**Dr.SNS RAJALAKSHIMI COLLEGE OF ARTS AND SCIENCE**



**INTRODUCTION OF INTERNET OF THINIGS**

**UNIT-I**

**Chapter-1**

**1.1. Evolution and progression of internet of things**

Internet of things is an ecosystem of connected devices that exchanges data over a wired or wireless network. These devices could be smartphones, laptops, smart electric appliances, smart office equipment or any device tagged with sensors. Data generated by these devices is then shared with servers located in cloud or on-premise, where it is processed to gain insights that help in taking decisions. The iot ecosystem can be established not only within small areas like our homes or office but over larger areas like gated communities, university campus and cities.

Smart devices that connect with each other are ubiquitous part of our lives. As an individual user or business owner providing iot related products and services, it makes sense to understand evolution of iot. Knowledge of past equips us to foresee the future and use any technology to our advantage.

As a child grows every day and amazes their parents every moment, but still there are some moments that become milestones in their life history. Let us attempt to chronicle such milestone moments in the evolution of iot:

Arpanet was the first connected network – granddad of the internet as we know it today. The history of iot starts with arpanet.

In 1982, a graduate student in carnegie mellon university’s computer science department, david nichols, wanted to know if the department’s coke vending machine had cold soda bottles. He was tired of going to the machine only to find there was no cold bottle available; the vending machine was quite some distance from his classrooms. So, he wanted to have information beforehand.

He was helped in this endeavour by mike kazar and ivor durham, two fellow students, and john zsarnay, a research engineer at the university. The code they wrote could check if coke was available in the vending machine, and if yes, whether it was cold or not. Anyone on the university arpanet could monitor the status of the coke vending machine.

In 1989 tim berners lee proposed the framework of world wIDE web, which laid the foundation of the internet.

In 1990 john romkey developed a toaster that could be turned on and off over the internet. It was a toaster wired to the computer as there was no wi-fi then!! This toaster is consIDEred to be the first iot device – the first “thing” that began internet of things.

Researchers and scientists seem to have a thing for caffeine – cold or hot. In 1993, the trojan room coffee pot was built in the computer laboratory of the university of cambridge by quentin stafford-fraser and paul jardetzky in 1993. An image of the interior of the pot was uploaded to the building server thrice every minute. Later on, when browsers began displaying images, these images could be viewed online.

The next milestone in development of iot came in 1999 when kevin ashton, current executive director of the auto-id labs, [coined the term internet of things](https://www.techaheadcorp.com/blog/internet-of-things-guide/). It was the title of a presentation he made at procter and gamble (where he was working at that point of time) about linking rfid in p&g’s supply chain to the internet.

The term iot began to be used in mainstream publications like the guardian and scientific american by 2003-2004. In the same period rfid deployed by the us department of defence and by walmart in its stores.

The united nations international telecommunications union acknowledged the impact of iot in its report in 2005. It predicted that iot will help create an entirely new dynamic network of networks.

In march 2008, the first iot conference was held in zurich. It brought together researchers and practitioners from both academia and industry to facilitate sharing of knowledge. In the same year, the us national intelligence council included the internet of things as one of the six disruptive civil technologies.

In its 2011 white paper, cisco internet business solutions group (cibsg) said that internet of things can truly be said to be born between 2008 and 2009 when the number of things connected to the internet exceeded the number of people connected to it. Cibsg calculated that the things to people ratio grew from approximately 0.8 in 2003 to 1.84 in 2010.

Together with the white paper, cisco released many educational materials on the topic and started marketing initiatives to attract clients looking to adopt iot. Ibm and ericsson joined the race soon after.

In 2011 gartner included iot in its hype cycle for emerging technologies that were on the rise.

In 2013 idc released a report that predicted iot market to grow at a cagr of 7.9% and reach usd 8.9 trillion by 2020.

