**Fundamentals of IoT**

**What is the Internet of Things?**

The Internet of Things (IoT) is a network of physical objects that actively collect, exchange and utilize data. Additionally, IoT devices use sensors to capture real-world data, and actuators to take physical actions. Data analytics techniques extract valuable insights from the data, enabling informed decision-making and optimization. Moreover, The dynamic nature of the IoT revolutionizes our interactions with technology and promises a future where objects intelligently interact, enhancing convenience, efficiency, and connectivity. The Internet of Things (IoT) uses multiple embedded systems to collect data about motion, temperature, and other aspects of the user’s environment. IoT is a great choice for businesses that want to offer better customer service. By creating devices that are aware of user requirements, businesses can improve accuracy, efficiency, and convenience. The concept of an intelligent home is achieved when all of these devices work together on IoT principles.

**Concepts of the Internet of Things**

The Internet of Things (IoT) is a network of physical objects that are embedded with sensors, software, and other technologies to collect and exchange data. These objects are referred to as “things” and can range from ordinary household objects to sophisticated industrial tools.

The IoT has the potential to revolutionize many industries and aspects of our lives. For example, it can be used to improve efficiency in manufacturing, track and manage assets, and provide better healthcare.

These objects can range from everyday devices like smartphones and smart appliances to complex systems such as industrial machinery and environmental monitoring devices. Understanding the concepts behind the Internet of Things is crucial to grasping its potential and implications. Let’s explore the key concepts in more detail:

* **Connectivity:** The IoT relies on the ability of physical objects to connect to the internet. This is made possible by the use of low-power, wide-area networks (LPWANs) such as Sigfox, LoRaWAN, and NB-IoT.
* **Sensing:** IoT devices are typically equipped with sensors that collect data about the environment. This data can be used to monitor conditions, track movement, and detect events.
* **Communication:** IoT devices need to be able to communicate with each other and with the cloud. This is typically done using standard protocols such as MQTT, CoAP, and HTTP.
* **Analytics:** The data collected by IoT devices can be analyzed to gain insights into the physical world. This data can be used to improve efficiency, optimize processes, and make better decisions.

**Technologies behind the Internet of Things**

The Internet of Things (IoT) relies on a diverse range of technologies that work together to enable its functionality and connectivity. Let’s explore the key technologies that underpin the Internet of Things.

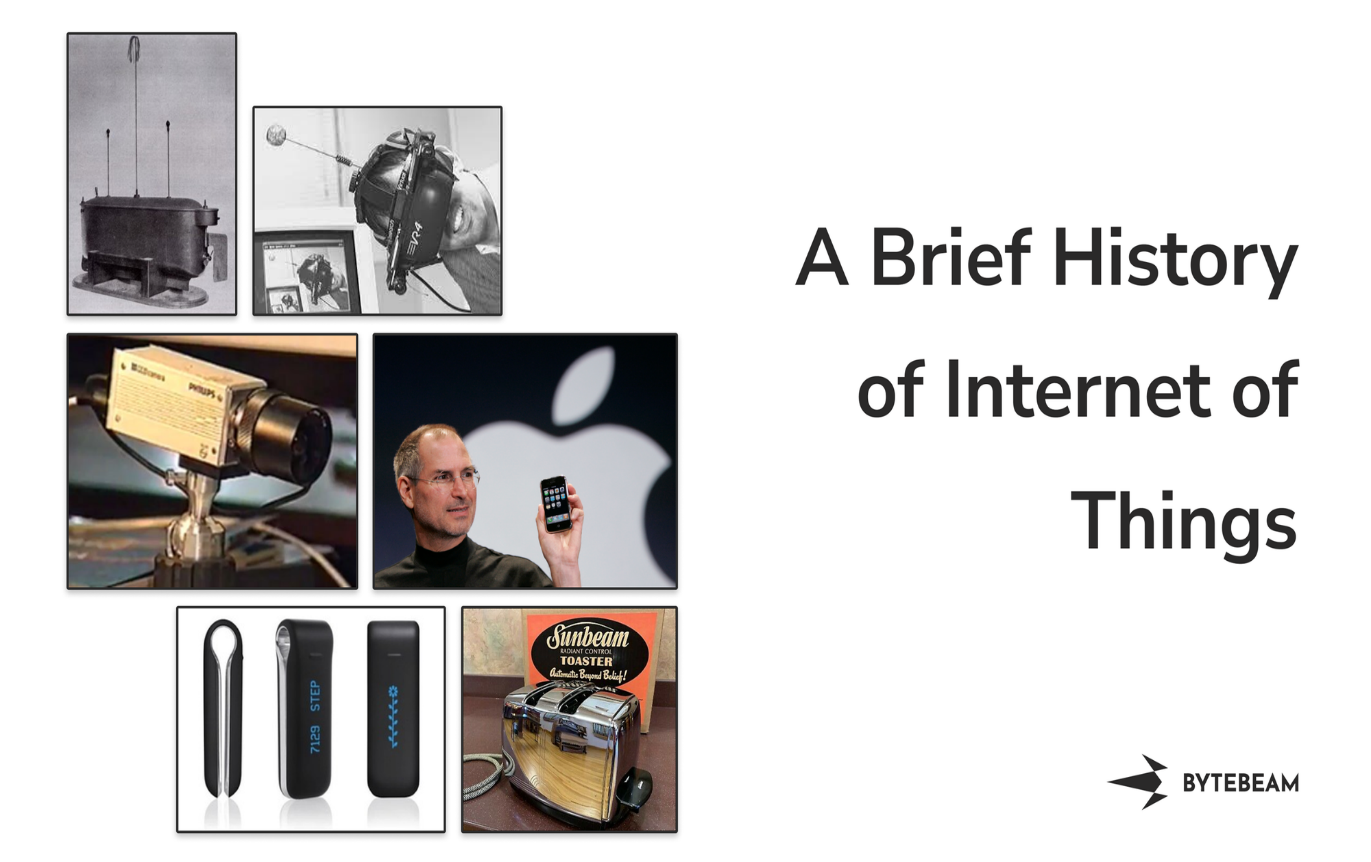
* **Sensors:** Sensors are devices that measure physical or environmental conditions and convert them into electrical signals. Additionally, These signals can then be transmitted to other devices or systems. Sensors are essential for the IoT, as they provide the data that allows IoT devices to make decisions and take action.
* **Communication protocols:** Communication protocols are the rules that govern how devices communicate with each other. There are many different communication protocols used in the IoT, each with its own advantages and disadvantages. Some of the most common communication protocols for IoT devices include MQTT, CoAP, and HTTP.
* **Networking technologies:** Networking technologies allow IoT devices to connect to the internet. Also,  There are a variety of networking technologies that can be used for IoT devices, including Wi-Fi, cellular, and LPWAN. Moreover, LPWAN (low-power wide-area network) is a type of networking technology that is designed for IoT devices that have limited power and bandwidth.
* **Cloud computing:** Cloud computing provides a platform for storing and processing data from IoT devices. Cloud computing is essential for the IoT, as it allows IoT devices to store and process large amounts of data without having to have their own dedicated hardware.
* **Data analytics:**Data analytics is the process of analysing data to extract insights. Also, Data analytics is essential for the IoT, as it allows businesses to gain insights from the data collected by IoT devices.

