**Network and Communication aspects in IoT**

**Wireless Media Access Issues in Internet of Things**

When it comes to communication using a wireless medium there is always a concern about the interference due to other present wireless communication technologies. Wireless means communication and message transfer without the use of physical medium i.e., wires.

Let us understand how communication is done between them. Different Mobile stations(MS) are attached to a transmitter/receiver which communicates via a shared channel by other nodes. In this type of communication, it makes it difficult for the MAC design rather than the wireline networks.

The very important issues which are observed are: Half Duplex operation, Time-varying channel, and Burst channel errors.  
These are explained as following below.

**1. Half Duplex operation:**  
Half-duplex transmission means when the sender and receiver both are capable of sharing data but one at a time. In wireless transmission, it is difficult to receive data when the transmitter is sending the data because during transmission a large amount or a large fraction of signal energy is leaked while broadcasting. The magnitude of the transferred signal and received signal differs a lot. Due to which collision detection is even not possible by the sender as the intensity of the transferred signal is large than the received one. Hence this causes the problem of collision and the prime focus should be to minimize the collision

**2. Time-varying channel :**  
Time-varying channels include the three mechanisms for radio signal propagations they are Reflection, Diffraction, and Scattering.

* **Reflection –**  
  This occurs when a propagating wave carrying information intrudes on an object that has very large dimensions than the wavelength of the wave.
* **Diffraction –**  
  This occurs when the radio path between the transmitter and the receiver is collided by the surface with sharp edges. This is a phenomenon which causes the diffraction of the wave from the targeted position.
* **Scattering –**  
  This occurs when the medium through from the wave is traveling consists of some objects which have dimensions smaller than the wavelength of the wave.

While transmitting the signal by the node these are time shifted and this is called multipath propagation. While when this node signals intensity is dropped below a threshold value, then this is termed as fade. As a result Handshaking strategy is widely used so as a healthy communication can be set up.

**3. Burst channel errors :**  
Burst channel errors are called as a contiguous sequence of symbols, which are received in a communication channel, in which the first and last symbols has an error and there is no evidence of contiguous sub-sequence of corrected received symbols. When time-varying channels are used then signals strengths are introduced due to which errors are observed in transmission. For these channels in wireline networks, the Bit rate is high as 10 -3.

**A Survey on Routing Protocols for Internet of Things**

**ABSTRACT**: Internet of Things (IoT) is a wireless network of inter connected objects. It’s a paradigm in which devices are embedded with sensors that will make them interact with other objects and humans as well. These objects are capable of capturing and transforming the information they receive from their environment. As IoT networks are self organizing and decentralized, the objects are transient and the network experiences dynamic changes in node position. Hence, routing has trivial importance where packets are transmitted between objects as a part of communication establishment and successful delivery of the packets should be ensured. Moreover due to its high dynamic nature route discovery incurs significant overhead and energy consumption. Thus there is a vital need to analyze the routing protocols for IoT. Popular routing protocols can be used in IoT, by intelligently considering the limited hardware available in devices, power consumption and their random behavior.

1. INTRODUCTION With the advent of the Internet, humans have been interconnected across geographical boundaries. IoT is a paradigm in which devices are embedded with sensors that will make them interact with other objects and humans as well. These objects are capable of capturing and transforming the information they receive from their environment. Advancement in sensing, computing and communication has brought in notable improvement in real time communication and decision making. Hence IoT aims to make the internet ubiquitous and pervasive in nature. The process of collecting, sharing and transmitting information will involve communication between nodes which act as both host and router with or without human intervention. In addition, the route discovery process incurs overhead due to beaconing, where the network is flooded with route request packets. Thus we have to quantify the energy and performance of each routing protocol. In addition, devices in IoT environment will be capable of location identification and notification and provide history of prior wireless connections. As billions of objects will be connected to the internet, it is vital to have an independent architecture that allows easy connection, communication and control. Interaction of these objects across platforms and times when they must be sharable and disjoint seems to be a challenge.
2. ROUTING PROTOCOLS FOR IOT There exist lots of routing protocols each having a unique operating standard with significant performance for Wireless Sensor Networks that can be deployed for IoT with few modifications for bandwidth and power consumption. We discuss few of the broad categories of routing protocols in this section.

A.Naive Routing

The idea deployed in naïve routing is flooding. Each node can overhear its neighbors within its range. The source node floods the network with route request packets called as beacons. Destination nodes respond with a route reply message to the beacon and communication link is established between these nodes. Beaconing is typically utilized for location tracking, discovering routes to destinations and tracking neighbors through keep-alive requests. One of the most important factors that affect performance is the beacon interval in the route discovery process. If the beacon interval is too small, the number of beacons generated becomes huge. On the other hand, a higher beacon interval incurs a lesser number of generated beacons. Popular routing protocols such as DSR, DSDV and AODV fall under this category. However this flooding causes overhead in the network. By using steady state transition probability, we can derive the power consumption for each node. This probability will give a clear picture of the individual node behavior and the overall network.

**B.Hierarchical Routing**: Nodes form clusters based on polling. The cluster head is responsible for all communications on behalf of the members of the cluster. Group mobility can be achieved by the cluster head following some metric to devise the mobility pattern of the nodes in the cluster. LEACH is a common example, where the cluster head is rotated among the members to facilitate load balancing that can be deployed for IoT environments.

**C.Query based Routing** The underlying principle of query based routing is data dissemination within the network. A querying node can retrieve data from any node in the network. Common examples are SPIN and Direct Diffusion.

**D.Multipath** **routing** Protocols employing multipath routing seek to and use alternate paths towards every destination. This distributes the cost of forwarding packets among more nodes, saving the energy of individual, highly-frequented nodes.

**E.Probabilistic routing Routing** decision is based on the calculated probabilistic value. A primitive method to compute these values is by gossiping. Data packets are flooded into the network like a rumor with a probability p. Unlike other flooding mechanisms, these packets are forwarded only once and thereby the traffic overhead is reduced. A highly structured approach is to refer the prior history of packet delivery and mobility pattern, based on this we can decide which nodes can form a route to the destination.

**F.Ad-hoc On-Demand Distance Vector (AODV) AODV** computes a loop free single path on demand. A mobile node discovers and maintains a route to another node only when it needs to communicate. One observation of AODV is that, though the source actually discovers multiple paths during the route discovery process, it chooses only the best route and discards the rest. Also, frequent route breaks cause the intermediate nodes to drop packets because no alternate path to the destination is available. This reduces the overall throughput and the packet delivery ratio. Moreover, in high mobility scenarios, the average end-to end delay can be significantly high due to frequent route discoveries. When route failures occur, the process of route discovery has to begin from scratch consuming more network resources and overhead [5].

**G. Adhoc On-Demand Multipath Distance Vector (AOMDV)** In order to route with low overheads even under highly dynamic conditions, Adhoc On-Demand Multipath Distance Vector was introduced. AOMDV computes multiple loop free and link disjoint paths providing fault tolerance and efficient recovery from route failures. Each node maintains a list of its next hop neighbors that are sorted based on the hop count. When failures occurs during routing an alternate path is chosen, if there is no alternate path a route error message is given. The routing metric considered is the number of hops, thus paths with a small number of long hops are chosen. When paths with long hops are chosen, there is high probability for the occurrence of fading. Moreover the stability of the path is completely ignored as the alternate paths are not maintained. Thus the paths are stale and cannot be used on a failure. Therefore AOMDV is not adaptive to the dynamic changes in network topology

**H. Routing Protocol for Low Power and Lossy Networks (RPL)** RPL is based on IPv6 and is a link independent routing protocol which supports routing with minimal requirements by building a robust topology over lossy links. This routing protocol achieves multipoint-to-point, point-to-multipoint and point-to-point communication for simple and complex traffic models. The core of RPL is represented by a Destination Oriented Directed Acyclic Graph (DODAG), which is a directed acyclic graph with a single root. Each node knows its parent but has no information about its related children. RPL maintains atleast one path for each node to the root along with a preferred parent to pursue a faster path establishment to increase the performance. In order to maintain the routing topology and to keep the routing information updated, RPL uses four types of control messages – DODAG Information Object (DIO), Destination Advertisement Object (DAO), DODAG Information Solicitation (DIS) and DAO Acknowledgment (DAS-ACK). The current rank of the node is stored in DIO, which determines the distance of each node to the root based on specific metrics and determines a unique parent path. The destination information is unicasted towards selected parents using DAO. RPL supports both upward and downward traffic. DIS is used to acquire DIO messages from a reachable adjacent node. DAO-ACK is a response to DAO message from a DAO parent node. DODAG is formed when the source nodes begins to send its location using DIO message to Low-power Lossy Network (LLN) levels. At each level the recipient routers register the paths for parent and participating nodes. As DIO messages propagate in the network, DODAG is built. After the construction of DODAG, a preferred parent establishes a default path with the root known as upward route. For downward routes, DAO message should be unicasted to the root through parents.