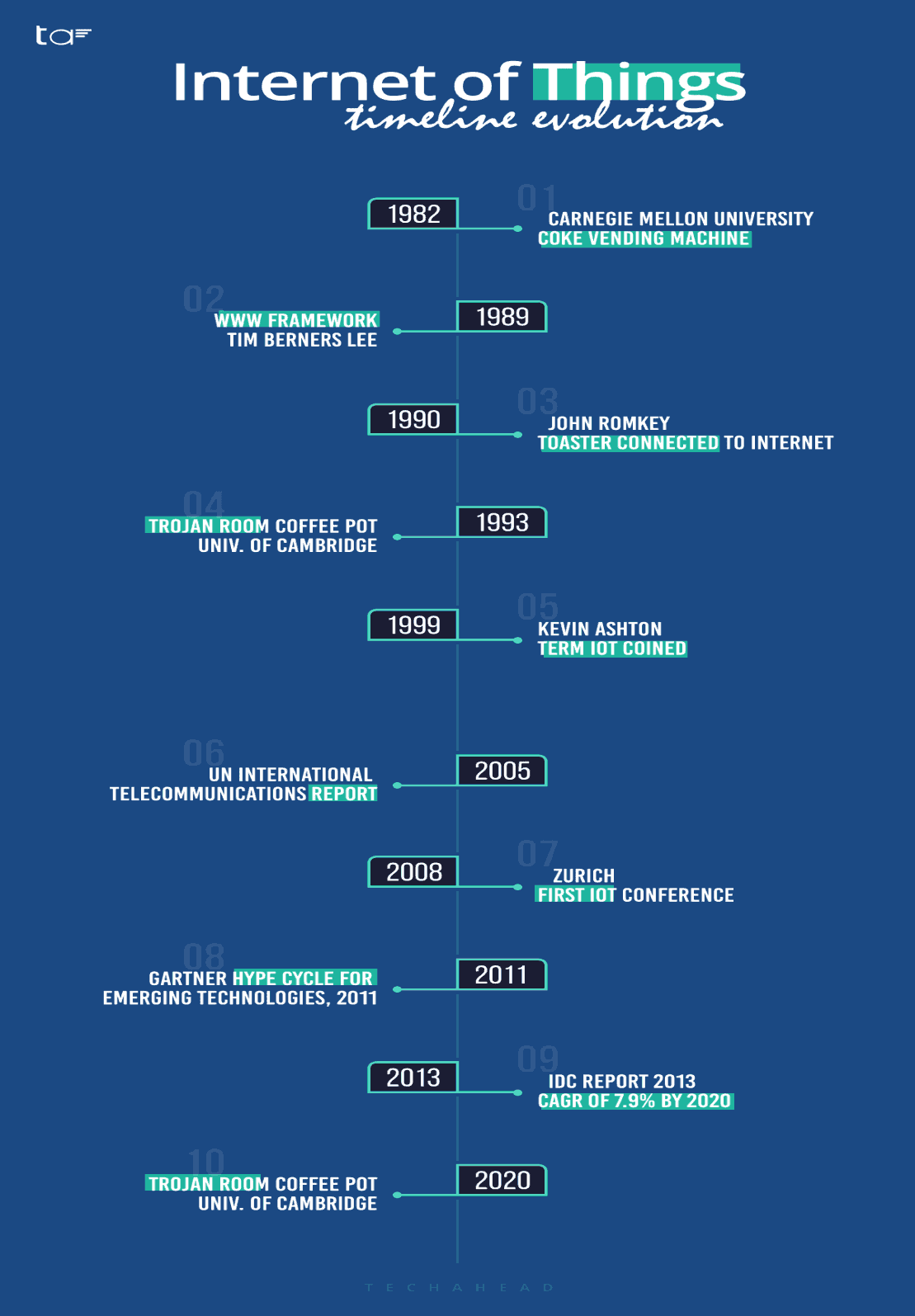


Figure: 1.1

**1.2. Genesis of iot:**

The concept of adding sensors and intelligence to physical objects was first discussed in the 1980s, when some university students decIDEd to [modify a coca-cola vending machine](https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/) to track its contents remotely. But the technology was bulky and progress was limited.

The [term ‘internet of things’ was coined in 1999](https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/#:~:text=Kevin%20Ashton%20is%20an%20innovator,and%20Discovery%2C%20out%20January%2020.) by the computer scientist kevin ashton. While working at procter & gamble, ashton proposed putting radio-frequency IDEntification (rfid) chips on products to track them through a supply chain.

He reportedly worked the[then-buzzword ‘internet’ into his proposal](https://www.verdict.co.uk/history-of-iot/) to get the executives’ attention. And the phrase stuck.

Over the next decade, public interest in iot technology began to take off, as more and more connected devices came to market.

In 2000, lg announced the first smart refrigerator, in 2007 the first iphone was launched and by 2008, the number of connected devices exceeded the number of people on the planet.

In 2009, google started testing driverless cars and in 2011, google’s nest smart thermostat hit the market, which allowed remote control of central heating.

**1.2.1. Iot and digitization:**

Digital transformation (dt) is all about data. While you can find many convoluted definitions for dt, the easiest way to think about it is that it enables companies to use customer data directly to drive their business. In a real sense, it enables companies to get closer to their customers.

Digital transformation for traditional companies is abstract because there’s nothing solid to anchor it to. So how does a traditional company transform into a company able to reap the rewards of digital transformation?

Their first step is to establish a digital link between their customers and their company, which can happen with the internet of things (iot). Iot technology starts with connectivity, but its digitization where things get interesting. All companies, big and small, can transform into digital companies by using an iot platform able to digitize their physical products.

This move to digitization is being led by some of the biggest companies out there. Pressures exerted by their more digitally-native competitors have led virtually all traditional fortune 500 companies to digitize at least some of their product lines so that they can be online and operating digitally native products.

this pressure to transform is not limited to the biggest companies, however. Timing is everything, and it’s no different in digital transformation. The more digital a company, the more competitive it is. The spoils of competitive advantages go to the first movers in each market.

Iot-based digital transformation is applied to physical products. For the traditional company, that’s terra firma selling products is how they make money, the reason for everything else. And because it’s aligned with its culture, iot-based digital transformation is both understandable and exciting enough to motivate employees to get behind it.

Central to both digital transformation and iot is data. When applied properly, iot technology collects source data from the physical world and converts it into useful information for the company.

Internal source data starts at the sensor. Converting that data into a digital payload, and then wrapping it with protocols so it can be sent on the network, is the work of a software agent that lives on the embedded system. This is the edge of the iot network, from which the data payload is gathered and sent over the operational technology network to the it network. From there, the data makes its way to the public cloud and then into a database, where it can be processed by analytics software or artificial intelligence. This processing creates models that produce information that is stored in the company’s business systems which various departments within the company can access and use to streamline and improve how they operate.

This process performed by the iot platform is what drives digital transformation. The iot platform that enables the digitization of physical products and the collection of their data also provIDEs the digital link between a company and its products and customers.

The most obvious data to collect from the product is about the product itself. A product’s utility, usability, and performance can be modelled and compared with its actual use resulting in innovations that improve products and lead to the creation of new ones.

**1.2.3.iot (internet of things) enabling technologies are:**

1. Wireless sensor network
2. Cloud computing
3. Big data analytics
4. Communications protocols
5. Embedded system

**Wireless sensor network (wsn):**

A **wsn** comprises distributed devices with sensors which are used to monitor the environmental and physical conditions. A **wireless sensor network** consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects wsn to the internet.  
Example –

* Weather monitoring system
* Indoor air quality monitoring system
* Soil moisture monitoring system
* Surveillance system
* Health monitoring system

**Cloud computing:**

It provIDEs us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations.  
With cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.

**ProvIDEs different services, such as**

**Iaas (**infrastructure as a service**)**

Infrastructure as a service provIDEs online services such as physical machines, virtual machines, servers, networking, storage and data centre space on a pay per use basis. Major iaas provIDErs are google compute engine, amazon web services and microsoft azure etc.   
Ex: web hosting, virtual machine etc.

**Paas (**platform as a service**)**

ProvIDEs a cloud-based environment with a very thing required to support the complete life cycle of building and delivering west web based (cloud) applications – without the cost and complexity of buying and managing underlying hardware, software provisioning and hosting. Computing platforms such as hardware, operating systems and libraries etc. Basically, it provIDEs a platform to develop applications.  
Ex: app cloud, google app engine

**Saas** **(**software as a service**)**

It is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management.  
Saas applications are sometimes called web-based software on demand software or hosted software.

Saas applications run on a saas provIDEr’s service and they manage security availability and performance.  
Ex: google docs, gmail, office etc.

**Big data analytics:**

It refers to the method of studying massive volumes of data or big data. Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases.  
Big data is gathered from a variety of sources including social network vIDEos, digital images, sensors and sales transaction records.  
Several steps involved in analysing big data –

* + - Data cleaning
    - Munging
    - Processing
    - Visualization

**Examples**

Bank transactions

Data generated by iot systems for location and tracking of vehicles

E-commerce and in big-basket

Health and fitness data generated by iot system such as a fitness bands

**Communications protocols:**

They are the backbone of iot systems and enable network connectivity and linking to applications. Communication protocols allow devices to exchange data over the network. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.  
They are used in

Data encoding

Addressing schemes

**Embedded systems:**

It is a combination of hardware and software used to perform special tasks.  
It includes microcontroller and microprocessor memory, networking units (ethernet wi-fi adapters), input output units (display keyword etc.) And storage devices (flash memory).  
It collects the data and sends it to the internet.  
Embedded systems used in

**Examples –**

Digital camera

Dvd player, music player

Industrial robots

Wireless routers etc.