These are just some of the technologies that make the IoT possible. As the IoT continues to grow, we can expect to see even more innovative technologies being developed to support this rapidly expanding field.

**Applications of the Internet of Things**

The Internet of Things (IoT) relies on a diverse range of technologies that work together to enable its functionality and connectivity. Let’s explore the key technologies that underpin the Internet of Things.

* **Smart homes:** IoT devices are being used to make homes more comfortable, efficient, and secure. For example, smart thermostats can adjust the temperature of your home based on your schedule, and smart locks can be opened and closed remotely.
* **Smart cities:** IoT devices are being used to improve the efficiency of city infrastructure. Sensors can be used to monitor traffic flow and optimize public transportation, and smart street lights can be dimmed or turned off when they are not needed.
* **Industrial IoT:** IoT devices are being used to improve the efficiency and productivity of industrial processes. Sensors can be used to monitor the condition of machinery and predict when repairs are needed, and actuators can be used to adjust the settings of machines in real-time.
* **Healthcare:** IoT devices are being used to improve the quality of healthcare. Wearable devices can be used to track patients’ vital signs and provide real-time feedback to doctors, and smart pills can release medication at specific times.
* **Logistics and supply chain:** IoT devices are being used to track and manage the movement of goods through the supply chain. This can help improve efficiency, reduce costs, and prevent fraud.
* **Agriculture:** IoT devices are being used to monitor and manage agricultural operations. This can help improve crop yields, reduce water usage, and prevent pests and diseases.
* **Environment:** IoT devices are being used to monitor and manage the environment. This can help track pollution levels, conserve resources, and protect wildlife.

****

he Internet of Things, commonly abbreviated as IoT, is a system of interconnected devices and sensors that share data with each other. While the term “Internet of Things” was coined in 1999 by Kevin Ashton, a British technology pioneer, the concept of connected devices dates back to the early days of radio and television. In this article, we’ll take a look at the history of IoT and how it has evolved over time.

## A Quick Glance at the History of IoT

IoT has a long and complex history, dating back to the early days of computing. Here is a very simplified timeline of the history of IoT and some of the key events that have shaped the IoT landscape:

**1970s**: The first wireless networks are developed, laying the groundwork for IoT technologies.

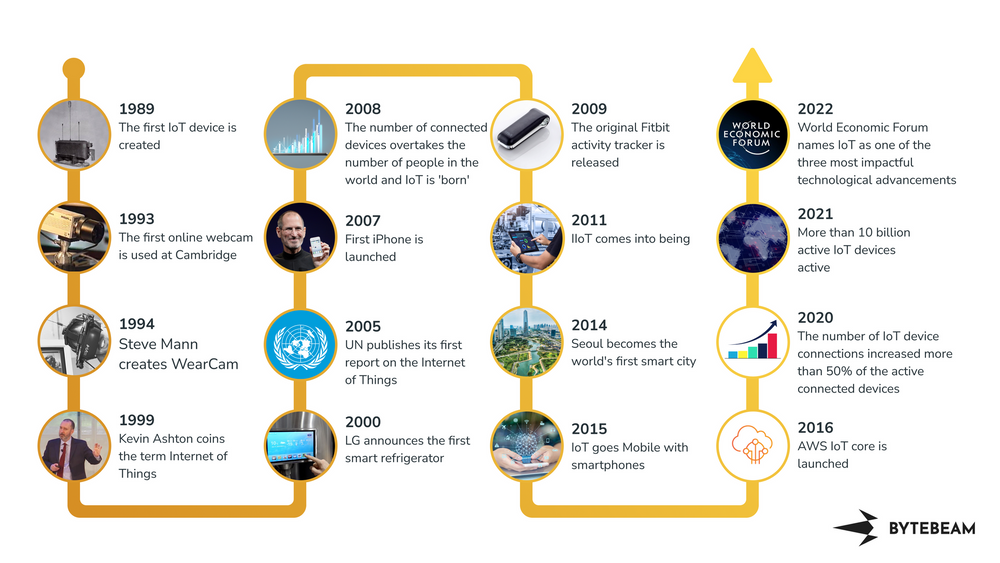
**1980s**: The first commercial cellular networks are launched, opening up new possibilities for mobile devices and wireless data transmission.

**1990s**: The first internet-connected devices appear, including early versions of smart home devices and wearable computers.

**2000s**: The proliferation of broadband internet and wireless networks leads to an explosion in the number of connected devices. IoT technologies begin to be widely used in a variety of industries, from manufacturing to healthcare.

**2010s**: IoT becomes a major force in the consumer market, with products like Nest thermostats and Amazon Echo becoming popular household items. Businesses continue to find new ways to use IoT technologies to increase efficiency and gain insights into their operations.

**2020s**: The IoT landscape continues to evolve, with 5G networks beginning to be rolled out and new applications for IoT technologies emerging constantly.



