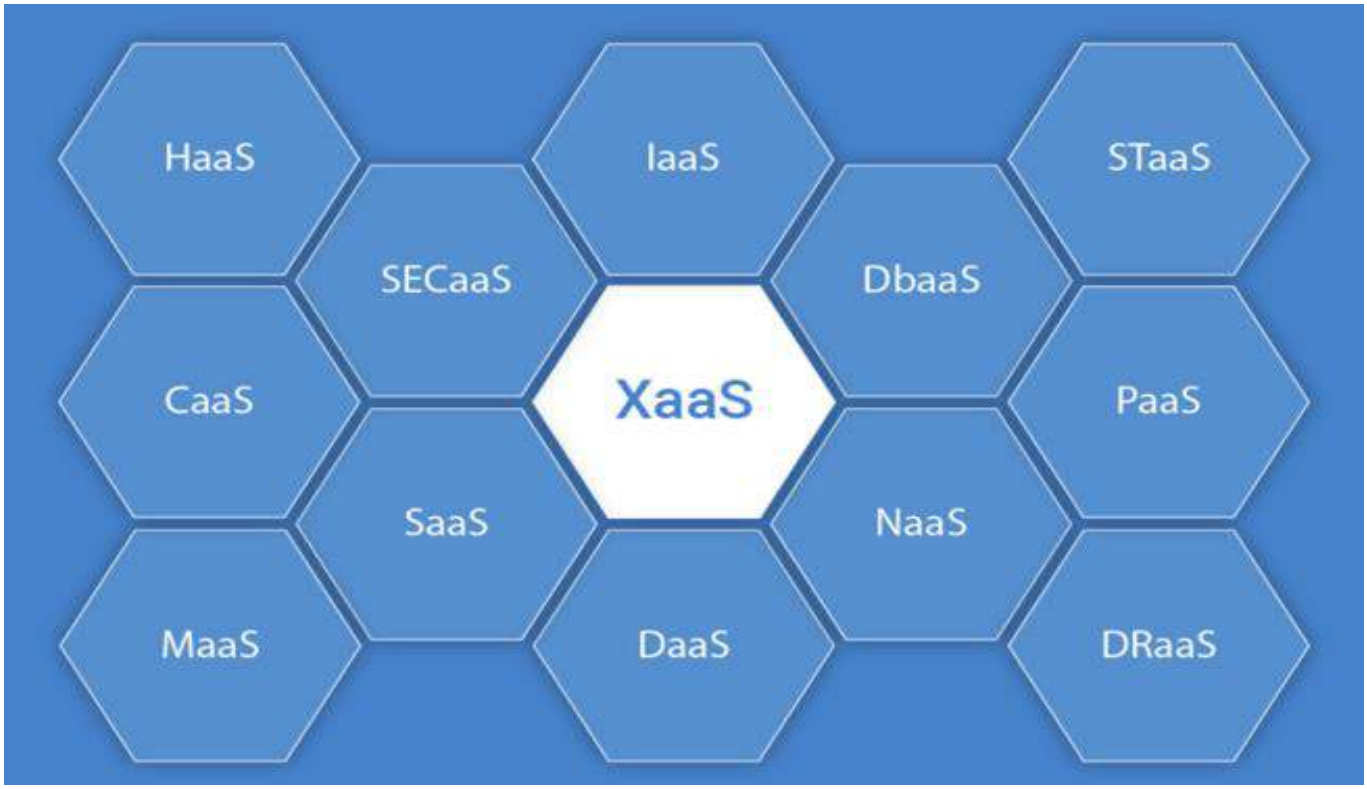
The IoT is changing the way we live our lives and that is something that will only grow and grow, and it's certainly something that all businesses need to adapt to. There are some obvious benefits and some aspects that will require adjustments to processes. Here are some of the main changes and challenges facing companies as the IoT becomes more ever-present:

- **Data**: As consumers use more and more devices that record data, there are opportunities for businesses to use this data for marketing and product development purposes, but only if the processes are in place to measure, analyze and report on this data. Business process management can automate this process and ensure that it remains effective and agile enough to keep pace with technological changes.
- **New ways of buying**: The IoT gives consumers the chance to buy directly from their devices, whether it's an Amazon Echo or a smartphone or even that legendary refrigerator ordering fresh milk. Technology is making everything faster and more easily, so they will also be expecting faster deliveries and better service. BPM needs to be used to manage the processes that will allow this kind of development to meet the demand. IoT software and tools can help with this though, with inventories able to be tracked automatically.
- **Innovation**: Whether it's new product development or upgrading existing products or services, the IoT offers the opportunities for businesses to deliver exciting new benefits for their customers.
- **Customer service**: Another area where processes need to be managed carefully because of the changes that the IoT have brought in is customer service. Products that utilize the internet should really be able to be fixed over the internet when something goes wrong. Consumers expect it and businesses should be able to deliver it, so BPM is needed to ensure that customer service processes are effective, efficient and easy to cope.
- **Centralized BPM**: Business process management isn't simply something that is needed to make the IoT run more smoothly, the benefits can flow back in the opposite direction too. Integrating BPM software into devices means that the data can be analyzed from a central location and any changes can be fed back out again.