**1.3. Iot architectures:**

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

**Sensing layer –**

The sensing layer is the first layer of the iot architecture and is responsible for collecting data from different sources. This layer includes sensors and actuators that are placed in the environment to gather information about temperature, humidity, light, sound, and other physical parameters. These devices are connected to the network layer through wired or wireless communication protocols.

**Network layer –**

The network layer of an iot architecture is responsible for providing communication and connectivity between devices in the iot system. It includes protocols and technologies that enable devices to connect and communicate with each other and with the wIDEr internet. Examples of network technologies that are commonly used in iot include wi-fi, bluetooth, zigbee, and cellular networks such as 4g and 5g. Additionally, the network layer may include gateways and routers that act as intermediaries between devices and the wIDEr internet, and may also include security features such as encryption and authentication to protect against unauthorized access.

**Data processing layer –**

The data processing layer of iot architecture refers to the software and hardware components that are responsible for collecting, analysing, and interpreting data from iot devices. This layer is responsible for receiving raw data from the devices, processing it, and making it available for further analysis or action. The data processing layer includes a variety of technologies and tools, such as data management systems, analytics platforms, and machine learning algorithms. These tools are used to extract meaningful insights from the data and make decisions based on that data. Example of a technology used in the data processing layer is a data lake, which is a centralized repository for storing raw data from iot devices.

**Application layer –**

The application layer of iot architecture is the topmost layer that interacts directly with the end-user. It is responsible for providing user-friendly interfaces and functionalities that enable users to access and control iot devices. This layer includes various software and applications such as mobile apps, web portals, and other user interfaces that are designed to interact with the underlying iot infrastructure. It also includes middleware services that allow different iot devices and systems to communicate and share data seamlessly. The application layer also includes analytics and processing capabilities that allow data to be analysed and transformed into meaningful insights. This can include machine learning algorithms, data visualization tools, and other advanced analytics capabilities.

**1.3.1. One m2m:**

Onem2m brings together all components in the iot solution stack. It avoids reinvention in favor of reusing existing technology components and standards. Onem2m's architecture defines a common middleware technology in a horizontal layer between devices and communications networks and iot applications.

This standardizes links between connected devices, gateways, communications networks and cloud infrastructure. It allows developers to mix and match components from different vendors.

Onem2m is a general-purpose standard that applies to all industry verticals. This ensures a high degree of re-use. It also means that vertical applications can interoperate with one another. This ability to work across application silos adds significant value and promotes innovation

The architecture standardised by onem2m defines an iot service layer, i.e. A vendor-independent software middleware between processing and communication hardware and iot applications providing a set of functions commonly needed by iot applications. The onem2m service layer provIDEs use case-independent functions.

• onem2m common service layer functions (csf’s) provIDE proper:

• IDEntification of users and applications

• authentication and authorization of users and applications

• end-to-end data encryption

• remote provisioning and service activation

• device management

• connectivity setup and data transmission scheduling

• data aggregation, buffering in case of missing connectivity and synchronisation upon connectivity re-establishment

• group management and application and data discovery functions

The functions listed above provIDEd by the onem2m common service layer, are exposed and controlled via globally standardized vendor-independent and uniform apis, towards the iot applications.

Iot applications or more generically “application entities” ae’s are generic terms for applications executed in so-called application dedicated nodes adns or middle nodes mns and at the infrastructure node in.

Applications (aes) at the device (adn, mn) and the infrastructure platform (in) are separated by the onem2m apis from the actual onem2m common service functions (csfs) like the ones listed above.

Details and specifics of the underlying - connectivity technologies, transport protocols and data serialisation formats are not exposed to the application developer. This avoids the necessity of detailed expertise in used connectivity technologies, and hence allows the application developer to focus on the actual customer iot application.

Interactions between onem2m common service functions (csfs) and the application are solely based on the onem2m globally standardised, vendor independent, uniform apis towards the applications.

For an application developer, onem2m based technology appears like an operating system, which takes over common basic functions in context of connectivity and hardware as listed above. Hence the iot service layer specified by onem2m can be seen in a similar way as a mobile operating system within the smart phone eco system.

Due to this separation, application developers can focus on developing the actual iot application for the device e.g focusing on:

• measuring physical parameters, pre-processing of data, controlling attached hardware or interworking with other technologies (modbus, can-bus, opc-ua gateways, etc.) On the infrastructure (platform) the separation by apis between onem2m csfs and applications, enables a separation between “low level” tasks in context of connectivity over wIDE area networks (device management, scheduling of data transmission, enrolment of security functions and credentials, revocation of faulty device applications), and actual cloud and iot application platforms like:

• data analytics, rule engines, presentation of data, user interfaces, etc.

Compared to iot devices being connected to iot platforms without onem2m, the separation between applications and onem2m csfs, enables the device to become independent from the actual cloud respective iot application platform provIDEr. Beneficially the onem2m csfs will become part of the communication chipset to achieve coverage in a wIDE range of devices.

**1.3.2. Iot world forum (iotwf):**

The 9th IEEE world forum on internet of things (IEEE wfiot2023) is the premier event of the IEEE iot technical community, a multiple society initiative aggregating the wIDE expertise inherent to the iot domain. This year, the theme for wfiot 2023 is "the blue planet: a marriage of sea and space”.

Iot architecture can comprise up to seven layers, which are known as the perception, transport, edge, processing, application, business, and security layers.

**Perception layer:**

The perception layer of an iot system architecture, also known as the device layer, consists of multiple elements – sensors, cameras, actuators, and similar devices that gather data and perform tasks.

For example, an [iot sensor](https://dgtlinfra.com/internet-of-things-iot-sensors/" \t "_blank) used on an automotive assembly line can conduct a quality control check on a nearby robot. Each time the robot assembles a fuse box, the iot sensor checks whether the robot has placed the fuse in the correct position by detecting the colour coding of the different fuses**.**

**Transport layer:**

The transport layer of an iot system architecture transmits data from multiple devices (e.g., on-site sensors, cameras, actuators) to an on-premise or cloud data centre.

As a first step, iot gateways must convert the incoming input from analog to digital format. Next, the gateway may employ any one of a range of data transfer protocols (dtps) to transmit the data to an on-premise or cloud data centre.

**Edge layer:**

As iot networks grow in scale, latency becomes one of the main performance challenges, as numerous devices connecting to a hub end up congesting the network. By enabling data processing and analysis as close to the source as possible, edge computing addresses these problems – which is handled through the edge layer of an iot system architecture.