### **The birth of the Internet and IoT**

In 1962, J.C.R. Licklider, the head of the Defense Advanced Research Projects Agency (DARPA), envisioned a galactic network of an interconnected set of computers. His concept later evolved into the Advanced Research Projects Agency Network (ARPANET) in 1969. By 1980, ARPANET was commercialized for public use, and thus the internet was born.

In 1989, David Nichols and his colleagues at MIT invented the first IoT device, and this was shortly followed by John Romkey and Simon Hackett creating [the Internet Toaster](https://www.livinginternet.com/i/ia_myths_toast.htm) in 1991. The Internet toaster was a big milestone, as Romkey and Hackett successfully connected a toaster to the internet and managed to turn it on and off remotely.

We can conclusively say that the early breakthroughs in Internet of Things were a result of researchers having fun with technology (and occasionally getting frustrated at the lack of beverages).

Don’t believe us?

Dr. Quentin Stafford-Fraser and his colleagues at the University of Cambridge invented the [first online webcam](https://www.bbc.com/news/technology-20439301) for the same reason the smart vending machine was invented. When the researchers at Cambridge wanted coffee, they had to leave their workstations to go fetch it. But they would often find the coffee pot empty. Dr. Stafford-Fraser and his colleagues then installed a camera near the coffee pot which would click pictures of the pot 3 times a minute. This would allow everyone to check if the pot was empty and save them the frustration. This camera was connected to the internet in 1993 and became the first online webcam.

A year later, [Steve Mann created WearCam](http://wearcam.org/biowaw.htm), which turned out to be the first major milestone for wearable technology.

### **IoT is christened**

By now, devices being connected to the internet was becoming a thing (pun intended). But it was still a result of odd scattered experiments as opposed to a single technology. This changed when [Kevin Ashton](https://www.historyofinformation.com/detail.php?id=3411), the co-founder of the Auto-ID Labs at MIT, coined the term ‘Internet of Things’ in 1999. Ashton, who believed that RFID is a prerequisite for IoT, was a big believer in the potential of the technology.

*He once said, “....today's information technology is so dependent on data originated by people that our computers know more about ideas than things. If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost….”*

### **IoT goes household**

At the turn of the millennium, smart technology began blooming. Internet of Things made its way to homes from research labs. In 2000, LG announced the [first ever smart refrigerator](https://www.ryt9.com/en/prg/23392), which paved the way for the commercialization of IoT.

In less than a decade of coining the term, Internet of Things had become a phenomenon. The United Nations published its first report on the Internet of Things in 2005, deeming it one of the technologies that had the most global potential.

The UN report’s predictions were pretty apt, as just two years later, Apple announced the first iPhone in 2007. Although the [first ever smartphone](https://en.wikipedia.org/wiki/Smartphone#History) would be the Simon Personal Communicator, created by IBM in 1994, it was the iPhone that popularized smartphones globally, even though the first iPhone only allowed users to browse the internet.

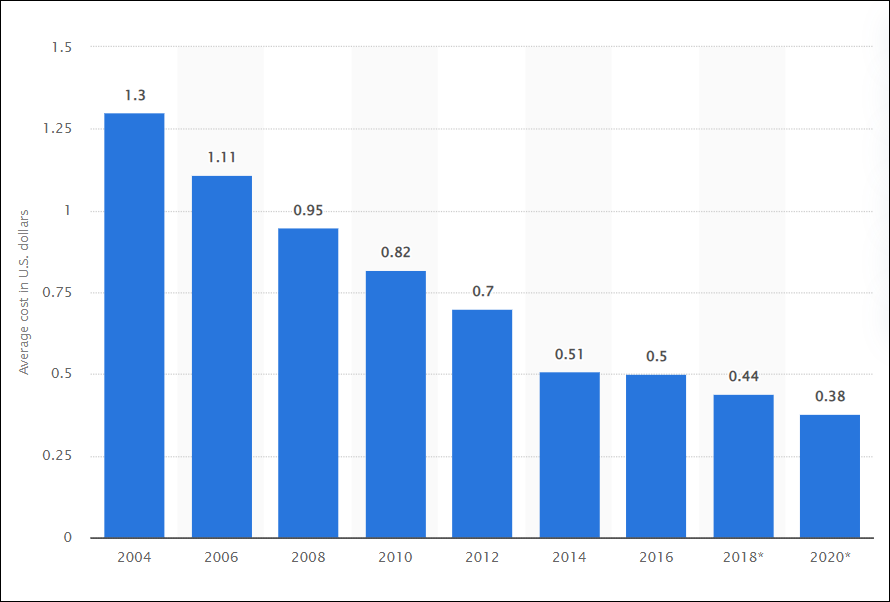
By 2008, the [number of connected devices](https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf) overtook the number of people in the world. This was the time that IoT was truly born, as the number of connected devices was officially at a stage where any data across the world could be collected if need be.

The 2000s was an exciting decade for IoT as several milestones were achieved in a short period. As the technology and the utility rapidly evolved, IoT could finally be a part of everyday life. In 2009, [Fitbit released its original activity tracker](https://en.wikipedia.org/wiki/Fitbit#:~:text=The%20first%20product%20released%20was,which%20was%20released%20in%202009.). This was the first wearable activity tracker that paved the way for modern smartwatches.

As we enter the 2010s, IoT milestones started getting more technical and specific. The underlying technology had already evolved enough that the sub-segments could start evolving on their own.