## **What is data aggregation**?

In layman’s terms, data aggregation is collecting and efficiently gathering data from various sources into a more digestible and insightful format. The goal is to generate meaningful patterns and actionable insights to drive strategic decision-making. In the context of IoT, the idea remains the same but with a much broader and more complex scale of operation.

## The role of IoT in data aggregation

The Internet of Things (IoT) is an innovative network framework with many interconnected devices. From our home appliances to smart vehicles and industrial machinery, these IoT devices are in a constant state of activity, creating a relentless data flow

## The significance: Why is data aggregation essential in IoT?

When the Internet of Things (IoT) intertwines with big data, it forms a potent blend that provides considerable benefits, delivering tangible value to businesses and individuals alike. This synergistic alliance empowers a multitude of benefits, from bolstering decision-making to amplifying operational efficiency and refining customer experiences. By methodically harvesting and analysing data from [IoT devices](https://infisim.com/blog/iot-device-management), organisations can unlock a treasure trove of insights that fuel growth and bolster competitiveness.

### Empowering IoT applications

Data aggregation enables many IoT applications, including [smart cities](https://infisim.com/m2m-by-industry/iot-in-smart-cities), industrial automation, healthcare monitoring, environmental monitoring, and more. It provides the necessary data inputs for these applications to operate efficiently and derive actionable intelligence.

### Optimising resource utilisation

Aggregating data at different levels, such as the base station, sink node, or cluster head, reduces redundant data transmission and minimises congestion, improving network performance. This optimisation leads to efficient resource utilisation, extended network longevity, and enhanced scalability.

### Enhancing energy efficiency

Data aggregation minimises energy consumption by reducing the number of transmissions and allowing individual nodes to conserve power. This is crucial in resource-constrained IoT environments where sensor devices may have limited battery life.

### Facilitating fault detection & anomaly detection

Aggregating data from multiple sensor nodes enables the detection of faults and anomalies in the network. By analysing aggregated data, organisations can identify deviations from expected patterns, detect malfunctioning nodes, and take proactive measures for system maintenance.

## Implementation of data aggregation in IoT

Implementing data aggregation in the Internet of Things (IoT) is an intricate process involving several steps:

### Step 1: Data collection

The process begins with data collection, which involves gathering data from multiple IoT devices. This data can be varied, both in terms of type and source. However, its raw and unstructured nature at this stage makes it challenging to directly derive meaningful insights.

### Step 2: Data pre-processing

Once the data is collected, it moves on to the pre-processing stage. Here, the raw data is cleaned and standardised. It involves removing inconsistencies, filling in missing values, and resolving conflicts to ensure the data is fit for statistical analysis.

### Step 3: Data aggregation

The next step is data aggregation, where the pre-processed data is compiled and summarised into a more digestible format. This process involves transforming the data by calculation, sorting, or grouping to provide a summary that can offer useful insights.

### Step 4: Data analysis

Finally, the aggregated data is analysed. This is where the data is examined in-depth to uncover trends, patterns, and correlations. With the help of data analysis tools, valuable insights are extracted from the aggregated data, which can then be utilised for decision-making.

# Data Dissemination

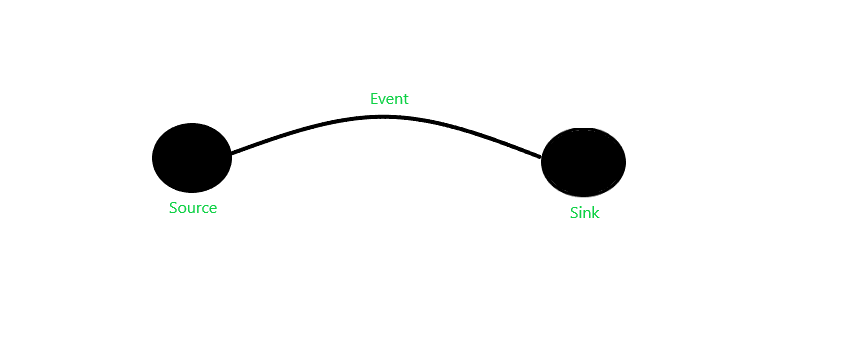
Data Dissemination is a procedure where the server initiates and manages transfer of data as well as updates. It also helps in maintaining data consistency and cache management. It is defined as “Pushing data to mobile devices from a server or some other computer.” Mobile devices can select time and cache required data. In ad-hoc network, traffic is peer to peer. Multi-hop routing is used to communicate data. In wireless sensor network, other traffic models are possible which are as follows:

* Data Collection Model: The source sends data to a collection periodically on demand
* Data Diffusion Model:  A sensor node that generates data based on its sensing mechanism’s observation.

 Data dissemination has two different entities:

* Source: Generating data.
* Event: Something that needs to be reported for example, in target detection, some abnormal activity.
* Sink: A node randomly located in the field, that is interested in events and seeks such information.

Event in the below diagram indicates the information to be reported or sent. After source receives an interest from the sink, the event is transferred from the source to the sink. Data dissemination is a two step process. First, the node that is interested in some events, broadcasts its interests to its neighbors periodically. Interests are then propagated through the whole sensor network. In the second step, nodes that have requested data, send back data after receiving the request. Intermediate nodes in the sensor network also keep a cache of received interests and data.



There exists several data dissemination methods:

**Flooding:**It is the simplest design. In this method, each node receiving data repeats it by broadcasting the data to every neighbor unless the maximum hop lifetime of the data has been reached.

Data dissemination is a critical function in wireless sensor networks (WSNs) that involves the transmission of sensor data from one or more nodes to a base station or other nodes in the network.

### The features of data dissemination in WSNs include:

**Energy Efficiency:**WSNs are typically powered by batteries or other low-power sources, and so energy efficiency is a crucial consideration in data dissemination. Techniques such as data aggregation, compression, and clustering can be used to reduce the amount of data transmitted and conserve energy.

**Reliability:**Data dissemination in WSNs must be reliable, meaning that all nodes in the network receive the necessary data without loss or duplication. Techniques such as error detection and correction can be used to ensure reliability.

**Scalability:** WSNs can range in size from a few nodes to thousands or even millions of nodes. Data dissemination techniques must be scalable to accommodate the number of nodes in the network.

**Security:** WSNs are vulnerable to security threats, such as eavesdropping, tampering, and denial of service attacks. Techniques such as encryption and authentication can be used to ensure the security of data dissemination.

**Adaptability:**WSNs must be adaptable to changing conditions in the environment, such as changes in the number and location of nodes, changes in data rates, and changes in network topology. Techniques such as dynamic routing and load balancing can be used to adapt to these changes.

**QoS Requirements:** In some applications, data dissemination may have Quality of Service (QoS) requirements such as delay, throughput, or reliability. Techniques such as priority scheduling and traffic shaping can be used to ensure that QoS requirements are met.

data dissemination in WSNs is a complex task that requires careful consideration of the above features to ensure efficient and reliable operation of the network.

