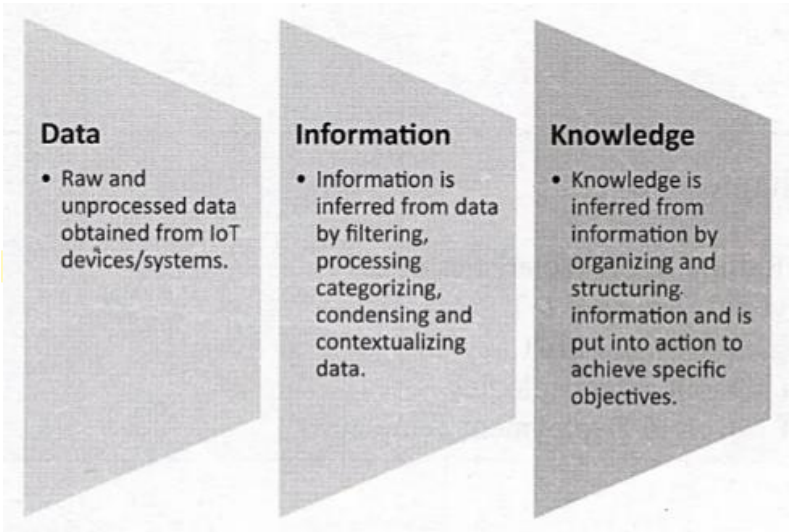
Reference book: "Internet of Things: A Hands-on Approach", by Arshdeep Bahga and Vijay Madisetti

Introduction:

Internet of Things(IoT) comprises things that have unique identities and are connected to the internet. While many existing devices, such as networked computers or 4G enabled mobile phones, already have some form of unique identities and are also connected to the internet the focus on IoT is in the configuration, control and networking via the internet of devices or "things" that are traditionally not associated with internet. These include devices such as thermostats, utility meters, a Bluetooth connected headset, irrigation pumps and sensors or control circuits for an electric car's engine. Internet of Things is a new revolution in the capabilities of the endpoints that are connected to the internet, and is being driven by the advancement in capabilities in sensor networks, mobile devices, wireless communications, networking and cloud technologies.

The scope of IoT is not limited to just connecting things to internet. IoT allows these things to communicate and exchange data while executing meaningful applications towards a common user or machine goal. Data itself does not have a meaning until it is contextualized processed into useful information. Applications on IoT network extract and create information from lower level data by filtering, processing, categorizing, condensing and contextualizing the data. This information obtained is then organized and structured to infer knowledge about the system and/or its users, its environment, and its operation and progress towards its objectives allowing a smarter performance. For example, consider a series of row sensor measurements ((75,45) ;(84,56)) generated by a weather monitoring station, which themselves do not have any meaning or context. To give meaning to the data, a context is added, which in this example can be that each tuple in data represents the temperature and humidity measured every minute. With this context added we know the meaning (or information) of the measured data tuples. Further information is obtained by categorizing, condensing or processing this data. For example, the average temperature and humidity readings for last five minutes is obtained by averaging the last five data tuples. The next step is to organize the information and relationships between pieces of information to infer knowledge which can be put into action. For example, an alert is raised if the average temperature in last five minutes exceeds 120F, and this alert may be conditioned on the users's geographical position as well.