### **IoT becomes accessible**

Now Industrial IoT was always a thing alongside IoT, as it was a specific application of the technology, but in 2010, the sensor prices dropped enough so that they could be used in a widespread manner. This enabled IIoT more than any other factor, as IIoT required a large-scale setup of devices to run. The following figure shows us the Average costs of industrial Internet of Things (IoT) sensors from 2004 to 2020, according to [Statista](https://www.statista.com/statistics/682846/vr-tethered-hmd-average-selling-price/)

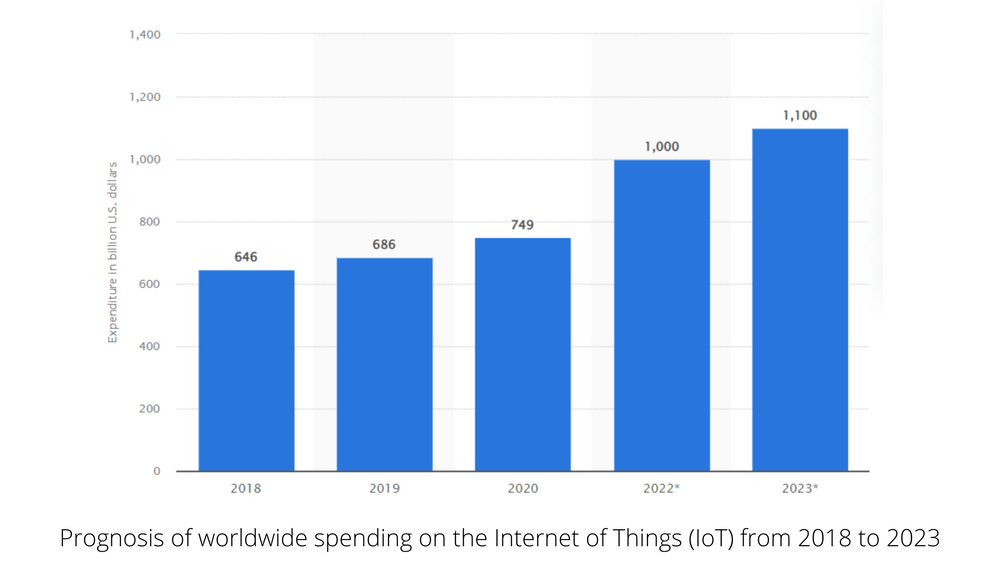


Industrial applications weren’t the only segment that received a boost from better and cheaper infrastructure. Smart cities suddenly became feasible with the widespread availability of IoT devices—and as a result, [Seoul became the world’s first smart city in 2014](https://www.theguardian.com/cities/2014/dec/22/songdo-south-korea-world-first-smart-city-in-pictures). Shortly after that Singapore, Amsterdam, and New York followed suit.

By this point in time, sensors were accessible enough to be used in every device, and wearable technology took advantage of this. IoT truly went mobile in 2015, as smartphones, smartwatches, health monitors, and GPS trackers became a household scene.

### **IoT today and tomorrow**

As global spending on IoT increased, businesses started investing in the technology. The following figure shows the spending rise in IoT.



As the technology became lucrative enough for several businesses to be interested, IoT platforms started cropping up. [AWS launched IoT core](https://aws.amazon.com/blogs/aws/aws-iot-now-generally-available/4) in 2015 and rolled it out completely by 2016. This was closely followed by [Azure IoT hub](https://venturebeat.com/business/microsoft-is-launching-its-azure-iot-hub-service-out-of-public-preview/) in 2016 and [Google IoT core](https://cloud.google.com/iot/docs/release-notes) in 2017.

In the following years, several other IoT platforms were launched, which allowed businesses to simplify their IoT projects and expand into the IoT space more easily. As a direct result, in 2021, [the number of connected devices](https://dataprot.net/statistics/iot-statistics/#:~:text=In%202021%2C%20there%20were%20more,to%20the%20internet%20per%20minute.) surpassed the number of non-connected devices worldwide.

To take note of its growing influence, the World Economic Forum named IoT as one of the [three most impactful technological advancements](https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/disruptive-technologies) in 2022.

The history of IoT is full of fun experiments, complex evolution, and some major industry overhauls. There are several predictions for where Internet of Things will go from here, but that’s for another post. For now, we hope to have enlightened you with the journey that led to today’s IoT landscape.

# Characteristics of Internet of Things

### **1.  Connectivity**

Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, the connection between people through Internet devices like mobile phones, and other gadgets, also a connection between Internet devices such as routers, gateways, sensors, etc.

### **2. Intelligence and Identity**

The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

### **3. Scalability**

The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

### **4. Dynamic and Self-Adapting (Complexity)**

IoT devices should dynamically adapt themselves to changing contexts and scenarios.  Assume a camera meant for surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, and night).

### **5. Architecture**

[IoT Architecture](https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/) cannot be homogeneous in nature. It should be hybrid, supporting different manufacturers ‘ products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.

### **6. Safety**

There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at risk. Therefore, equipment safety is also critical.

For more, refer to [Challenges to IoT](https://www.geeksforgeeks.org/challenges-in-internet-of-things-iot/).

### **7. Self Configuring**

This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

### **8. Interoperability**

IoT devices use standardized protocols and technologies to ensure they can communicate with each other and other systems. Interoperability is one of the key characteristics of the Internet of Things (IoT). It refers to the ability of different IoT devices and systems to communicate and exchange data with each other, regardless of the underlying technology or manufacturer.

Interoperability is critical for the success of IoT, as it enables different devices and systems to work together seamlessly and provides a seamless user experience. Without interoperability, IoT systems would be limited to individual silos of data and devices, making it difficult to share information and create new services and applications.

To achieve interoperability, IoT devices, and systems use standardized communication protocols and data formats. These standards allow different devices to understand and process data in a consistent and reliable manner, enabling data to be exchanged between devices and systems regardless of the technology used.

#### Examples of standards used in IoT

**MQTT (Message Queuing Telemetry Transport):**[MQTT (Message Queuing Telemetry Transport**)**](https://www.geeksforgeeks.org/introduction-of-message-queue-telemetry-transport-protocol-mqtt/) is a publish/subscribe communication protocol used for IoT device communication.

**CoAP (Constrained Application Protocol):** [CoAP (Constrained Application Protocol)](https://www.geeksforgeeks.org/difference-between-coap-and-mqtt-protocols/) is a lightweight communication protocol for IoT devices with limited resources.

**Bluetooth Low Energy (BLE):** [Bluetooth Low Energy](https://www.geeksforgeeks.org/bluetooth-vs-bluetooth-low-energy/) is a wireless communication technology used for IoT devices with low power consumption requirements.