Advantages

* Simple to setup and implement.
* Data and queries reach all the nodes in the network.

Disadvantages of Flooding

* Implosion- No restriction on multiple nodes sending same packets to the same destination.
* Overlapping- Neighbor nodes may receive the same message if the nodes access the same event.
* Resource Blindness- Flooding does not care about energy efficiency of the nodes.

**Gossiping:**It is the enhancement of Flooding. In this, when a node receives data, it randomly chooses a neighbor and sends the data to it. Unlike Flooding, we does not need to bother about duplicate data packets being sent to the same location. It also contributes to the latency of network.

Advantages

* This protocol is easily scalable.
* It eliminates some of the shortcomings of Flooding.
* This protocol sends data in autonomous and decentralized manner

Disadvantages of Gossiping

* The destination is selected randomly so it may lead to starvation for some nodes as they may not be selected to send data at all.

**SPIN:**Sensor Protocols for Information via Negotiation (SPIN) has the required features which can overcome the shortcomings of flooding. When interested nodes send a request, SPIN will send the data to the corresponding node otherwise it will not on its own. SPIN messages can be distinguished into three types:

* ADV- ADV message is used to signal that the sensor has data to send and describes the data by the help of a sensor
* REQ- REQ message is used when a node is ready to receive data from neighboring node
* DATA- The information to be sent is contained here

Advantages

* SPIN is more efficient than flooding since the negotiation reduces the implosion and overlap.

Disadvantages

* SPIN-2 is more effective than SPIN-1 as it uses energy or resource threshold so that limited number of nodes can participate in data transmission.

**Cost- field Approach:**The goal of the cost-field approach is the efficient flow of data from source to sink through a path which is free of obstacles. It’s job is to keep the path obstacle free. The cost-field approach relies upon two steps to work properly. The first step is that all sensor nodes should have a cost field, based on parameters like delay. In the second step, data is distributed based on the parameter of costs. It is imperative that the lower the cost at each node from the source to the sink, the more optimal the path is. This approach does not require to maintain information about the path of the nodes arranged in the configuration sequence.

Advantages

* Makes sure sensor path is problem free
* Does not need to maintain explicit path information
* The cost at each node is the minimum cost from the node to the sink, which occurs on the optimal path

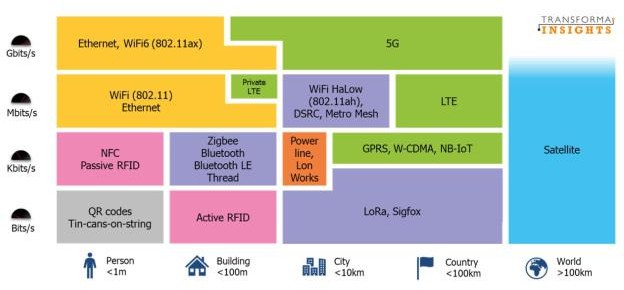
Disadvantages

* Time consuming. As it uses back-off timers for forwarding data to other nodes

Communication Technologies

The following communication protocols have immediate importance to consumer and industrial IoTs:

* + IEEE 802.15.4
  + Zigbee
  + 6LoWPAN
  + Wireless HART
  + Z‐Wave
  + ISA 100
  + Bluetooth
  + NFC
  + RFID



# What is Bluetooth?

Bluetooth is a wireless technology that lets devices like phones, tablets, and headphones connect to each other and share information without needing cables. Bluetooth simply follows the principle of transmitting and receiving data using [radio waves](https://www.geeksforgeeks.org/radio-waves/). It can be paired with the other device which has also Bluetooth but it should be within the estimated communication range to connect. When two devices start to share data, they form a network called piconet which can further accommodate more than five devices.

## **Key Features of Bluetooth**

* The transmission capacity of Bluetooth is 720 kbps.
* Bluetooth is a wireless device.
* Bluetooth is a Low-cost and short-distance radio communications standard.
* Bluetooth is robust and flexible.
* The basic architecture unit of Bluetooth is a piconet.

## Architecture of Bluetooth

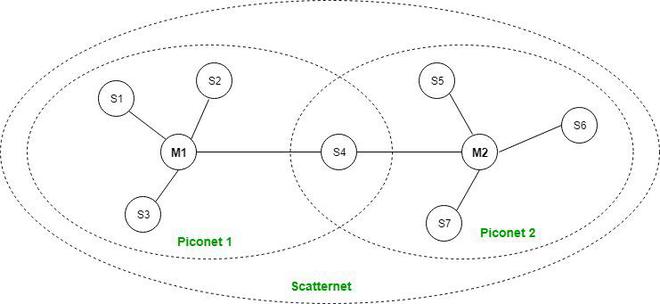
The architecture of Bluetooth defines two types of networks:

### **Piconet**

Piconet is a type of Bluetooth network that containsone primary node called the master node and seven active secondary nodes called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

### **Scatternet**

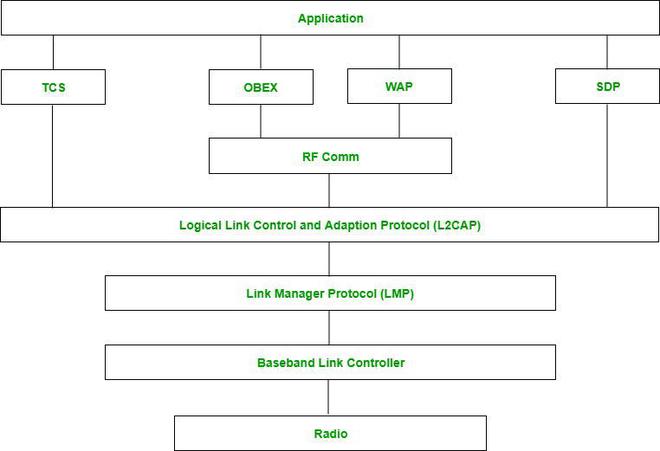
It is formed by using various piconets. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.



*Bluetooth Architecture*

## Bluetooth Protocol Stack

* **Radio (RF) Layer:** It specifies the details of the air interface, including frequency, the use of frequency hopping and transmit power. It performs modulation/demodulation of the data into [RF signals](https://www.geeksforgeeks.org/introduction-of-radio-frequency-identification-rfid/). It defines the physical characteristics of Bluetooth transceivers. It defines two types of physical links: connection-less and connection-oriented.
* **Baseband Link Layer:** The baseband is the digital engine of a Bluetooth system and is equivalent to the [MAC](https://www.geeksforgeeks.org/mac-address-in-computer-network/) sublayer in LANs.  It performs the connection establishment within a piconet, addressing, packet format, timing and power control.
* **Link Manager Protocol Layer:** It performs the management of the already established links which includes authentication and encryption processes. It is responsible for creating the links, monitoring their health, and terminating them gracefully upon command or failure.
* **Logical Link Control and Adaption (L2CAP) Protocol Layer:** It is also known as the heart of the Bluetooth protocol stack. It allows the communication between upper and lower layers of the Bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs segmentation and [multiplexing](https://www.geeksforgeeks.org/multiplexing-channel-sharing-in-computer-network/).
* **Service Discovery Protocol (SDP) Layer:** It is short for Service Discovery Protocol. It allows discovering the services available on another Bluetooth-enabled device.
* **RF Comm Layer:** It is a cabal replacement protocol. It is short for Radio Frontend Component. It provides a serial interface with [WAP](https://www.geeksforgeeks.org/wireless-application-protocol/)and OBEX. It also provides emulation of serial ports over the logical link control and adaption protocol(L2CAP). The protocol is based on the ETSI standard TS 07.10.
* **OBEX:** It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.
* **WAP:** It is short for Wireless Access Protocol. It is used for internet access.
* **TCS:** It is short for [Telephony Control Protocol](https://www.geeksforgeeks.org/internet-telephony-protocol-h-323/). It provides telephony service. The basic function of this layer is call control (setup & release) and group management for the gateway serving multiple devices.
* **Application Layer:** It enables the user to interact with the application.