1.8 EVERYTHING AS A SERVICE (XAAS)

XaaS is a general, collective term that refers to the delivery of **anything as a service**. It recognizes the vast number of products, tools and technologies that vendors now deliver to users as a **service** over a network -- typically the internet -- rather than provide locally or on-site within an enterprise.

Most major companies now offer some form of XaaS, including Microsoft Azure, the various Amazon Web Services (AWS), and even Google Apps. In fact, if there are any types of IT services or computer-based functionality you require, then there is a high probability you can obtain it as XaaS. Some of the most common types of XaaS include:



Types of XaaS

1. Hardware-as-a-Service (HaaS)
2. Communication-as-a-Service (CaaS)
3. Monitoring as a Service (MaaS)
4. Security-as-a-Service (SECaaS)
5. Software-as-a-Service (SaaS)
6. Infrastructure as a service (IaaS)
7. Desktop-as-a-Service (DaaS)
8. Database-as-a-Service (DBaaS)
9. Network-as-a-service (NaaS)
10. Storage-as-a-Service (STaaS)
11. Platform-as-a service (PaaS)
12. Disaster recovery-as-a-service (DRaaS)

1. **Hardware-as-a-Service (HaaS):** Managed service providers (MSP) own some hardware and install it on customers' sites on demand. Customers utilize the hardware in accordance with service level

agreements. This pay-as-you-go model is similar to leasing and can be compared to IaaS when computing resources are located at MSP's site and provided to users as virtual equivalents of physical hardware.

2. **Communication-as-a-Service (CaaS):** This model includes different communication solutions such as VoIP (voice over IP or Internet telephony), IM (instant messaging), video conference applications that are hosted in the vendor's cloud. A company can selectively deploy communication apps that best suit their current needs for a certain period and pay for this usage period only.
3. **Monitoring-as-a-Service (MaaS)** is a security service that provides security to IT assets of any business 24/7. It plays a vital role in securing an enterprise or government clients from any possible cyber threats. MaaS is a monitoring service that can be outsourced in a flexible and consumption-based subscription model.
4. **Security-as-a-Service (SECaaS):** This is the model of outsourced security management. A provider integrates their security services into your company's infrastructure and, as a rule, delivers them over the Internet. Such services may include anti-virus software, encryption, authentication, intrusion detection solutions and more.
5. **Software-as-a-Service (SaaS):** It is a cloud-based method of providing software to users. SaaS users subscribe to an application rather than purchasing it once and installing it. Users can log into and use a SaaS application from any compatible device over the Internet. The actual application runs in cloud servers that may be far removed from a user's location.
6. **Infrastructure-as-a-Service(IaaS)** is an instant computing infrastructure, provisioned and managed over the internet. A cloud computing service provider, such as Azure, manages the infrastructure, while you purchase, install, configure and manage your own software—operating systems, middleware and applications.
7. **Desktop-as-a-Service (DaaS):** Desktops are delivered as virtual services along with the apps needed for use. Thus, a client can work on a personal computer, using the computing capacities of third-party servers (which can be much more powerful than those of a PC).
8. **Database-as-a-Service (DBaaS)** is a cloud computing service model that provides users with some form of access to a database without the need for setting up physical hardware, installing software or configuring for performance. All of the administrative tasks and maintenance are taken care of by the service provider so that all the user or application owner needs to do is use the database. Of course, if the customer opts for more control over the database, this option is available and may vary depending on the provider.
9. **Network-as-a-Service-(NaaS)** brings Software Defined Networking (SDN), programmable networking and API-based operation to WAN services, transport, hybrid cloud, multi-cloud, Private Network Interconnect, and Internet Exchanges.Historic definitions focused on fundamental concepts of NaaS including: NaaS describes services for network transport connectivity.NaaS involves the optimization of resource allocations by considering network and computing resources as a unified whole.
10. **Storage-as-a-Service (SaaS)** is a cloud business model in which a company leases or rents its storage infrastructure to another company or individuals to store data.The client transfers the data meant for storage to the service provider on a set schedule over the SaaS provider's wide area network or over the Internet.
11. Platform-as-a-Service (PaaS) as the name suggests, provides you computing platforms which typically includes operating system, programming language execution environment, database, web server etc. Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos.
12. Disaster recovery-as-a-Service**(DRaaS)** is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third party cloud computing environment and provide all the DR orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster. The as-a-service model means that the organization itself doesn't have to own all the

resources or handle all the management for disaster recovery, instead relying on the service provider.