One feature that all iot edge devices have in common is that they are capable of transmitting what they detect, in the form of data packets, to nodes that then process the data further. Some ‘smart’ edge devices are additionally programmed to halt the target process – or initiate some damage control measure – upon detecting a serious anomaly.

**Processing layer:**

A fundamental component of an iot system architecture is its processing layer, also called the middleware layer, which typically leverages many connected computers simultaneously, in the form of [cloud computing](https://dgtlinfra.com/cloud-internet-of-things-iot/), to deliver superior compute, storage, networking, and security performance.

Particularly, the processing layer within an iot system architecture is responsible for analysing input data to generate new insights, useful predictions, and timely warnings.

An iot system typically handles huge volumes of data, generated by numerous edge devices, at multiple sites on the edges of the network. The ‘middleware’ of the processing layer utilizes a three-stage approach to prepare this data for the application layer:

**Data accumulation:**

Middleware correctly IDEntifies and assigns different data types to the appropriate storage. Unstructured data, such as audio and vIDEo streams and images, typically require more storage space and are [housed in data lakes](https://dgtlinfra.com/data-lake-cloud-aws-azure/). Whereas structured data, comprising instrument readings, log values, and measurements (telemetry data) are more space-efficient and are stored in data warehouses

**Data abstraction:**

Involves aggregating data from multiple sources, as well as ensuring that data is converted into a format that can be “read” by the software of the application layer

**Data analysis:**

Employs machine learning (ml) or deep learning algorithms, which are specialized in detecting patterns within large and seemingly random data sets

**Application layer:**

The application layer of an iot system architecture involves decoding promising patterns in iot data and compiling them into summaries that are easy for humans to understand, such as graphs and tables. Programs for device control and monitoring, as well as process control software, are typical examples of the application layer of iot architecture.

**Business layer:**

Patterns decoded at the application level can be used to further distill business insights, project future trends, and drive operational decisions that improve the efficiency, safety, cost-effectiveness, customer experience, and other important aspects of business functionality. Indeed, all of this can be accomplished at the business layer of an iot system architecture.

**Security layer:**

Security is one of the most important requirements for an iot system architecture. Ironically, it also happens to be one of the key challenges facing iot architecture, and iot devices themselves. Broadly, the iot security layer comprises three main aspects:

**Equipment security:**

Involves the actual iot devices, and protecting these endpoints from malware and hijacks

**Cloud security:**

With most iot data being processed in the cloud, cloud security is crucial to prevent data leaks

**Connection security:**

Focused on securing data transmitted across networks, primarily with encryption. The transport layer security (tls) protocol is consIDEred the benchmark for iot connection security

**1.3.3 alternatives to wi-fi for iot connectivity:**



**Cellular connectivity** – also referred to as satellite connection is the wi-fi alternative to connect iot devices which is typically used when we talk about machine-to-machine (m2m) connectivity. It’s the same type of connectivity that we use to connect our smartphones and tablets and uses a broadcast tower to function typically within a range of around 10 – 15 miles.

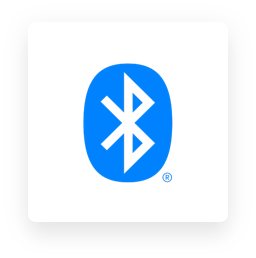


**Low power wIDE area network** (lpwan) is a fairly new contender in the iot network space, but it offers a lot in terms of breadth of coverage while still maintaining low power consumption. Lpwan does this by using small, cheap batteries to power its connectivity.



**Zigbee** - another popular alternative to wi-afi iot networks and connectivity. It works using a mesh network structure connecting a host of sensors or devices so that they work seamlessly together to distribute data to the chosen device. With a mesh network, all iot devices in the system are able to distribute signals and information around the network.

Designed especially for iot, zigbee can connect up to 65,000 devices in its mesh and is already supported by mainstream iot devices such as amazon echo.



**Bluetooth:** most of us are familiar with the concept of bluetooth having used it on our phones for the last decade. Bluetooth enables users to send data across short distances using wireless technology.

In recent years, bluetooth has improved drastically in terms of power consumption. Where before it could flatten a battery fairly easily, today’s bluetooth connections run on a fairly low-power model.

Bluetooth had a competitive bandwidth of 2mbps but only has low range capabilities of below 30ft (10m).

Bluetooth iot network connectivity is a great option if you’re looking to send information across a close range, with medium to low bandwidth.



**Z-wave**: runs on a radio-frequency (rf) based connection. Unlike zigbee, however, z-wave usually needs to run via a central hub, which can mean the connection is interrupted with latency issues and a limited coverage range.

It’s worth noting that z-wave is slightly slower than zigbee but does have a more impressive coverage range (of more than 30 feet).

Z-wave uses a 908 mhz band to operate, which enables an increase in coverage range as well as reducing the likelihood of interference. When placed next to each other, z-wave is typically more reliable than zigbee but z-wave is supported on far fewer devices.

**1.4. Simplified iot architecture:**

Iot architecture consists of the devices, network structure, and cloud technology that allows iot devices to communicate with each other. A basic iot architecture consists of three layers

The internet of things (iot) describes physical objects embedded with sensors and actuators that communicate with computing systems via wired or wireless networks—allowing the physical world to be digitally monitored or even controlled.

The iot devices include wireless sensors, software, actuators, computer devices and more. They are attached to a particular object that operates through the internet, enabling the transfer of data among objects or people automatically without human intervention.

One example is the automotive industry, which uses iiot devices in the manufacturing process. The automotive industry extensively uses industrial robots, and iiot can help proactively maintain these systems and spot potential problems before they can disrupt production.

Iot architecture consists of the devices, network structure, and cloud technology that allows iot devices to communicate with each other. A basic iot architecture consists of three layers: perception (the sensors, gadgets, and other devices) network (the connectivity between devices)