*Bluetooth Protocol Stack*

## Types of Bluetooth

Various types of Bluetooth are available in the market nowadays. Let us look at them.

* **In-Car Headset:**One can make calls from the car speaker system without the use of mobile phones.
* **Stereo Headset:** To listen to music in car or in music players at home.
* **Webcam:** One can link the camera with the help of Bluetooth with their laptop or phone.
* **Bluetooth-Equipped Printer:** The printer can be used when connected via Bluetooth with mobile phone or laptop.
* **Bluetooth Global Positioning System (GPS):** To use [Global Positioning System (GPS)](https://www.geeksforgeeks.org/gps-full-form/) in cars, one can connect their phone with car system via Bluetooth to fetch the directions of the address.

## Applications of Bluetooth

* It can be used in wireless headsets, wireless [PANs, and LANs.](https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/)
* It can connect a digital camera wireless to a mobile phone.
* It can transfer data in terms of videos, songs, photographs, or files from one cell phone to another cell phone or computer.
* It is used in the sectors of Medical healthcare, sports and fitness, Military.

## Advantages

* It is a low-cost and easy-to-use device.
* It can also penetrate through walls.
* It creates an [Ad-hoc connection](https://www.geeksforgeeks.org/applications-of-ad-hoc-network-and-its-problems/) immediately without any wires.
* It is used for voice and data transfer.

## Disadvantages

* It can be hacked and hence, less secure.
* It has a slow data transfer rate of 3 Mbps.
* Bluetooth communication does not support [routing](https://www.geeksforgeeks.org/types-of-routing/).

# Introduction of ZigBee

ZigBee is a Personal Area Network task group with low rate task group 4. It is a technology of home networking. ZigBee is a technological standard created for controlling and sensing the network. As we know that ZigBee is the Personal Area Network of task group 4 so it is based on IEEE 802.15.4 and is created by Zigbee Alliance.

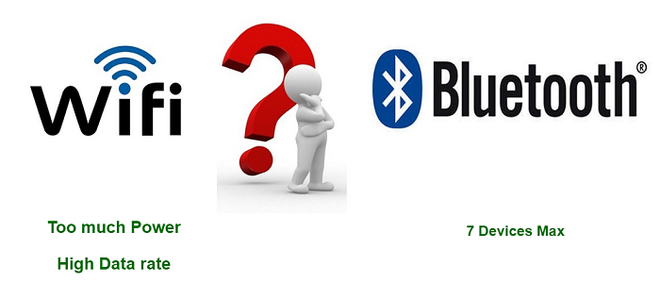
  ZigBee is an open, global, packet-based protocol designed to provide an easy-to-use architecture for secure, reliable, low power wireless networks. Flow or process control equipment can be place anywhere and still communicate with the rest of the system. It can also be moved, since the network doesn’t care about the physical location of a sensor, pump or valve.

*IEEE802.15.4 developed the PHY and MAC layer whereas, the ZigBee takes care of  upper higher layers.*

ZigBee is a standard that addresses the need for very low-cost implementation of Low power devices with Low data rates for short-range wireless communications.

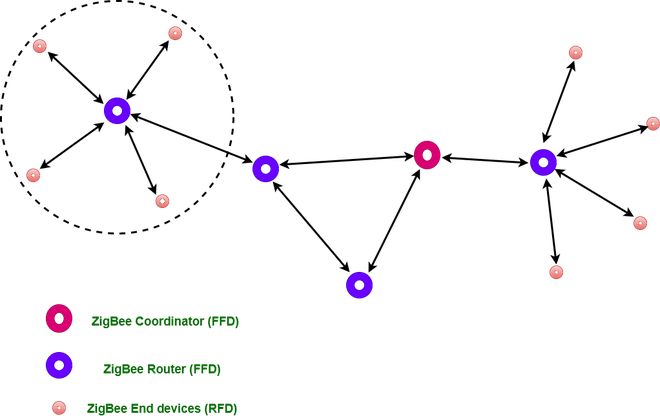
IEEE 802.15.4 supports star and peer-to-peer topologies. The ZigBee specification supports star and two kinds of peer-to-peer topologies, mesh and cluster tree. ZigBee-compliant devices are sometimes specified as supporting point-to-point and point-to-multipoint topologies.

**Why another short-range communication standard??**



### Types of ZigBee Devices:

* **Zigbee Coordinator Device:** It communicates with routers. This device is used for connecting the devices.
* **Zigbee Router:** It is used for passing the data between devices.
* **Zigbee End Device:** It is the device that is going to be controlled.



### General Characteristics of Zigbee Standard:

* Low Power Consumption
* Low Data Rate (20- 250 kbps)
* Short-Range (75-100 meters)
* Network Join Time (~ 30 msec)
* Support Small and Large Networks (up to 65000 devices (Theory); 240 devices (Practically))
* Low Cost of Products and Cheap Implementation (Open Source Protocol)
* Extremely low-duty cycle.
* 3 frequency bands with 27 channels.

**Operating Frequency Bands** (Only one channel will be selected for use in a network):

1. **Channel 0**: 868 MHz (Europe)
2. **Channel 1-10**: 915 MHz (the US and Australia)
3. **Channel 11-26**: 2.4 GHz (Across the World)

### Features of Zigbee:

**1. Stochastic addressing:** A device is assigned a random address and announced. Mechanism for address conflict resolution. Parents node don’t need to maintain assigned address table.

**2. Link Management:**Each node maintains quality of links to neighbors. Link quality is used as link cost in routing.

**3. Frequency Agility:**Nodes experience interference report to channel manager, which then selects another channel

**4. Asymmetric Link:**Each node has different transmit power and sensitivity. Paths may be asymmetric.

**5. Power Management:** Routers and Coordinators use main power. End Devices use batteries.

**Advantages of Zigbee:**

1. Designed for low power consumption.
2. Provides network security and application support services operating on the top of IEEE.
3. Zigbee makes possible completely networks homes where all devices are able to communicate and be
4. Use in smart home
5. Easy implementation
6. Adequate security features.
7. **Low cost**: Zigbee chips and modules are relatively inexpensive, which makes it a cost-effective solution for IoT applications.
8. **Mesh networking:** Zigbee uses a mesh network topology, which allows for devices to communicate with each other without the need for a central hub or router. This makes it ideal for use in smart home applications where devices need to communicate with each other and with a central control hub.
9. **Reliability:** Zigbee protocol is designed to be highly reliable, with robust mechanisms in place to ensure that data is delivered reliably even in adverse conditions.

**Disadvantages of Zigbee :**

1. **Limited range:** Zigbee has a relatively short range compared to other wireless communications protocols, which can make it less suitable for certain types of applications or for use in large buildings.
2. **Limited data rate:** Zigbee is designed for low-data-rate applications, which can make it less suitable for applications that require high-speed data transfer.
3. **Interoperability:** Zigbee is not as widely adopted as other IoT protocols, which can make it difficult to find devices that are compatible with each other.
4. **Security:** Zigbee’s security features are not as robust as other IoT protocols, making it more vulnerable to hacking and other security threats.

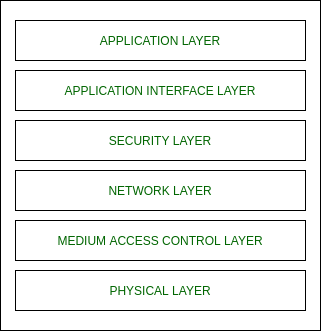
### Zigbee Network Topologies:

* **Star Topology** (ZigBee Smart Energy): Consists of a coordinator and several end devices, end devices communicate only with the coordinator.
* **Mesh Topology** (Self Healing Process): Mesh topology consists of one coordinator, several routers, and end devices.
* **Tree Topology**: In this topology, the network consists of a central node which is a coordinator, several routers, and end devices. the function of the router is to extend the network coverage.