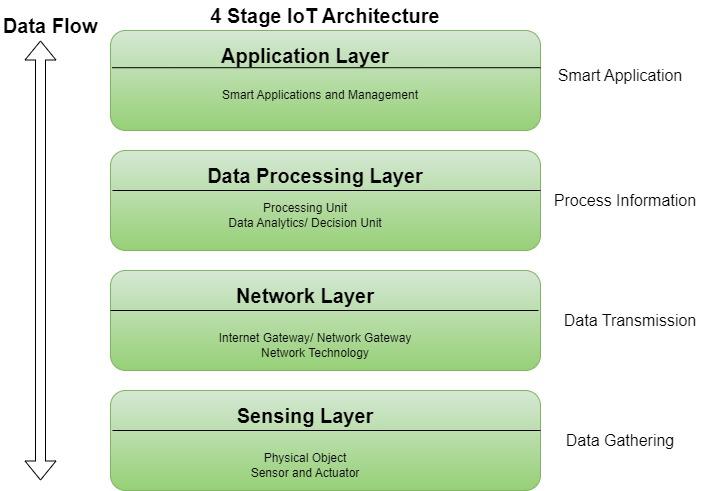
**Wi-Fi:** A wireless communication technology used for IoT devices that require high data transfer rates.

**Zigbee:** A low-power, low-cost wireless communication technology used for IoT devices.

**Architecture of IoT**

The architecture of IoT is divided into 4 different layers i.e. Sensing Layer, Network Layer, Data processing Layer, and Application Layer.

* **Sensing Layer:**The sensing layer is the first layer of the [Internet of Things](https://www.geeksforgeeks.org/introduction-to-internet-of-things-iot-set-1/) architecture and is responsible for collecting data from different sources. This layer includes [sensors](https://www.geeksforgeeks.org/sensors-in-internet-of-thingsiot/) and [actuators](https://www.geeksforgeeks.org/actuators-in-iot/) that are placed in the environment to gather information about temperature, humidity, light, sound, and other physical parameters. Wired or wireless communication protocols connect these devices to the network layer.
* **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 [WiFi,](https://www.geeksforgeeks.org/what-is-wi-fiwireless-fidelity/" \t "_blank) Bluetooth, Zigbee, and cellular networks such as 4G and [5G technology](https://www.geeksforgeeks.org/5g-technology-and-its-significance/). Additionally, the network layer may include [gateways](https://www.geeksforgeeks.org/introduction-of-gateways/) and [routers](https://www.geeksforgeeks.org/introduction-of-a-router/)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, analyzing, 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](https://www.geeksforgeeks.org/ml-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 analyzed and transformed into meaningful insights. This can include machine learning algorithms, [data visualization tools](https://www.geeksforgeeks.org/data-visualization-tools/), and other advanced analytics capabilities.

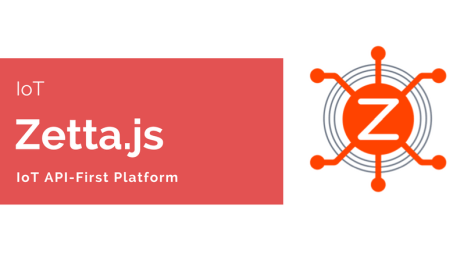


**source of the IoT**

## 1.****Kaa****

is one of the best open-source IoT frameworks that enable the management of data of connected objects and is very flexible. It is highly efficient. Also, it is highly secure as it uses encrypted channels and also uses standard open protocols. Most of the time directly or via gateways, the devices in this platform can be connected. It is user-friendly and device management is the best as it arranges devices into groups and manages the credentials of every connected device. Data collection is also a big advantage as this platform can collect data on a large scale and can process both structured and unstructured data without any issue.

## 2. Zetta

[](https://i0.wp.com/miro.medium.com/max/810/0*TzB-Kyh2iX9VaE8m.png?ssl=1)

is an open-source IoT framework. The server uses Node.js for integration. It combines REST APIs, web sockets, and reactive programming. They perfectly assemble data and manages the devices. It can link to boards like Raspberry Pi, Arduino, Spark Core, and PCs together with cloud platforms like Heroku. Its server assigns every device a REST API both locally and in the cloud which makes every device an API itself. It also presents a visual of huge data collected through the server. It allows the user to create various smartphone apps and cloud apps. Whenever a complex situation occurs, Zetta handles it itself

## 3. thinger.io

 is an open-source IoT framework with few limitations. Device connectivity is simple because of basic code requirements. Due to this sending and receiving, data is very easy. It also helps in controlling the functionalities of the device. The integration of every type of device is possible. Their processor, manufacturer certainly doesn’t matter. They have a unique communication paradigm that enables the IoT server to receive or send data only when required. The framework can connect multiple devices with less computation load and very low bandwidth. However, It allows creating bidirectional communications with several devices like Arduino, Raspberry Pi, etc including MQTT devices or other internet API data resources. It consists of multiple widgets for better display and arrangement of data in the platform.

**4. ThingsBoard**

[](https://i0.wp.com/thingsboard.io/images/thingsboard_logo.png?ssl=1)

[**ThingsBoard**](https://thingsboard.io/) is an open-source IoT framework. The main purpose of the framework is data collection and device management. Further, it uses IoT protocols like HTTP, MQTT, and CoAP for device connectivity. It is also highly scalable as every type of device easily integrated. Also, it never loses any data because of its fault tolerance and performance. Visualization of data is great due to the presence of automatic or custom widgets. ThingsBoard also supports both cloud and on-premises deployments. It is very secure encryption for both MQTT and HTTP protocols is enabled. Also, the credentials of devices are managed by device authentication

**5. DeviceHive**

[](https://i0.wp.com/www.iot-now.com/wp-content/uploads/2014/09/DeviceHive-logo-v2.jpg?ssl=1)

[**DeviceHive**](https://devicehive.com/)is an open-source IoT framework that provides instruments for smart device communication and management. Its architecture consists of a communication layer, control software, and multi-platform libraries. It mainly focuses on providing services that aim in the development of smart energy, home automation, remote sensing, remote control, and much more. It is basically a scalable, hardware-cum-cloud service platform with APIs in different protocols, which allows the user to set up, control, and analyze the behavior of the data. Its application varies from data transition, validation, and collection up to Machine Learning and Artificial Intelligence. It supports a variety of libraries including Python, Node.js, Java, and even ESP8266 Firmware

**6. Mainflux**

[](https://avatars3.githubusercontent.com/u/13207490?s=400&v=4)

[**Mainflux**](https://www.mainflux.com/) is an open-source IoT framework. It is capable of developing IoT applications and control various smart connected products. Mainflux IoT platform works as a software infrastructure that provides various advantages. Device management is very easy including data management and aggregation. The connectivity between multiple devices is very safe and remains stable. The interface is very user friendly which helps in easy understanding for beginners. It has the license of Apache 2.0 and there is complete transparency between devices and the platform. A user gets full support and their bugs are fixed. The connection is fully secure by authentication and authorization Server with help of customizable API keys. The execution is very fast and robust which results in a great performance. This platform is very scalable as well and also fault tolerance which is also the reason for better performance.