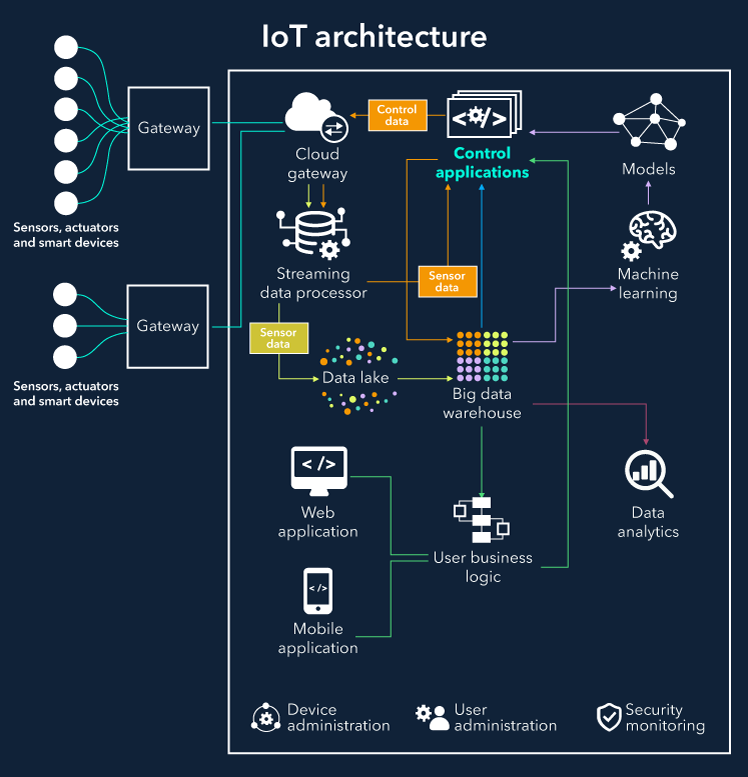


Figure 1.2

**1.4.1. Core iot functional stack:**

The stack comprises five layers: devices, communications, protocols, cloud platform, and applications. Knowing the key terminology used to describe each of these layers will help you understand how the iot works and make it easier to find the right solution for your needs.

The “internet of things” (iot) is a term for the network of physical objects connected to the internet. These objects can include anything from home appliances, wear ables, factory equipment and vehicles. The iot can radically improve how we live, work and play.

However, several different technologies need to work together for the iot to reach its full potential. This is where the iot technology stack comes in.

Knowing the terms that make up the stack and how they work together can help you to understand the iot.

In this article, we’ll look at the different layers of the iot stack and some of the technologies used at each level.

The iot technology stack refers to the multiple layers of hardware, software and communication technologies that connect objects over the internet to monitor or control them. The following layers make up the iot technology stack:

**Layer 1: device hardware**

The first layer of the iot stack is the device hardware that acts as the interface between the physical object and the server (cloud or on-premise).

Collecting of the data from individual or multiple sensors requires the appropriate type of processor and suitably rated electrical interfaces. This can be as simple as a microcontroller or as complex as an industrial computer.

The device hardware runs the device software and may also include additional sensors, actuators and other input/output (i/o) components.

Sensors measure physical parameters, such as temperature, humidity, pressure or vibration. Actuators can be used to control devices, such as motors, pumps, heaters or lights.

Other i/o components may include buttons, displays or speakers.

If the object or sensors that are to become a ‘connected device’ lack the suitable processing requirements, then a single board computer (sbc) combined with an appropriate interface cape may be installed as an embedded device.

An sbc and appropriate interface cape can also be used when there is no easy way of connecting the machine via a port (e.g. Rs232) and no industrial standard communication protocol is used.

**Layer 2: device software**

The second layer of the iot stack is the device software. This code runs on the device’s processor and controls its functionality.

Device software typically consists of an operating system (os) and application software.

The os configures and manages the device’s hardware to provIDE a platform for the application software to run on.

Common open source and licenced embedded operating systems include bare metal rtos, free rtos, vxworks, qnx and embedded linux.

Application software uses the os’s interfaces to give the device its specific functionality. For example, an application might be used to control a motor, read sensor data and transmit live or periodic status reports over a wired or wireless connection.

In the iot world the use of open source software offers immense flexibility and adaptability as business needs and technologies evolve.

**Layer 3: communications**

The third layer of the iot stack is communications. This is how devices connect to the internet and transfer data.

When there is a requirement for devices to communicate with each other, they need to be able to speak the same language. This is where communication protocols come in and come in many different standards published for reference when implementing a new product or service.

Protocols are like rules for how data should be formatted and transmitted. Standard protocols used in the iot include mqtts, https and coap.

**Layer 4: cloud platform**

The fourth layer of the iot stack is the cloud platform. This is the hardware and software services located in internet-based data centres. It is where the data from iot devices is recorded, captured, processed, analysed and stored.

Cloud computing in iot offers a centralised service containing computing resources and databases that can be accessed whenever from wherever.

Unlike on-premise alternatives, the cloud offers ease of scalability in terms of infrastructure capacity and the of device data.

Cloud platforms usually provIDE tools and services that make it easier to develop and deploy iot applications.

With iot services it is advised to compare the total cost of ownership (tco) when it comes to hosting and running the iot services in the cloud:

**Layer 5: cloud applications**

The fifth and final layer of the iot stack is cloud applications. These applications run on top of the cloud platform and provIDE the end-user with a way to interact with the iot system.

Cloud applications include the user interfaces of dashboards, reporting suites, analytical and artificial intelligence modules. They can be used to view data from sensors and control actuators embedded in static or mobile machinery, plant or fleets of vehicles.

**Iot technology stack diagram:**

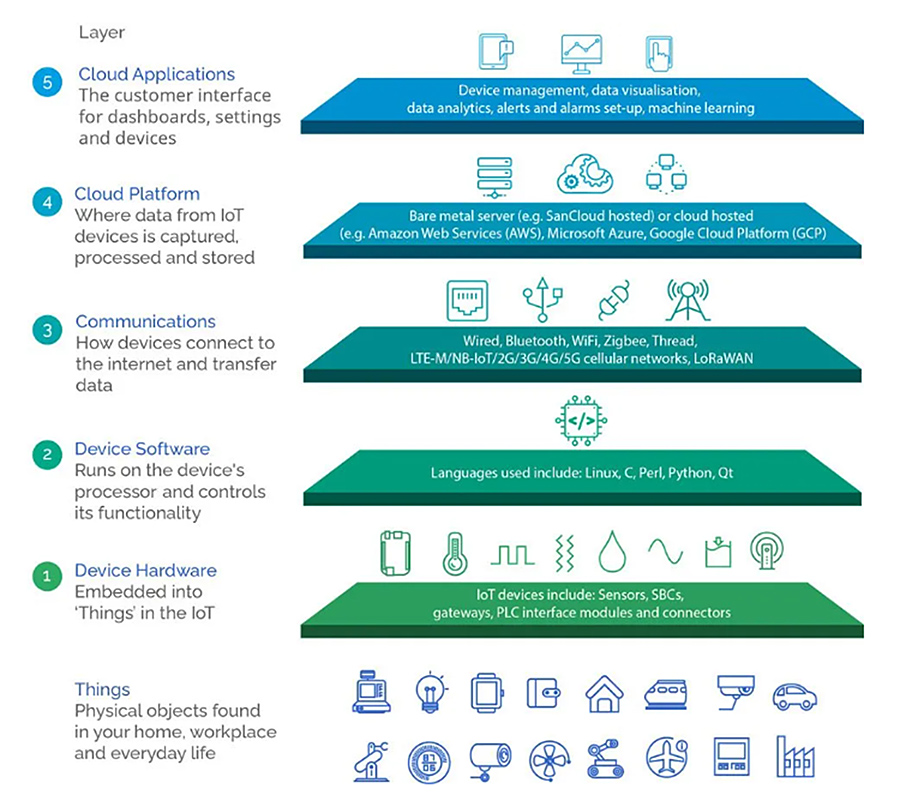
[](https://i0.wp.com/iotbusinessnews.com/WordPress/wp-content/uploads/2022/07/IoT-technology-stack-diagram.jpg?ssl=1)