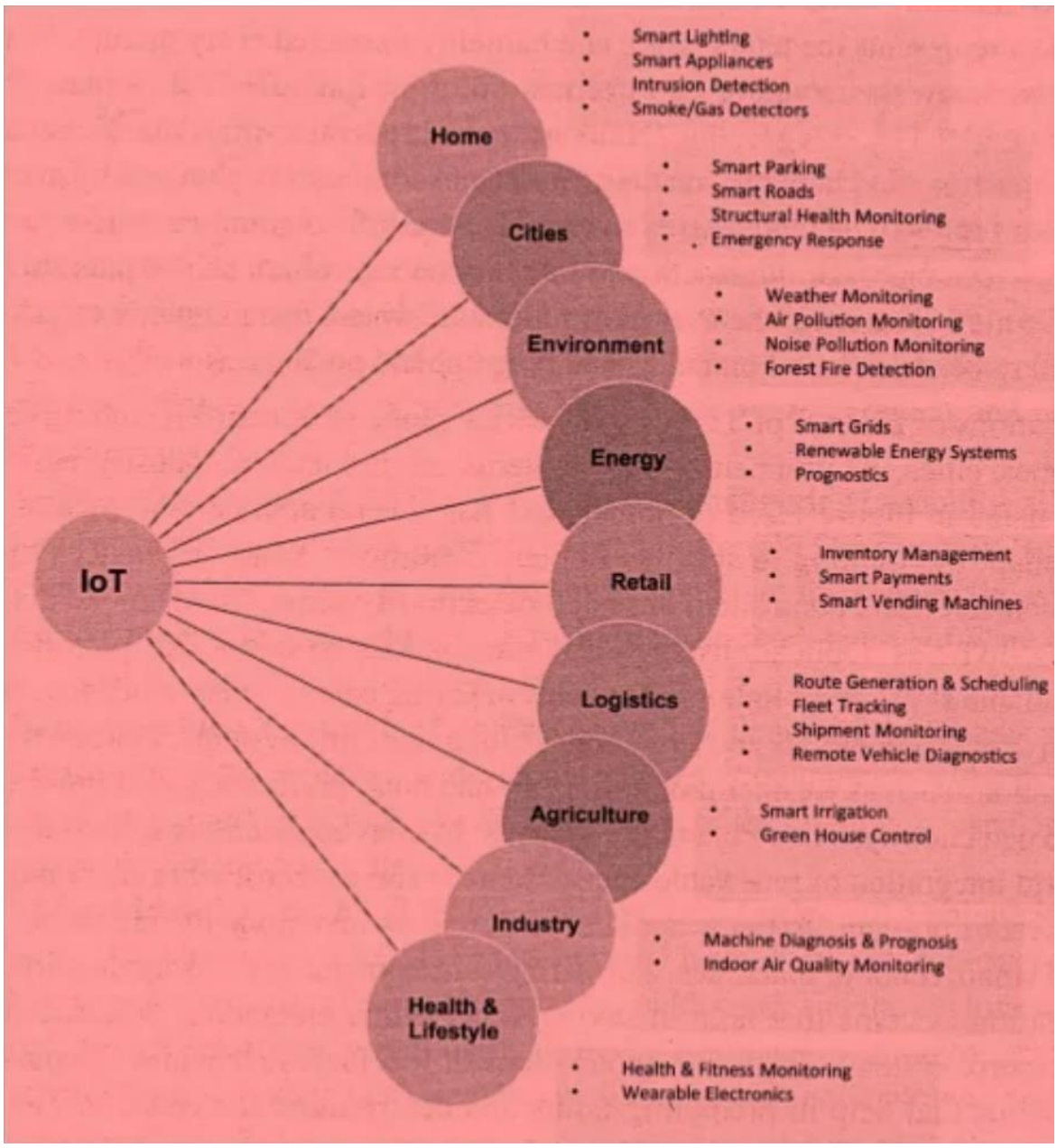
Example Of thermometer



The applications of IoT span a wide range of domains including (but not limited to)
1) Home
2) Cities
3) Environment
4) Energy
5) Retail

6) Logistics
7) Agriculture
8) Industry
9) Health & Life Style

For homes, IoT has several applications such as smart lighting that adapt the lighting to suit the ambient conditions, smart appliances that can be remotely monitored and controlled intrusion detection systems, smart smoke detectors etc. For cities, IoT has applications such as smart parking systems that provide status updates on available slots, smart lighting that helps in saving energy, smart roads that provide information on driving conditions and structural health monitoring systems. For environment, IoT has applications such as weather monitoring, air and noise pollution, forest fire detection and river flood detection systems. For energy systems, IoT has applications such as including smart grids, grid integration of renewable energy sources and prognostic health management systems. For retail domain, IoT has applications such as inventory management, smart payments and smart vending machines. For agriculture domain, IoT has applications such as smart irrigation systems that help in saving water while enhancing productivity and green house control systems. Industrial applications of IoT include machine diagnosis and prognosis systems that help in predicting faults and determining the cause of faults and indoor air quality systems. For health and lifestyle, IoT has applications such as health and fitness monitoring systems and wearable electronics.