**7. ThingSpeak**

[](https://i0.wp.com/brands.home-assistant.io/_/thingspeak/logo.png?ssl=1)

[**ThingSpeak**](https://thingspeak.com/) is an open-source IoT framework with some limitations. This framework has enough free services to use. This framework allows us to analyze real-time data and control live streams in the cloud. The data sent to the cloud is used to make instant alerts on the platform. Data from sensors is privately collected and sent to the cloud. The data is analyzed and visualized with MATLAB. Then alerts or triggers are set to act according to the data. Various tools are present for exploring data using MATLAB. Due to the presence of these tools and features, this platform is very user friendly.

**8. myDevices**



[**myDevices**](https://mydevices.com/) is an open-source IoT framework which has front end IoT with application features. The data of sensors are very easily manageable and also the platform helps in fixing bugs. It is very easy to set up using plug and play getaways. This platform enables a user to set alerts according to the data received through the sensors. Steps are taken inside the app If there is an issue. Third-party apps and services can also receive data from the app. The old data can be retrieved from the app for future needs

**9. openremote**

[](https://lh3.googleusercontent.com/proxy/EO2t_EzEOwD_1sDcqw52R4qAAowUx9n_UrOjv5sIpIDi_1lZIbQCuoRsqoQNLfM9psuVxi2XLJ_CV1BwiUJawaK6yoB_DRvMthpWcjhDzbkspLPLsdGTeJwefZiZtHM8SXyYtGw)

[**openremote**](https://openremote.io/) is a 100% open-source IoT framework. It can make multiple IoT applications. The framework uses protocols like HTTP REST or MQTT which helps in connection with IoT devices and gateways. It is can make apps suitable for both Android and iOS. The connection of multiple devices is possible due to its device management. Device integration is easy. It can control multiple devices in a single interface. Several tools are present which makes the data manageable and user-friendly. Designing is very easy as the data can be transformed into applications using the platform. Progress of the project is noted using visualization dashboards.

**10. WSO2**

[](https://iot4beginners.com/top-10-open-source-iot-frameworks/image/png;base64,)

[**WSO2**](https://wso2.com/iot/) is an open-source IoT framework that allows its enterprises to control their mobile applications and devices. It provides a secure way of manufacturing the devices and manages them efficiently. The optimal design of the platform ensures the protection of both device and its data. Also, the capability of analyzing the gathered data helps in real-time visualizing. The identification of different types of patterns and data is possible. They get converted into meaningful responsive actions. CDM (Connected Device Management Core) is the controlling unit or the brain of the WSO2 platform. The evolution of the CDM core has boosted the capability of the platform which has enabled it to integrate with devices of any type.

# IoT/M2M systems layers and Design standardization in IOT

## [Design Standardization](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Design%20Standardization)

* Design standardization in IoT refers to the development and adoption of common technical specifications,
* protocols, and guidelines to ensure **compatibility and interoperability**among various IoT devices and systems.
* This standardization facilitates**seamless communication and integration**
* between devices from **different manufacturers,** enabling them to work together effectively.

### [**Communication Protocols**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Communication%20Protocols)

* Standardized communication protocols, such as **HTTP,**
* are essential for enabling seamless data exchange between IoT devices from different manufacturers.
* Regardless of their origin, thereby facilitating a unified and efficient IoT ecosystem.

### [**Data Formats**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Data%20Formats)

* Standardizing data formats and structures allows for consistent data interpretation and processing across various devices and platforms.
* This means that data generated by one device can be easily understood
* and utilized by another, and simplifying data integration and analysis.

### [**Security Standards**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Security%20Standards)

* Implementing uniform security measures is crucial for protecting IoT systems against threats.
* Standardized security protocols, such as encryption, authentication,
* and access control, ensure that all devices within the network adhere to the same security practices.

### [**Hardware Interfaces**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Hardware%20Interfaces)

* Standardized hardware interfaces and connectors ensure that different sensors, actuators, and devices can be easily integrated into various IoT systems.
* This compatibility simplifies the deployment and maintenance of IoT infrastructure, allowing for more flexible and scalable solutions.

### [**Interoperability Guidelines**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Interoperability%20Guidelines)

* Developing guidelines and best practices for interoperability ensures that
* devices and systems from different manufacturers can work together without conflicts.
* These guidelines help in achieving a cohesive and functional IoT ecosystem.

### [**What do you mean by Communicational Technology ?**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#What%20do%20you%20mean%20by%20Communicational%20Technology%20?)

* Communicational technology refers to the various methods, protocols, and
* systems used to enable data exchange between IoT devices, networks, and platforms.
* These technologies are crucial for ensuring that IoT devices can effectively
* communicate with each other, share data, and interact with centralized systems for analysis and control.

### [**Key aspects of communicational technology in IoT**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Key%20aspects%20of%20communicational%20technology%20in%20IoT)

#### [Wireless Communication Protocols](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Wireless%20Communication%20Protocols)

* Wireless protocols such as **Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN**, and**NB-IoT** enable IoT devices to communicate without physical connections.
* These protocols vary in range, power consumption, and data rates, catering to different IoT applications.
* For example, Bluetooth is suitable for short-range, low-power communication,
* while LoRaWAN supports long-range, low-power communication ideal for wide-area networks.