Figure 1.3

**1.5. Fog, edge and cloud in iot:**

**1.5.1. Cloud**

Most businesses are familiar with cloud computing since it’s now the golden standard in most industries. Put simply, cloud computing stands for storing and accessing data and programs over the internet, rather than on your computer’s hard drive. For it to be consIDEred ‘cloud computing’, you need to access your data or your programs over the internet, or have that data synced with other information over the web.

Cloud computing allows organisation to significantly exceed the normal available storage, without having to host extra servers on site. Data can also be collected from multiple sites and devices, accessible anytime, anywhere.

Fog and edge computing push both data and intelligence to analytic platforms that are situated either on, or close to where the data originated from. This helps to reduce latency cost and increase user experience. However, there are key differences between the two.

**1.5.2. Fog**

Fog computing – a term created by cisco – refers to extending cloud computing to the edge of an enterprise’s network. It pushes intelligence down to the local area network (lan) level of network architecture, processing data in a fog node or iot gateway. Simply put, it involves moving your computers closer to the sensors they are talking to.

One example of fog computing would be with trains. As part of the rise in the industrial internet of things, trains and tracks are being equipped with a new generation of gadgets and sensors, with trains acting as the central hub for all the data gathered from these sensors. The issue is that because trains move so fast, it’s difficult to maintain a connection with the cloud. By installing some fog computing nodes in the locomotive, you bypass this issue.

However, fog computing’s architecture relies on many links in a communication chain to move data from the physical world of our assets into the digital world of information technology. Each of these links is a potential point of failure.

**1.5.3. Edge**

Edge computing can be defined as the processing of sensor data away from the centralised nodes and close to the logical edge of the network, toward individual sources of data. It effectively pushes the computational functions to the edge of the network. In other words, rather than pumping all the data back up to the cloud for analysis and action, this process takes place much closer to the data’s source.

Edge computing triages the data locally, reducing the backhaul traffic to the central repository. It simplifies fog’s communication chain and reduces potential points of failure.

Edge devices can be anything with sufficient compute capacity and capability such as routers, switches and even the iot sensors collecting the data.

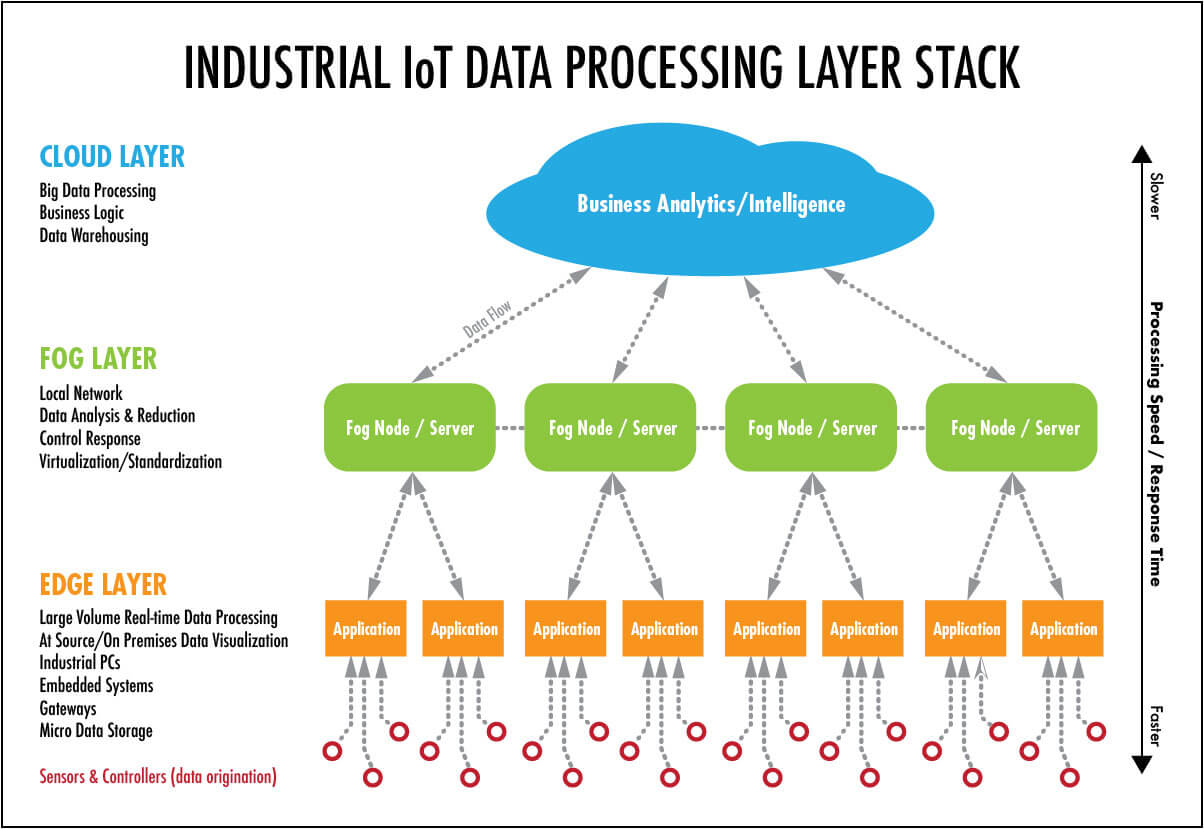


Figure 1.4

**1.6. Functional blocks of an iot ecosystem:**

The internet of things denotes the connection of devices, machines, and sensors to the internet. An iot system comprises four basic building blocks: sensors, processors, gateways, and applications. This article will thoroughly discuss what each component of the iot architecture represents.

**Sensors**

It convert a non-electrical input to an electrical signal. Sensors are classified into two types: active and passive sensors. Whereas active sensors use and emit their own energy to collect real-time data (ex.: gps, x-ray, radars), passive sensors use energy from external sources (ex: cameras). Additionally, sensors differentiate themselves by position, occupancy, and motion, velocity and acceleration, force, pressure, flow, humidity, light, radiation, temperature, etc.