Definition of IoT:

"A dynamic global network 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 the information network, often communicate data associated with users and their environments."

Characteristics of IoT:

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, user's context, or sensed environment. For example, consider a surveillance system comprising of a number of surveillance cameras. The surveillance cameras can adapt their modes (to normal or infra-red night modes) based on whether it is day or night. Cameras could switch from lower resolution to higher resolution modes when any motion is detected and alert nearby cameras to do the same. In this example, the surveillance system is adapting itself based on the context and changing (e.g., dynamic) conditions.

Boat speaker

Self-Configuring: IoT devices may have self-configuring capability, allowing a large number of devices to work together to provide certain functionality (such as weather monitoring). These devices have the ability configure themselves (in association with the IoT infrastructure), setup the networking, and fetch latest software upgrades with minimal manual or user intervention.

Interoperable Communication Protocols: IoT devices may support a number of interoperable communication protocols and can communicate with other devices and also with the infrastructure.

Unique Identity: Each IoT device has a unique identity and a unique identifier (such as an IP address or a URI). IoT systems may have intelligent interfaces which adapt based on the context, allow communicating with users and the environmental contexts. IoT device interfaces allow users to query the devices, monitor their status, and control them remotely, in association with the control, configuration and management infrastructure.

Integrated into Information Network: IoT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems. IoT devices can be dynamically discovered in the network, by other devices and/or the network, and have the capability to describe themselves (and their characteristics) to other devices or user applications. For example, a weather monitoring node can describe its monitoring capabilities to another connected node so that they can communicate and exchange data. Integration into the information network helps in making lot systems "smarter" due to the collective intelligence of the individual devices in collaboration with the infrastructure. Thus, the data from a large number of connected weather monitoring IoT nodes can be aggregated and analysed to predict the weather.

Reference book: The Internet of Things by Pethuru Raj, Anupama C. Raman

The IoT Challenges and the Research Domains

With the projection of extreme data, billions of devices, and trillions of digital entities, the challenges on IoT are bound to rise up sharply. The current IoT environments are bound to face a variety of shortcomings for **storing the massive amount of IoT data** and for subjecting the collected IoT **data appropriate analytics to extract timely and actionable insights**. International Data Corporation (IDC) has clearly visualized and portrayed the following critical and crucial challenges for IoT for the envisioned IoT days. We need elastic **compute servers, storage appliances, and network connectivity solutions on the infrastructure front**. On the platform side, we need highly synchronized platforms for simplifying **data cleansing,**

translation, aggregation, mining, and processing. Further, **knowledge discovery and dissemination platforms** are insisted on sharing what is extracted out of IoT data. Data centers are transitioning toward cloud centers (cloud 1.0) and the next evolution is cloud enabled data centers (cloud 2.0) through the incorporation of powerful concepts such as software defined compute, storage, and networking. That is, **future data centers will be software-defined, automated, optimized, and virtualized**. The containerization concept being expounded by the Docker technology is another interesting thing to watch for in the years to unfold. Thus, the traditional IoT infrastructures and platforms are being tweaked to be highly right and relevant for the projected IoT era.