### Architecture of Zigbee:

Zigbee architecture is a combination of 6 layers.

1. Application Layer
2. Application Interface Layer
3. Security Layer
4. Network Layer
5. Medium Access Control Layer
6. Physical Layer



* **Physical layer:**The lowest two layers i.e the physical and the MAC (Medium Access Control) Layer are defined by the IEEE 802.15.4 specifications. The Physical layer is closest to the hardware and directly controls and communicates with the Zigbee radio. The physical layer translates the data packets in the over-the-air bits for transmission and vice-versa during the reception.
* **Medium Access Control layer (MAC layer):**The layer is responsible for the interface between the physical and network layer. The MAC layer is also responsible for providing PAN ID and also network discovery through beacon requests.
* **Network layer:**This layer acts as an interface between the MAC layer and the application layer. It is responsible for mesh networking.
* **Application layer:**The application layer in the Zigbee stack is the highest protocol layer and it consists of the application support sub-layer and Zigbee device object. It contains manufacturer-defined applications.

**Channel Access:**

1. **Contention Based Method** (Carrier-Sense Multiple Access With Collision Avoidance Mechanism)
2. **Contention Free Method** (Coordinator dedicates a specific time slot to each device (Guaranteed Time Slot (GTS)))

### Zigbee Applications:

1. Home Automation
2. Medical Data Collection
3. Industrial Control Systems
4. meter reading system
5. light control system
6. Commercial
7. Government Markets Worldwide
8. Home Networking

# Z-Wave Protocol

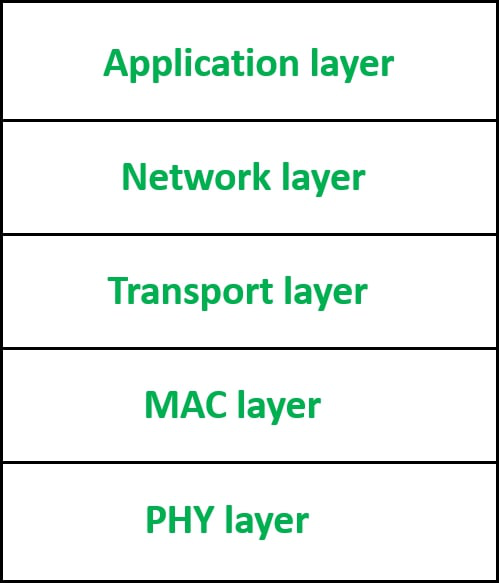
Z-Wave it is a wireless communication protocol used by automatic or automotive appliances for the purpose of connection and communication. It is invented in 1999 by Zensys a Danish-American company. In this article we are going to see some characteristics of Z-Wave, Components of Z-Wave, Z-Wave protocol stack, and some applications of Z-Wave.

### Z-Wave Protocol Stack :

Z-Wave protocol stack contains five layers physical layer, MAC layer, transport layer, network layer, and application layer.

* **PHY layer:**This layer has many functions but the important one is modulation and coding. In this layer, data is transferred in 8-bit blocks and the most significant bit is sent first.
* **MAC layer:**MAC layer as the name suggests takes care of medium access control among slave nodes based on collision avoidance and backoff algorithms. also, it takes care of network operations based on Home ID, Node ID, and other parameters in the z-wave frame.
* **Transport layer:** Z-Wave transport layer is mainly responsible for retransmission, packet acknowledgement, and packet origin authentication. the z-wave layer consists of four basic frame types:
  + Single cast frame
  + ACK frame
  + Multicast frame
  + Broadcast frame
* **Network layer:**Z-Wave network layer controls the frame routing from one node to another node.
* **Application layer:**This layer is responsible for decoding and execution of commands in the z-wave network.

The following diagram shows us various layers of the z-wave protocol stack:

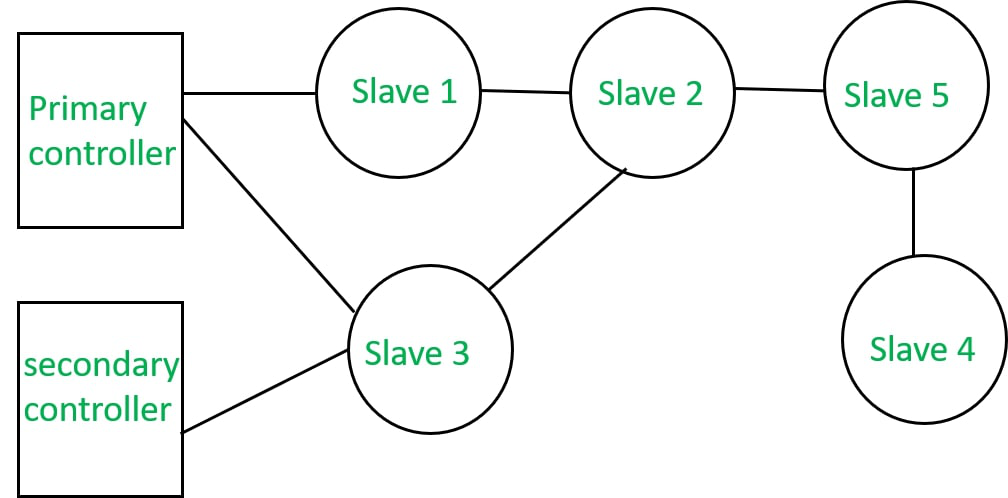


### Z-Wave Components :

The components of z-wave include controllers, slave nodes, Home ID, Node ID, and routing tables.

* **Controllers:** A controller is a unit that has the ability to compile a routing table of the network and can calculate routes to the different nodes. There are two types of controllers –
  + Primary controller: Primary controller is the device that contains a description of the z-wave network and controls the output. It assigns network ID or Home ID or Node ID to the z-wave during the enrollment process.
  + Secondary controller: It also has a Network ID and it remains constant to maintain routing tables.
* **Slave nodes:** Slave nodes are the nodes that do not contain routing tables but may contain a network map. slave nodes have the ability to receive frames and respond to them if necessary.
* **Home ID:**  The ID used by z-Wave for the separation of the network from each other is called Home ID. It is created by the primary controller and is 32-bit in size.
* **Node ID:** The identification number or an address that is given to every device during the process of inclusion is called Node ID.
* **Routing table:**It is used by controllers for calculating routes.

The following diagram shows us z-wave network .



### Characteristics of Z-Wave :

* Uses RF for signaling and control
* Frequency : 900 MHz (ISM)
* Range : 30 meter
* Data rates : upto 100 kbps
* FSK Modulation

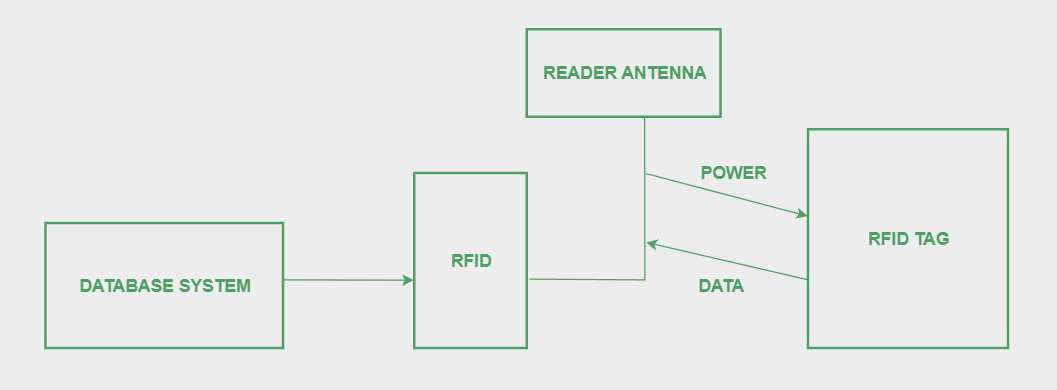
### Applications of Z-Wave :

* Home automation
* Water management using flood sensors
* Fingerprint scanner

# Introduction of Radio Frequency Identification (RFID)

**Radio Frequency Identification (RFID)** is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal, or person. It uses radio frequency to search, identify, track, and communicate with items and people.