**Processors**

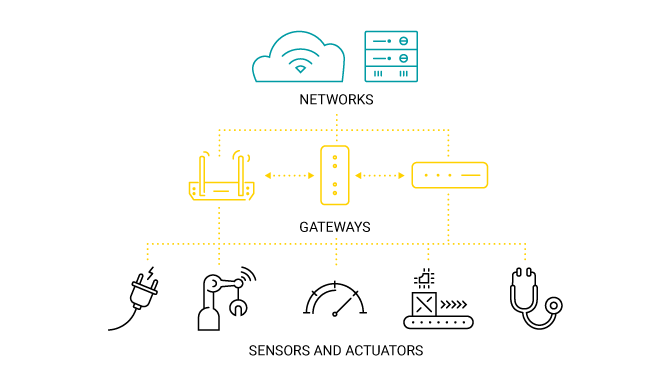
It is the brain, the main part of the iot system. They process the raw data captured by the sensors and extract valuable information. Examples of processors are microcontrollers and microcomputers.

**Gateways**

It is the combination of hardware and software used to connect one network to another. Gateways are responsible for bridging sensor nodes with the external internet or world wIDE web. The figure below depicts how using gateways works.

**applications**

It provIDE a user interface and effective utilization of the data collected.



**Figure1.5**

**1.7. Sensors**

Sensors are used for sensing things and devices etc.

A device that provIDEs a usable output in response to a specified measurement. The sensor attains a physical parameter and converts it into a signal suitable for processing (e.g. Electrical, mechanical, optical) the characteristics of any device or material to detect the presence of a particular physical quantity.

**types of sensors:**

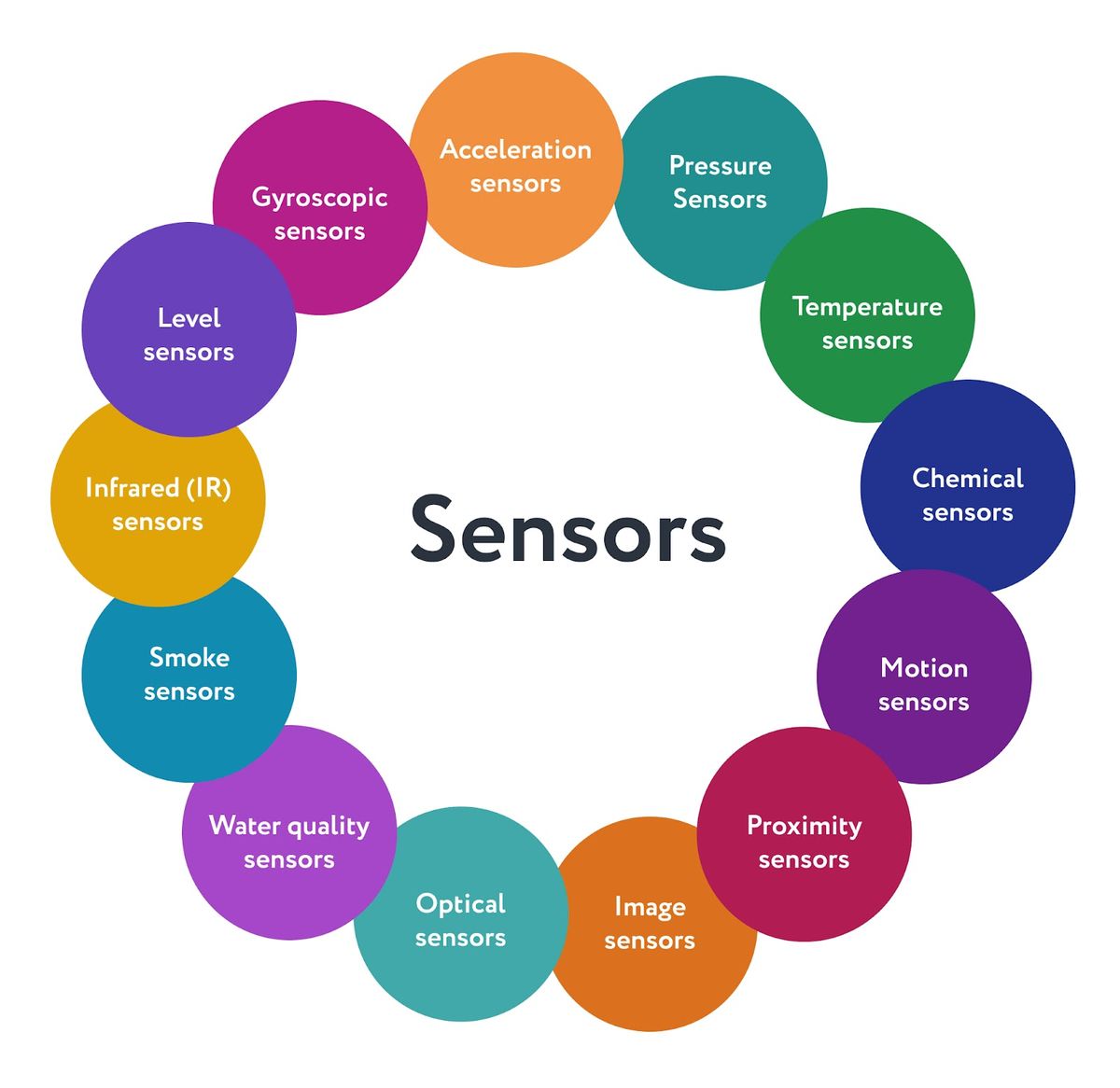


Figure 1.6

* Pressure sensors can sense changes of pressure in liquids and gasses, as well as measure force per unit area
* Temperature sensors can measure device or environment  temperature and detect how it changes
* Chemical sensors can detect the presence of chemical substances in the environment
* Motion sensors are able to detect the movement of a physical object
* Proximity sensors can determine how far an object is
* Water quality sensors can check the presence of chemicals in water, its oxygen and ph levels, as well as electrical conductivity
* Smoke sensors can detect presence of smoke on the premises
* Infrared (ir) sensors can measure the level of infrared radiation and heat
* Level sensors can be used to measure the level of liquids, powders, and granular materials in some tanks
* Image sensors can capture the images for their further processing and analysis
* Acceleration sensors can measure the acceleration of an object
* Gyroscopic sensors can determine an object's orientation, measuring its angular velocity
* Optical sensors can detect objects via the detection of light reflection

**1.7.1. Actuators:**

An [iot](https://www.geeksforgeeks.org/introduction-to-internet-of-things-iot-set-1/) device is made up of a physical object (“thing”) + controller (“brain”) + [sensors + actuators](https://www.geeksforgeeks.org/difference-between-sensor-and-actuator/) + networks (internet). An actuator is a machine component or system that moves or controls the mechanism of the system. Sensors in the device sense the environment, then control signals are generated for the actuators according to the actions needed to perform.