#### [Wired Communication Protocols](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Wired%20Communication%20Protocols)

* Wired protocols, like **Ethernet and serial communication (RS-232, RS-485**), provide reliable, secure, and high-speed data transfer.
* They are often used in industrial and high-stakes environments where
* stability and security are paramount, such as factory automation and critical infrastructure.

#### [Low-Power Wide-Area Networks (LPWAN)](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Low-Power%20Wide-Area%20Networks%20(LPWAN))

* LPWAN technologies like Sigfox, LoRaWAN, and NB-IoT are designed for long-range communication with minimal power consumption.
* These networks are ideal for IoT applications that require devices to operate on battery power for years,
* such as **environmental monitoring, smart agriculture**, and remote asset tracking.
* LPWANs support low data rates but cover extensive areas, making them suitable for scattered or rural deployments.

#### [Edge and Fog Computing](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Edge%20and%20Fog%20Computing)

* Edge computing processes data on the device or nearby, while fog computing processes data within a local network of devices.
* Both methods reduce the need to send data to a central cloud server, lowering latency and bandwidth usage.
* This approach is beneficial for real-time applications, such as autonomous vehicles and industrial automation, where quick data processing is crucial.

### [**What do you mean by data enrichment ?**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#What%20do%20you%20mean%20by%20data%20enrichment%20?)

* Data enrichment in the Internet of Things (IoT) refers to the process of enhancing raw data collected from IoT devices by adding context,
* meaning, and additional information to **make it more valuable and useful**for analysis and decision-making.
* This can involve combining the r**aw data with other data sources,**applying algorithms, or using metadata to provide deeper insights.

### [**Key aspects of data enrichment in IoT**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#%20Key%20aspects%20of%20data%20enrichment%20in%20IoT)

#### [Contextualization](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Contextualization)

* Adding **contextual information s**uch as time, location, or environmental conditions to the raw data to make it more meaningful.
* For example, temperature readings from sensors are more valuable when paired with the exact time and location of the measurement.

#### [Integration with External Data](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Integration%20with%20External%20Data)

* Combining IoT data with external data sources, such as weather data, traffic information, or social media feeds,
* to provide a more comprehensive understanding of the situation.

#### [Data Aggregation](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Data%20Aggregation)

* Summarizing or aggregating data from multiple IoT devices to identify trends or patterns.
* For instance, aggregating energy usage data from multiple smart meters
* can help in analyzing overall energy consumption patterns in a neighborhood.

#### [Application of Algorithms](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Application%20of%20Algorithms)

* Using machine learning and other algorithms to analyze and interpret the data,
* identifying anomalies, predicting future events, or providing actionable insights.
* For example, predictive maintenance algorithms can analyze data from machinery sensors to predict when maintenance is needed.

#### [Adding Metadata](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Adding%20Metadata)

* Enhancing raw data with metadata, which provides additional details about the data, such as the source, format, or quality.
* Metadata helps in organizing, searching, and understanding the data more effectively.

### [**What do you mean by data consolidation ?**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#What%20do%20you%20mean%20by%20data%20consolidation%20?)

* Data integration is the process of combining data from multiple sources into a unified database.
* This process is essential for achieving a comprehensive view of the data, improving data quality, and enabling more effective analysis.
* In Internet of Things (IoT), data consolidation involves aggregating data
* collected from various IoT devices, sensors, and systems into a centralized database or data warehouse.

### [**Key aspects of data consolidation**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Key%20aspects%20of%20data%20consolidation)

#### [Data Aggregation](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Data%20Aggregation)

* Gathering data from different IoT devices and sources, such as sensors, machines, and external databases, and combining it into a single dataset.
* This step ensures that all relevant data is available in one place for analysis.

#### [Data Cleaning](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Data%20Cleaning)

* Identifying and correcting errors, inconsistencies, and duplicates in the collected data.
* Data cleaning is crucial to ensure that the consolidated dataset is accurate, reliable, and ready for analysis.

#### [Data Transformation](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Data%20Transformation)

* Converting data from different formats and structures into a standardized format.
* This step ensures that data from various sources can be easily integrated and compared within the unified dataset.

#### [Data Integration](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Data%20Integration)

* Merging data from different sources while preserving its integrity and consistency.
* Data integration often involves resolving conflicts and discrepancies between datasets to create a cohesive and accurate consolidated dataset.

#### [Data Storage](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Data%20Storage)

* Storing the consolidated data in a centralized repository, such as a data warehouse or cloud storage.
* This repository provides a single source of truth for the data, making it easier to access, manage, and analyze.

### [**How can we differentiate between data enrichment and consolidation**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#How%20can%20we%20differentiate%20between%20data%20enrichment%20and%20consolidation)

Data enrichment and data consolidation are two distinct processes in data management, each serving a different purpose:

#### [Data Enrichment](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Data%20Enrichment)

* Enhances existing data by adding more information to make it more valuable and insightful.
* Involves adding context, integrating external data, applying algorithms, and attaching metadata.
* Combining temperature sensor data with weather reports to provide context for the readings.

#### [Data Consolidation](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Data%20Consolidation)

* Merges data from various sources into a single, cohesive dataset.
* Involves aggregating, cleaning, transforming, integrating, and storing data.
* Merging data from multiple sensors in different locations into a central database.

#### [Key Differences](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Key%20Differences)

* Enrichment is about enhancing and adding value to data, while consolidation is about combining and unifying data.
* Enriched data provides deeper insights, whereas consolidated data provides a comprehensive dataset from multiple sources.

### [**What do you mean by ease of designing and affordability in IOT?**](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#What%20do%20you%20mean%20by%20ease%20of%20designing%20and%20affordability%20in%20IOT?)

#### [Ease of Designing](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Ease%20of%20Designing)

* The concept of ease of designing in IoT (Internet of Things) pertains to the simplicity,
* efficiency, and user-friendliness of the design process for IoT solutions. Here's how it applies:

#### [Intuitive Design Tools](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Intuitive%20Design%20Tools)

* Design tools specific to IoT, such as IoT development platforms and integrated development environments (IDEs), should be intuitive and user-friendly.
* These tools should simplify the process of creating IoT applications, enabling designers to easily prototype, iterate, and refine their ideas.