It is a method that is used to track or identify an object by radio transmission over the web. Data is digitally encoded in an RFID tag which might be read by the reader. This device works as a tag or label during which data is read from tags that are stored in the database through the reader as compared to traditional barcodes and QR codes. It is often read outside the road of sight either passive or active RFID.



## **Types of RFID**

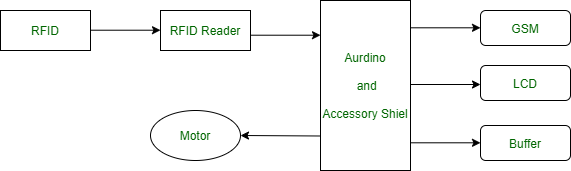
There are many kinds of RFID, each with different properties, but perhaps the most fascinating aspect of RFID technology is that most RFID tags have neither an electric plug nor a battery. Instead, all of the energy needed to operate them is supplied in the form of radio waves by RFID readers. This technology is called passive RFID to distinguish it from the(less common) active RFID in which there is a power source on the tag.

* **UHF RHID ( Ultra-High Frequency RFID )**. It is used on shipping pallets and some driver’s licenses. Readers send signals in the 902-928 MHz band. Tags communicate at distances of several meters by changing the way they reflect the reader signals; the reader is able to pick up these reflections. This way of operating is called backscatter.
* **HF RFID (High-Frequency RFID ).** It operates at 13.56 MHz and is likely to be in your passport, [credit cards](https://www.geeksforgeeks.org/how-credit-cards-impact-your-credit-score/), books, and noncontact payment systems. HF RFID has a short-range, typically a meter or less because the physical mechanism is based on induction rather than backscatter.
* **Passive RFID:**Passive RFID tags does not have their own power source. It uses power from the reader. In this device, RF tags are not attached by a power supply and passive RF tag stored their power. When it is emitted from active antennas and the RF tag are used specific frequency like 125-134KHZ as low frequency, 13.56MHZ as a high frequency and 856MHZ to 960MHZ as ultra-high frequency.
  + No need embedded power
  + Tracking inventory
  + Has unique identification number
  + Sensitive for interference
  + Semi-passive RFID
* **Active RFID:**In this device, RF tags are attached by a power supply that emits a signal and there is an antenna which receives the data. means, active tag uses a power source like battery. It has it’s own power source, does not require power from source/reader.
  + Embedded power: communication over large distance
  + Has unique identifier /identification number
  + Use other devices like sensors
  + Better than passive tags in the presence of metal

There are also other forms of RFID using other frequencies, such as LF RFID(Low-Frequency RFID), which was developed before HF RFID and used for tracking.

## **Working Principle of RFID**

Generally, RFID uses radio waves to perform AIDC function. AIDC stands for Automatic Identification and Data Capture technology which performs object identification and collection and mapping of the data. An antenna is an device which converts power into radio waves which are used for communication between reader and tag. RFID readers retrieve the information from RFID tag which detects the tag and reads or writes the data into the tag. It may include one processor, package, storage and transmitter and receiver unit.



## **Working of RFID System**

Every RFID system consists of three components: a scanning antenna, a [transceiver](https://www.geeksforgeeks.org/transceivers/)and a [transponder](https://www.geeksforgeeks.org/transponder/). When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers- fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

The transponder is in the RFID tag itself. The read range for RFID tags varies based on factors including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers. Tags that have a stronger power source also have a longer read range.

## **Features of RFID**

* An RFID tag consists of two-part which is an microcircuit and an antenna.
* This tag is covered by protective material which acts as a shield against the outer environment effect.
* This tag may active or passive in which we mainly and widely used passive RFID.

## **Application of RFID**

* It utilized in tracking shipping containers, trucks and railroad, cars.
* It uses in Asset tracking.
* It utilized in credit-card shaped for access application.
* It uses in Personnel tracking.
* Controlling access to restricted areas.
* It uses ID badging.
* [Supply chain management.](https://www.geeksforgeeks.org/supply-chain-management/)
* Counterfeit prevention (e.g., in the pharmaceutical industry).

## RFID Standards

* ISO 14443
* Components operating at 13.56Mhz
* Power consumption 10mW
* Data [throughput](https://www.geeksforgeeks.org/difference-between-bandwidth-and-throughput/)is 100 kbps
* Operates at working distance 10 cm
* ISO 15693
* Components operating at 13.56Mhz
* Operating at working distances as high as 1m
* Data throughput few kbps

## **Application Area of RFID**

* [Warehouses](https://www.geeksforgeeks.org/data-warehouse-architecture/)retailer automotive
* Grocery chain transportation
* Distribution center asset management
* Manufacturing
* Inventory management
* Warehousing and distribution
* Shop floor (Production)
* Document tracking and asset management
* Industrial application (e.g. time and attendances, shipping document tracking, receiving fixed assets)
* Retail applications.

## **Advantages of RFID**

* It provides data access and real-time information without taking to much time.
* RFID tags follow the instruction and store a large amount of information.
* The RFID system is non-line of sight nature of the technology.
* It improves the Efficiency, traceability of production.
* In RFID hundred of tags read in a short time.

## **Disadvantages of RFID**

* It takes longer to program RFID Devices.
* RFID intercepted easily even it is [Encrypted](https://www.geeksforgeeks.org/difference-between-encryption-and-encoding/).
* In an RFID system, there are two or three layers of ordinary household foil to dam the [radio wave](https://www.geeksforgeeks.org/radio-waves/).
* There is privacy concern about RFID devices anybody can access information about anything.
* Active RFID can costlier due to battery.

# Near Field Communication (NFC)

Near Field Communication (NFC) is a short-range wireless technology that enables communication between two electronic devices over a distance of 4 centimeters (1.6 inches) or less. In this article, we will discover near-field communication in detail along with its advantages and disadvantages.

## What is NFC?

NFC stands for Near Field Communication. It enables short-range communication between compatible devices. At least one transmitting device and another receiving device are needed to transmit the signal. Many devices can use the NFC standard and are considered either passive or active.

## Types of NFC

* **Passive NFC devices:**These near-field communication devices include tags and other small transmitters that can send information to other NFC devices without the need for a power source of their own. These devices don’t really process any information sent from other sources, and can not connect to other passive components. These often take the form of interactive signs on walls or advertisements.
* **Active NFC devices:**These near-field communication devices can do both things i.e. send and receive data. They can communicate with each other as well as with passive devices. Smartphones are the best example of active NFC devices. Card readers in public transport and touch payment terminals are also good examples of the technology.

## **How Does NFC Work?**

NFC relies on inductive coupling between two electromagnetic coils present on NFC-enabled devices (such as [smartphones](https://www.geeksforgeeks.org/various-smartphone-sensors/)). Communication occurs at a frequency of 13.56 MHz within the globally available unlicensed radio frequency ISM band. Data rates range from 106 to 848 kbit/s. NFC can be used for various purposes, including contactless transactions, data exchange, and simplified setup of more complex communications (e.g., [Wi-Fi](https://www.geeksforgeeks.org/what-is-wi-fiwireless-fidelity/)). When one of the connected devices has internet connectivity, data exchange with online services is also possible. The NFC standard currently has three distinct modes of operation to determine what sort of information will be exchanged between devices.