The Research Domains

There are conferences and confluences fostering the deep discussion on IoT-related issues focusing on technical enablers of the next-generation IoT applications. The first and foremost thing is to establish and sustain seamless and spontaneous connectivity between multiple and heterogeneous elements and entities. The **connectivity with remote applications and data sources too has to be realized** for physical devices to be intelligent. The other principal requirement is **the service enablement** as every important thing is being expressed and exposed as a service through one or more interfaces for the outside world. Any service requesters and users can easily find and send out requests to services-providing devices. The key research topics include:

1. Energy-efficient device architectures: Energy conservation and preservation occupy an important research topic due to the fact that any environment or physical asset comprises a variety of sensors and actuators attached to it. Owing to the multiplicity of devices, the energy need is bound to zoom up and hence energy optimization turns out to be an important topic for study and research. Energy harvesting and novel hardware designs are being given extra thrust considering the faster stabilization of the IoT days.

2. Elastic IoT infrastructures: There can be an unexpected spike in the number of devices and people participating in any IoT environment and applications. Thus, IoT platforms and infrastructures need to be highly adaptive and accommodative to have a large number of communicating devices and digitized objects.

3. Highly optimized communication protocol: There are a massive number of resource-constrained, networked, and embedded devices in an IoT environment. Further, there is an emerging phenomenon of edge or fog computing devices such as IoT gateways, smart meters and appliances, smartphones, data aggregators, and so on. For transmitting data and document messages within themselves as well as with remote control or analytical application packages, a suite of pioneering protocols is being insisted across. Standard protocols are being tweaked to be highly beneficial for specific application domains.

4. Data deduplication and compression mechanisms: These are all very important in restricted environments.

5. Data reliability is another important criterion for the IoT era to succeed immensely. That is, the timeliness and trustworthiness of IoT data need to be guaranteed in order to arrive at correct decisions. Any kind of ambiguity, internal misrepresentation, external manipulation, and so on of data lands in irreparable risks. There are evidence and belief theories extensively discussed and discoursed for enhancing the quality of captured sensor data.

6. Device security is emerging as a top trend for researchers to unearth ground breaking inventions and innovations for ensuring foolproof, impenetrable, and utmost security for devices

and their data.

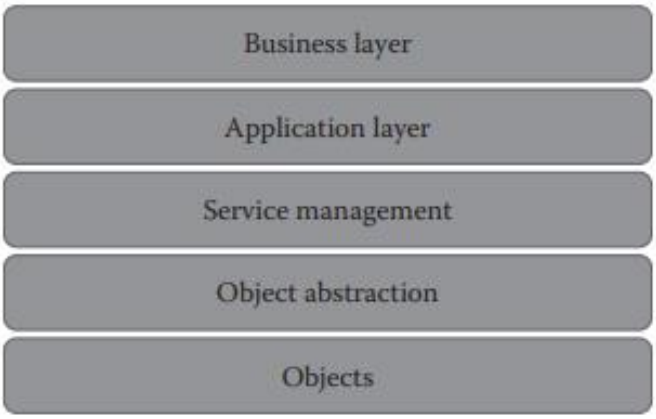
Thus, there are innumerable fresh opportunities and possibilities with a comity of interesting and inspiring upgrades in the IoT technology and tool landscapes.

Layered Architecture for IoT

There is no standard architecture for the IoT ecosystem. A reference architecture we are going to use is shown in following figure.

The different layers are as follows:

- Objects layers
- Object abstraction layer
- Service management layer
- Application layer
- Business layer



Layered architecture for IoT.

Objects Layer:

Objects layer, also known as devices layer, comprises the physical devices that are used to collect and process information from the IoT ecosystem. Physical devices include different types of sensors such as those that are typically based on micro-electromechanical systems (MEMS) technology. Sensors could be optical sensors, light sensors, gesture and proximity sensors, touch and fingerprint sensors, pressure sensors, and more. Standardized plug and play mechanisms should be used by the objects layer in order to integrate and configure the heterogeneous types of sensors that belong to the IoT device ecosystem. The device data that are collected at this layer are transferred to the object abstraction layer using secure channels.

Object Abstraction Layer

This layer transfers data that are collected from objects to service management layer using secure transmission channels. Data transmission can happen using any of the following technologies:

- RFID
- 3G
- GSM
- UMTS
- Wi-Fi

- Bluetooth low energy
- Infrared
- ZigBee

Specialized processes for handling functions such as cloud computing and data management are also present in this layer.