1.9 ROLE OF CLOUD IN IOT AND SECURITY ASPECTS IN IOT

Role of Cloud in IoT

- The Cloud is a centralized system that helps to deliver and transport data and various files across the Internet to data centers. The different data and programs can be accessed easily from the centralized Cloud system. Cloud Computing is an economic solution, as it does not require on-site infrastructure for storage, processing and analytics. The scalability of Cloud Computing means that as your business grows, your technological and analytical capabilities can too.
- There are different types of Cloud services available, including Microsoft Azure Cloud development, and more information on each of these varying types of Cloud solutions can be found in our previous guide.
- it is essential that both cloud and IoT form cloud-based IoT applications in a bid to make the most out of their combination. This alliance has led to the success of IoT. In addition to this, here are a few more pointers as to why the cloud is important from the point of view of IoT's success that are-

1.Provides remote processing power

Cloud as a technology empowers IoT to move beyond regular appliances such as air conditioners, refrigerators etc. This is because the cloud has such a vast storage that it takes away dependencies on on-premise infrastructure. With the rise of miniaturization and transition of 4G to higher internet speeds, the cloud will allow developers to offload fast computing processes.

2.Provides security and privacy

IoT's role in harnessing mobility is immense. However, its prowess would be incomplete without security. Cloud has made IoT more secure with preventive, detective and corrective controls. It has enabled users with strong security measures by providing effective authentication and encryption protocols. In addition to this, managing and securing the identity of users has been possible for IoT products with the help of biometrics. All of this is possible because of cloud's security.

3.Removes entry barrier for hosting providers

Today, many innovations in the field of IoT are looking at plug-and-play hosting services. Which is why the cloud is a perfect fit for IoT. Hosting **providers** do not have to depend on massive equipment or even any kind of hardware that will not support the agility IoT devices require. With the cloud, most hosting providers can allow their clients a ready-to-roll model, removing entry barriers for them.

4.Facilitates inter-device communication

Cloud acts as a bridge in the form of a mediator or communication facilitator when it comes to IoT. Many powerful APIs like Cloudflare, Cloud Cache and Drops are enabled by cloud communications, allowing easy linking to smartphones. This eases devices to talk to each other and not just us, which essentially is the tenet of IoT cloud.

It would be fair to say that cloud can accelerate the growth of IoT. However, deploying cloud technology also has certain challenges and shortcomings. Not because the cloud is flawed as a technology but the combination of IoT cloud can burden users with some obstacles. If you ever go ahead with an IoT cloud solution, it is better if you know the kind of challenges you may face in advance.

Security Aspect in IoT

As most of the systems are using existing wireless networks such aswifi, zigbee, zwave, GSM etc.IoT systems can be hacked using wireless devices. In order to have safe and secure use of IoT devices and IoT network, following precautions are advisable. These are very useful as IoT security aspects for both the user as well as IoT network service provider.

1. Do not store any critical business or personal data in internet cloud.
2. Do not store any password in your IoT device or anywhere in internet cloud.
3. Do not install any malware without verifying its authenticity.
4. Always install third-party software from authentic and genuine websites.
5. Do not be hurry in start using the IoT device, first secure your newly purchased IoT device with anti-malware and anti-virus softwares.
6. If possible, regularly change the password of IoT device in order to improve the security.
7. Do not bring any sensitive business material for re-work at home if home network is less secured compare to office network. Do not store such material in easily hackable storage devices or public storage locations. Moreover, avoid using wifi network for such work.
8. Switch off unused IoT devices as they are vulnerable for potential attack by hackers in a home network. For example, switch off IoT compliant thermostats when not needed.
9. Switch off wifi in your smartphone when you do not require internet access. This is because it has been found that smartphone-based fitness applications are vulnerable to leak passwords as well as location information easily over public wifi networks.
10. Business, finance and banking related companies should store the data and retain them till they are needed. Once they are no longer required, they should be deleted to minimize the possible hacking.
11. House owner should be cautious enough so that no unclaimed IoT device get installed or placed in their premises without their notice. As later these devices can be utilized by hackers for their bad intention.
12. IoT Service provider should provide regular software patches for smart watch, IoT sensors, IoT gadgets, healthcare applications used in smartphone etc. This helps IoT devices to be more secure. These patches should be robust enough to take care of modern and latest malwares and viruses.
13. Individually wireless networks based on various technologies are already been secured, which also helps avoid any possible security threats. Refer following links for further study on IoT security.