* The most commonly used in smartphones is the [peer-to-peer mode](https://www.geeksforgeeks.org/what-is-p2p-peer-to-peer-process/). The exchange of various pieces of information is allowed between 2 devices. In this mode both devices switch between active when sending data and passive when receiving.
* The second mode i.e. read/write mode is a one-way data transmission. The active device, possibly your smartphone, links up with another device in order to read information from it. NFC advertisement tags use this mode.
* The third mode of operation is card emulation. The NFC device can function as a smart or contactless credit card and make payments or tap into public transport systems.

## **Comparisons with Bluetooth**

There are several important technological differences between NFC and [Bluetooth](https://www.geeksforgeeks.org/bluetooth/) but NFC has some significant benefits in certain circumstances. The major advantage of NFC over Bluetooth is that it requires much less power consumption than Bluetooth. This makes NFC perfect for passive devices, such as the advertising tags as they can operate without a major power source. NFC android has one another major advantage i.e. faster connectivity. It uses inductive coupling(i.e. the absence of manual pairing) which takes less than one tenth of a second to establish a connection between two devices. While modern Bluetooth connects pretty fast, NFC is still super handy for certain scenarios such as mobile payments.

Samsung Pay, Android Pay, and even Apple Pay use NFC technology though Samsung Pay works a bit differently than the others. While Bluetooth works better for connecting devices together for file transfers, sharing connections to speakers, and more, we anticipate that NFC will always have a place in this world thanks to mobile payments — a quickly expanding technology.

| **Criteria** | **NFC** | **Bluetooth** |
| --- | --- | --- |
| **Power consumption** | Low | High |
| **Range** | Short (up to 10 cm) | Long (up to 10 meters) |
| **Data transfer speed** | Slower (up to 424 kbit/s) | Faster (up to 2.1 Mbit/s for Bluetooth 2.1 and 1 Mbit/s for Bluetooth Low Energy) |
| **Connectivity** | Faster (less than 1s to establish a connection) | Slower (may require manual pairing |
| **Suitable for** | Passive devices like tags and advertising signs | File transfers, sharing connections to speakers, and more |
| **Applications** | Mobile payments (Samsung Pay, Android Pay, Apple Pay) | File sharing, music streaming, connecting devices |

## Applications of NFC

* **Data Transfer**: You can share small amounts of data (such as contacts, [URLs](https://www.geeksforgeeks.org/url-full-form/), or files) between NFC-enabled devices.
* **Access Control**: NFC tags can grant access to buildings, public transport, or events.
* **Smart Pairing**: NFC simplifies pairing Bluetooth devices by tapping them together.
* **Smart Posters and Tags**: NFC tags embedded in posters, products, or advertisements can provide additional information when tapped.

## Benefits of NFC

* **Convenient Transactions**: NFC allows seamless payments and other transactions using smartphones through wallet apps.
* **Versatile Applications**: It finds applications in various domains such as banking, reservations, ticket booking, and entry/exit passes.
* **Secured Access**: It provides secure access for students and employees within their premises.
* **Enhanced Security**: Compared to magnetic strip-based debit and credit cards, NFC offers better security and uses PINs.
* **Easy Connectivity**: NFC doesn’t require search and pair procedures like Bluetooth.
* **No Special Software Needed**: It works without additional software or manual configurations.
* **Compatibility**: NFC is compatible with existing [RFID networks](https://www.geeksforgeeks.org/rfid-full-form/)

## Limitations of NFC

* **Short Range**: NFC operates within shorter distances (about 10-20 cm).
* **Low Data Transfer Rates**: It offers very low data transfer rates (106, 212, or 424 Kbps).
* **Costly Adoption**: Companies find it expensive to adopt NFC-enabled devices.
* **Complex Procedures**: Users may find NFC procedures more complex compared to other simpler options.

# TCP/IP Model

TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of communication protocols that define the standards for transmitting data over computer networks, including the internet. The TCP/IP protocol is the foundation of the internet and enables devices to communicate with each other using a common language.

The TCP/IP protocol is divided into two layers: the Transport layer and the Internet layer. The Transport layer is responsible for ensuring that data is transmitted reliably from one device to another. This layer is comprised of two protocols: the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). TCP is used for reliable data transmission, while UDP is used for fast transmission of data that can tolerate some packet loss.

The Internet layer is responsible for transmitting data packets between devices. This layer is comprised of two protocols: the Internet Protocol (IP) and the Address Resolution Protocol (ARP). IP is responsible for routing data packets between devices, while ARP is used to map IP addresses to physical addresses.

TCP/IP also includes a number of application layer protocols that are used to provide services to end-users. These include protocols such as HTTP (Hypertext Transfer Protocol) for web browsing, FTP (File Transfer Protocol) for file transfer, and SMTP (Simple Mail Transfer Protocol) for email.

**TCP/IP**stands for **Transmission Control Protocol/ Internet Protocol.** It is a set of conventions or rules and methods that are used to interconnect network devices on the Internet. The internet protocol suite is commonly known as TCP/IP, as the foundational protocols in the suite are Transmission Control Protocol and Internet Protocol. It chooses how the information will be traded over the web through end-to-end communications that incorporate how the information ought to be organized into bundles (bundles of data), addressed, sent, and received at the goal. This communication protocol can also be utilized to interconnect organize devices in a private network such as an intranet or an extranet.

### History of TCP/IP:

The Defense Advanced Research Projects Office (DARPA), the investigation department of the U.S. Department of Defense, made the TCP/IP shown in the 1970s for utilization in ARPANET, a wide zone organize that gone before the web. TCP/IP was initially planned for the Unix working framework, and it has been built into all of the working frameworks that came after it.

### Characteristics of TCP/IP:

* **Share Data Transfer:**The TCP allows applications to create channels of communications across a network. It also permits a message to be separated into smaller packets before they are transmitted over the web and after that collected in the right order at the destination address. So, it guarantees the solid transmission of data across the channel.
* **Internet Protocol:** The IP address tells the packets the address and route so that they reach the proper destination. It includes a strategy that empowers portal computers on the internet-connected to arrange forward the message after checking the IP address.
* **Reliability:** The most vital feature of TCP is solid data delivery. In arrange to supply unwavering quality, TCP must recover information that’s harmed, misplaced, copied, or conveyed out of arranging by the Arrange Layer.
* **Multiplexing:** Multiplexing can be achieved through the number of ports.
* **Connections:** Before application forms can send information by utilizing TCP, the devices must set up a connection. The associations are made between the harbor numbers of the sender and the collector devices.
* **Compatibility:** TCP/IP is designed to be compatible with a wide range of hardware and software platforms. This makes it a versatile protocol suite that can be used in a variety of network environments.
* **Scalability**: TCP/IP is highly scalable, which means that it can be used in networks of any size, from small home networks to large enterprise networks.
* **Open standards:** TCP/IP is based on open standards, which means that the protocol specifications are publicly available and can be implemented by anyone. This fosters innovation and competition in the networking industry.
* **Modular architecture:**TCP/IP is designed with a modular architecture, which means that different protocols can be added or removed as needed. This allows network administrators to tailor their networks to specific needs.
* **Reliability:** TCP/IP is designed to be highly reliable, with built-in error checking and correction mechanisms that ensure data is transmitted accurately and reliably.
* **Flexibility:** TCP/IP is a flexible protocol suite that can be used for a wide range of applications, including web browsing, email, file sharing, and more.
* **End-to-end connectivity:**TCP/IP provides end-to-end connectivity between devices, which means that data can be transmitted directly from the source device to the destination device without being routed through intermediate devices.

### TCP/IP Layers

* **Application Layer** An application layer is the topmost layer within the TCP/IP model. When one application layer protocol needs to communicate with another application layer, it forwards its information to the transport layer.
* **Transport Layer** It is responsible for the reliability, flow control, and correction of data that is being sent over the network. There are two protocols used in this layer are User Datagram Protocol and Transmission control protocol.
* **Internet/Network Layer** It is the third layer of the TCP/IP Model and also known as the Network layer. The main responsibility of this layer is to send the packets from any network, and they arrive at the goal irrespective of the route they take.
* **Network Access Layer** It is the lowest layer of the TCP/IP Model. It is the combination of the Physical Layer and the Data link layer which present in the OSI Model. Its main responsibility is to the transmission of information over the same network between two devices.