Service Management Layer:

This layer acts as middleware for the IoT ecosystem. This layer pairs specific services to its requester based on addresses and names. This layer provides flexibility to the IoT programmers to work on different types of heterogeneous objects irrespective of their platforms. This layer also processes the data that are received from the object abstraction layer. After data processing, necessary decisions are taken about the delivery of required services, which are then done over network wire protocols.

Application Layer:

This layer provides the diverse kinds of services requested by the customer. The type of service requested by the customer depends on the specific use case that is adopted by the customer. For example, if smart home is the use case under consideration, then the customer may request for specific parameters such as heating, ventilation, and air conditioning (HVAC) measurements or temperature and humidity values.
This layer provides the various types of smart services, which are offered by various IoT verticals. Some of the prominent IoT verticals are as follows:

- Smart cities
- Smart energy
- Smart health care
- Smart buildings or homes
- Smart living
- Smart transportation
- Smart industry

Business Layer:
This layer performs the overall management of all IoT activities and services. This layer uses the data that are received from the network layer to build various components such as business models, graphs, and flowcharts. This layer also has the responsibility to design, analyze, implement, evaluate, and monitor the requirements of the IoT system. This layer has the capability to use big data analysis to support decision-making activities. This layer also performs a comparison of obtained versus expected outputs to enhance the quality of services.

IoT vs M2M
M2M describes the technology that enables the communication between two or more machines. With M2M, one could connect machines, devices, and appliances in a wired or wireless fashion via a variety of communications techniques to deliver services with limited human intervention.

The difference between machine to machine (M2M) and IoT can be confusing to many. In fact, the misconception that M2M and IoT are the same has been a continuing subject of debate in the realm of tech industry.

Both M2M and IoT are connectivity solutions that provide remote access to machine data. They both have the capability of exchanging information among machines without human intervention. Thus, the two terms have been mistakenly interchanged often. However, M2M is a predecessor to IoT and had revolutionized enterprise operations by enabling them to monitor and manage their machines and hardware components remotely. M2M set the underlying basis

of machine connectivity on which IoT built upon. Nevertheless, IoT is the ultimate manifestation when it comes to connectivity.

The main objective of M2M is to connect a machine/device to another machine (typically in an industrial setting) via cellular or wired network so that its status can be monitored and its data can be collected, remotely. IoT is more of a universal market technology that aims at serving consumers, industries, and enterprises. Consumer IoT connects users to their devices and enables remote access. On the other hand, enterprise and industrial IoT take it further by allowing tracking, control, and management. IoT and M2M diverge immensely when it comes to the way they access devices remotely. M2M relies on point-to-point communications enabled by dedicated hardware components integrated within the machine. The communication among these connected machines is made possible via wired or conventional cellular network and dedicated software. IoT, on the other hand, typically uses IP networks and integrates web applications to interface device/machine data to a middleware, and in the majority of cases, to cloud. It is worth noting that IoT is intrinsically more scalable than M2M since cloudbased architectures do not need additional hard-wired connections and subscriber identification modules (SIM) which are required in M2M.

Machine-to-Machine (M2M) and Internet of Things (IoT) are both connectivity solutions for remote access to machine data, often confused due to their similarities. M2M is the precursor to IoT and paved the way for connecting and managing machines remotely. IoT is a broader technology that serves consumers, industries, and enterprises.

M2M primarily aims to connect machines within an industrial setting through cellular or wired networks, allowing remote monitoring and data collection. IoT, on the other hand, caters to a wide range of markets, including consumers, industries, and enterprises, providing remote access and control.

The key difference lies in how they access devices remotely. M2M relies on point-to-point communications with dedicated hardware components integrated into the machines, often using wired or conventional cellular networks. IoT, in contrast, predominantly uses IP networks and web applications to interface with device data, often connecting to cloud-based systems. IoT is more scalable, as it doesn't require additional hard-wired connections and subscriber identification modules (SIM) like M2M.