A servo motor is an example of an actuator. They are linear or rotatory actuators, can move to a given specified angular or linear position. We can use servo motors for iot applications and make the motor rotate to 90 degrees, 180 degrees, etc., as per our need.

The control system acts upon an environment through the actuator. It requires a source of energy and a control signal. When it receives a control signal, it converts the source of energy to a mechanical operation. On this basis, on which form of energy it uses, it has different types given below.

**Types of actuators:**

**Hydraulic actuators**

A hydraulic actuator uses hydraulic power to perform a mechanical operation. They are actuated by a cylinder or fluid motor. The mechanical motion is converted to rotary, linear, or oscillatory motion, according to the need of the iot device. Ex- construction equipment uses hydraulic actuators because hydraulic actuators can generate a large amount of force.

**Pneumatic actuators**

A pneumatic actuator uses energy formed by vacuum or compressed air at high pressure to convert into either linear or rotary motion. Example- used in robotics, use sensors that work like human fingers by using compressed air.

**Electrical actuators**

An electric actuator uses electrical energy, is usually actuated by a motor that converts electrical energy into mechanical torque. An example of an electric actuator is a solenoid based electric bell.

**Thermal/magnetic actuators**

These are actuated by thermal or mechanical energy. Shape memory alloys (smas) or magnetic shape‐memory alloys (msmas) are used by these actuators. An example of a thermal/magnetic actuator can be a piezo motor using sma.

**Mechanical actuators**

A mechanical actuator executes movement by converting rotary motion into linear motion. It involves pulleys, chains, gears, rails, and other devices to operate.

**1.8. Smart objects and connecting smart objects:**

The internet of things (iot) describes a vision in which everyday objects are connected to the internet, be identified and communicate with other devices. These objects are typically referred to as "smart objects." the aim is to digitizing applications and processes to make them easier and more efficient.

The concept of smart in iot is used for physical objects that are active, digital, networked, can operate to some extent autonomously, reconfigurable and has local control of the resources. The smart objects need energy, data storage, etc.

A smart object is an object that enhances the interaction with other smart objects as well as with people also. The world of iot is the network of interconnected heterogeneous objects (such as smart devices, smart objects, sensors, actuators, rfid, embedded computers, etc.) Uniquely addressable and based on standard communication protocols.

Smart objects are utilized wIDEly to transform the physical environment around us to a digital world using the internet of things (iot) technologies.

A smart object carries blocks of application logic that make sense for their local situation and interact with human users. A smart object sense, log, and interpret the occurrence within themselves and the environment, and intercommunicate with each other and exchange information with people.

The work of smart object has focused on technical aspects (such as software infrastructure, hardware platforms, etc.) And application scenarios. Application areas range from supply-chain management and enterprise applications (home and hospital) to healthcare and industrial workplace support. As for human interface aspects of smart-object technologies are just beginning to receive attention from the environment.



**Figure:1.7**

**1.8.1. Smart objects:**

It is an object that enhances interplay with not solely humans however also with different smart objects. Also recognized as smart connected products or smart connected things (scot), they are products, assets, and different matters embedded with processors, sensors, software program and connectivity that helps in permitting information to be exchanged between the product and its environment, and different products and systems. Connectivity additionally allows some abilities of the product to present outsIDE the physical device, in what is regarded as the product cloud. The records gathered from these products can be then analysed to inform decision-making, allow operational efficiencies, and constantly enhance the overall performance of the product.

Smart objects are an autonomous physical and/or digital object that have sensing, processing, and networking capabilities, and carry application logic.  They make sense of their local environment and interact with human users.

They sense, log, and interpret what’s occurring within themselves and the world, act on their own, intercommunicate with each other, and exchange information with people.

Smart objects are small computers with a sensor or actuator and a communication device, embedded in objects such as thermometers, car engines, light switches, and industry machinery.

Smart objects enable a wIDE range of applications in areas such as home automation, building automation, factory monitoring, smart cities, structural health management systems, smart grid and energy management, and transportation.

Until recently, smart objects were realized with limited communication capabilities, such as rfid tags, but the new generation of devices has bidirectional wireless communication and sensors that provIDE real-time data such as temperature, pressure, vibrations, and energy measurement.

Iot connected devices are creating a world in which data is exchanged between physical objects such as sensors, on-device software and adjacent technologies with other systems and devices. The essential enabling technology is the connection between the 'things' of iot which enables these exchanges to happen.

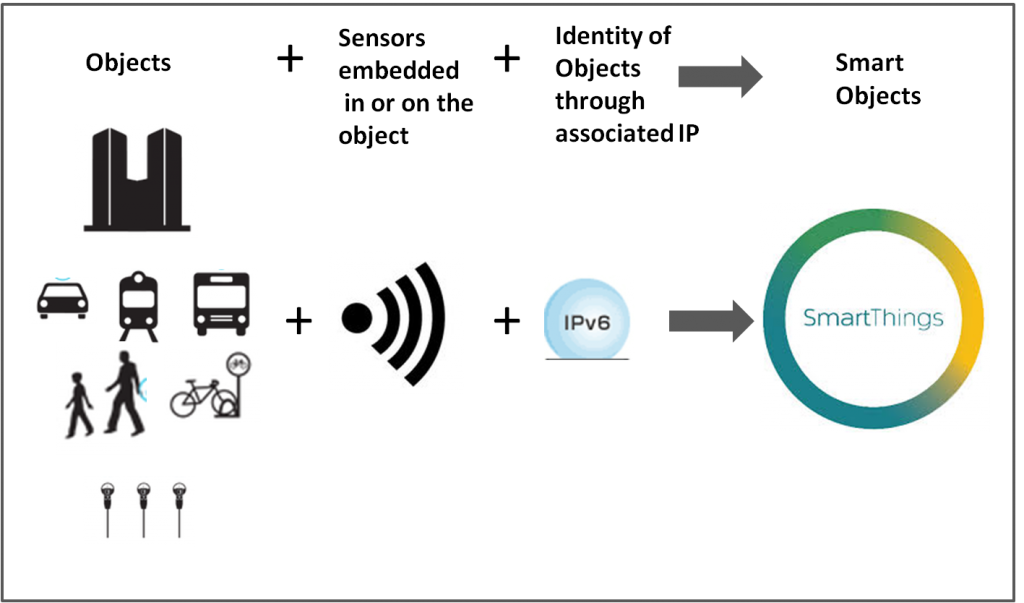


figure1.9