#### [Modular and Reusable Components](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Modular%20and%20Reusable%20Components)

* Designing IoT solutions becomes easier when designers can leverage modular and reusable components.
* This allows them to quickly assemble and integrate various hardware and software modules to create custom IoT devices and applications without starting from scratch.

#### [Prototyping and Simulation](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Prototyping%20and%20Simulation)

* Ease of designing IoT solutions is enhanced through tools that support rapid prototyping and simulation.
* Designers can create virtual prototypes of IoT devices and systems, simulate their behavior in different scenarios.

#### [Visualization and Interface Design](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Visualization%20and%20Interface%20Design)

* Visualization tools and interface design frameworks play a crucial role in IoT design.
* Designers should have access to tools that allow them to create intuitive user interfaces and visualize data from IoT devices in a clear and actionable manner, enhancing the overall user experience.

#### [Collaboration and Integration](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Collaboration%20and%20Integration)

* Collaboration tools and integration capabilities facilitate teamwork among designers, developers, engineers, and stakeholders involved in IoT projects.
* Designers should be able to seamlessly collaborate, share ideas, and integrate their work with other team members' contributions to ensure cohesion and alignment throughout the design process.

#### [Documentation and Support](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Documentation%20and%20Support)

* Comprehensive documentation and support resources are essential for designers working on IoT projects.
* Access to tutorials, guidelines, reference materials, and community forums can help designers navigate challenges.

#### [Affordability](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Affordability)

* In Internet of Things (IoT), affordability refers to the cost-effectiveness of IoT solutions, devices, and infrastructure.
* It encompasses several aspects related to the financial accessibility and sustainability of IoT implementations.

#### [Cost-Effective Solutions](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Cost-Effective%20Solutions)

* IoT solutions should be designed and developed with a focus on minimizing costs without compromising quality, performance, or security.
* This involves optimizing hardware, software, and deployment processes to reduce expenses associated with manufacturing, installation, maintenance, and operation.

#### [Affordable Devices and Components](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Affordable%20Devices%20and%20Components)

* IoT devices, sensors, and components should be **affordable and accessible** to a wide range of users, including individuals, businesses, and organizations with varying budgets and resources.
* This may involve leveraging cost-effective materials, **manufacturing techniques,** and supply chains to keep production costs low.

#### [Scalability and Cost Efficiency](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Scalability%20and%20Cost%20Efficiency)

* IoT deployments should be scalable and cost-efficient, allowing for incremental expansion and growth without significant increases in expenses.
* This includes designing systems that can **accommodate additional devices,** users, and data volume without substantial investments in infrastructure or resources.

#### [Energy Efficiency](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Energy%20Efficiency)

* Affordability in IoT also involves minimizing energy consumption and operational costs associated with IoT devices and networks.
* Energy-efficient designs,**low-power components, and optimized communication protocols** help reduce electricity bills and extend the lifespan of battery-powered devices.

#### [Total Cost of Ownership (TCO)](https://bcalabs.org/subject/iot-m2m-systems-layers-and-design-standardization-in-iot#Total%20Cost%20of%20Ownership%20(TCO))

* Affordability considerations in IoT extend beyond initial purchase costs to include the total cost of ownership over the device or solution's lifecycle.
* This encompasses ongoing expenses such as **maintenance, upgrades, software updates,** data storage, and support services

## Major Components of IoT

### Things or Devices

The key physical items being tracked are Things or Devices. Smart sensors are connected to things/devices which further continues to collect data from the device and send it to the next layer, which is the portal or also called as the gateway Small smart sensors for a variety of applications are now possible because of new advancements in microelectronics.

Some commonly used sensors are:

* Temperature sensors and thermostats
* Pressure sensors
* Humidity / Moisture level
* Light intensity detectors
* Moisture sensors
* Proximity detection
* RFID tags

### User Interface

User interface also termed as UI is nothing but a user-facing program that allows the user to monitor and manipulate data.

The user interface (UI) is the visible, tangible portion of the IoT device that people can interact with. Developers must provide a well-designed user interface that requires the least amount of effort from users and promotes additional interactions.

### Cloud

Cloud storage is used to store the data which has been collected from different devices or things. Cloud computing is simply a set of connected servers that operate continuously(24\*7) over the Internet.

IoT devices, applications, and users generate massive amounts of data, which must be managed efficiently. Data collection, processing, management, and archiving are among the responsibilities of IoT clouds. The data can be accessed remotely by industries and services, allowing them to take critical decisions at any time.

In the simplest terms, an IoT cloud is a network of servers optimized to handle data at high speeds for a large number of different devices, manage traffic, and analyze data with great accuracy. An IoT cloud would not be complete without a distributed management database system.

### Analytics

After receiving the data in the cloud, that data is processed. Data is analyzed here with the help of various algorithms like machine learning and all.

Analytics is the conversion of analog information via connected sensors and devices into actionable insights that can be processed, interpreted, and analyzed in depth. Analysis of raw data or information for further processing is a prerequisite for the monitoring and enhancement of the Internet of things (IoT).

Among the most significant benefits of a well-designed IoT system is real-time smart analysis, which enables designers to spot anomalies in gathering information and respond quickly to avoid an undesirable situation. If information is collected correctly and at the right moment, network operators can plan for the next steps.

### Network Interconnection

Over the past few years, the IoT has seen massive growth in devices controlled by the internet and connected to it. Although IoT devices have a wide variety of uses, there are some common things among them also along with the differences between them.

IoT is enabled by a variety of technologies. The network used to communicate with other devices in an IoT deployment is critical to the field, a position that numerous wireless or wired technologies can fill.

### System Security

Security is a crucial component of IoT implementation, but this security point of view is too often overlooked during the design process. Day after day weaknesses within IoT are being attacked with evil intent – however, the majority of them that can be easily and inexpensively addressed.

A secure network begins with the elimination of weaknesses within IoT devices as well as the provision of tools to withstand, recognize, and recoup from harmful attacks.

### Central Control Hardware

The two or more data flow among multiple channels and interfaces is managed by a Control Panel. The additional duty of a control panel is to convert various wireless interfaces and ensure that linked sensors and devices are accessible.