### How TCP/ IP works?

* TCP/IP employs the client-server demonstration of communication in which a client or machine (a client) is given a benefit (like sending a webpage) by another computer (a server) within the network.
* Collectively, the TCP/IP suite of conventions is classified as stateless, which suggests each client request is considered new since it is irrelevant to past requests. Being stateless liberates up network paths so they can be utilized continuously.
* The transport layer itself, is stateful. It transmits a single message, and its connection remains open until all the packets in a message have been received and reassembled at the destination.
* The TCP/IP model differs from the seven-layer Open System Interconnection (OSI) model designed after it.

### Application/Uses of TCP/IP

Some Real-Time Applications are:

* **Simple Mail Transfer Protocol(SMTP):** It helps to send email to another email address.
* **File Transfer Protocol(FTP):** It is used for sending large files.
* **Dynamic Host Configure Protocol(DHCP):** It assigns the IP address.
* **Telnet:** Bi-directional text communication via a terminal application.
* **HyperText Transfer Protocol(HTTP):** Used to transfer the web pages.
* **Domain Name System(DNS):**It translates the website name to IP addresses.
* **Simple Network Time Protocol(SNTP):**It provides the time of a day to the network devices.

### Benefits of TCP/IP

* It is an **industry–standard demonstrate** that can be viably deployed in commonsense organizing problems.
* It is **interoperable**, i.e., it permits cross-platform communications among heterogeneous networks.
* It is an **open convention suite.** It isn’t claimed by any specific established and so can be utilized by any individual or organization.
* It may be **versatile, client-server engineering.** This permits systems to be included without disturbing the current services.
* It allots an **IP address to each computer on the organize,**hence making each device to be identifiable over the arrange. It allots each location a space title. It gives the title and addresses determination administrations.

### Challenges of TCP/IP:

* It is **not generic in nature.** So, it comes up short to represent any protocol stack other than the TCP/IP suite. For the case, it cannot depict the Bluetooth connection.
* It does **not clearly isolate** the concepts of services, interfacing, and protocols. So, it isn’t appropriate to portray unused advances in modern networks.
* It does **not recognize between the data link and the physical layers,**which has exceptionally distinctive functionalities.
* The **information interface layer** ought to concern with the **transmission of outlines.** On the other hand, the physical layer ought to lay down the physical characteristics of the transmission.
* In this, model the transport layer does not guarantee delivery of packets.
* Security: TCP/IP was originally designed for an open and trusting environment, and as a result, it is not inherently secure. This has led to a range of security challenges, including attacks such as DDoS, man-in-the-middle attacks, and other types of network-based attacks.
* Complexity: The TCP/IP protocol suite is highly complex, with many different protocols and layers that interact with each other. This complexity can make it difficult to troubleshoot network issues and can increase the likelihood of errors and misconfigurations.
* Scalability: While TCP/IP is highly scalable, there are limits to its scalability. As networks grow larger and more complex, it can become more difficult to manage and optimize TCP/IP-based networks.
* Congestion: TCP/IP was not designed with congestion management in mind, which can lead to issues such as network congestion and packet loss. This can result in reduced network performance and reliability.
* Legacy systems: TCP/IP is based on legacy technology that was designed in the 1970s and 1980s. While the protocol has been updated over the years, it can still struggle to support modern networking needs, such as real-time applications, mobile devices, and the Internet of Things.
* IPv4 address depletion: The IPv4 address space is limited and has been depleted in many regions, which has led to the widespread adoption of IPv6. However, the transition from IPv4 to IPv6 has been slow, and many networks still rely on IPv4.

# Architecture of Cloud Computing

## What is Cloud Computing?

**Cloud Computing** means storing and accessing the data and programs on remote servers that are hosted on the internet instead of the computer’s hard drive or local server. Cloud computing is also referred to as Internet-based computing, it is a technology where the resource is provided as a service through the Internet to the user. The data that is stored can be files, images, documents, or any other storable document. Transparency, scalability, security and intelligent monitoring are some of the most important constraints which every cloud infrastructure should experience. Current research on other important constraints is helping cloud computing system to come up with new features and strategies with a great capability of providing more advanced cloud solutions.

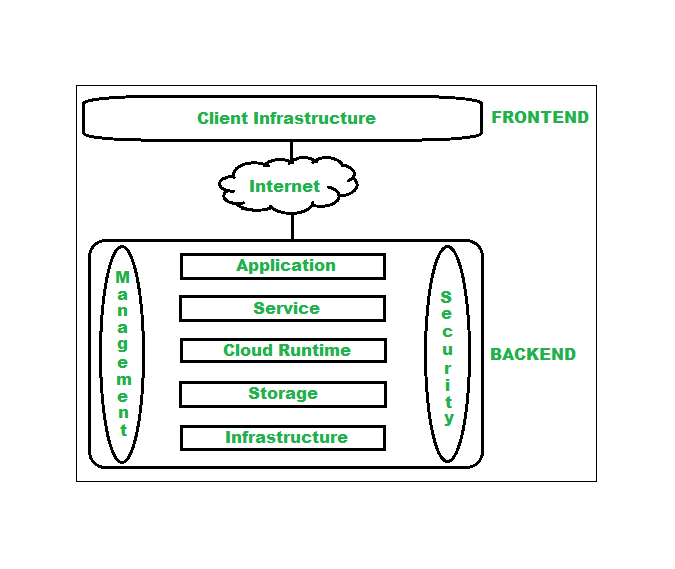
## **Cloud Computing Architecture**

Architecture of cloud computing is the combination of both [SOA (Service Oriented Architecture)](https://www.geeksforgeeks.org/service-oriented-architecture/) and EDA (Event Driven Architecture). Client infrastructure, application, service, runtime cloud, storage, infrastructure, management and security all these are the components of cloud computing architecture.

The cloud architecture is divided into 2 parts, i.e.

1. Frontend
2. Backend

The below figure represents an internal architectural view of cloud computing.



*Architecture of Cloud Computing*

### **1. Frontend**

Frontend of the cloud architecture refers to the client side of cloud computing system. Means it contains all the user interfaces and applications which are used by the client to access the cloud computing services/resources. For example, use of a web browser to access the cloud platform.

### **2. Backend**

Backend refers to the cloud itself which is used by the service provider. It contains the resources as well as manages the resources and provides security mechanisms. Along with this, it includes huge storage, virtual applications, virtual machines, traffic control mechanisms, deployment models, etc.

## Components of Cloud Computing Architecture

Following are the components of Cloud Computing Architecture

1. **Client Infrastructure –** Client Infrastructure is a part of the frontend component. It contains the applications and user interfaces which are required to access the cloud platform. In other words, it provides a GUI( Graphical User Interface ) to interact with the cloud.
2. **Application**: Application is a part of backend component that refers to a software or platform to which client accesses. Means it provides the service in backend as per the client requirement.
3. **Service**: Service in backend refers to the major three types of cloud based services like [SaaS, PaaS and IaaS](https://www.geeksforgeeks.org/cloud-based-services/). Also manages which type of service the user accesses.
4. **Runtime Cloud**: Runtime cloud in backend provides the execution and Runtime platform/environment to the Virtual machine.
5. **Storage:**Storage in backend provides flexible and scalable storage service and management of stored data.
6. **Infrastructure:**Cloud Infrastructure in backend refers to the hardware and software components of cloud like it includes servers, storage, network devices, virtualization software etc.
7. **Management:**Management in backend refers to management of backend components like application, service, runtime cloud, storage, infrastructure, and other security mechanisms etc.
8. **Security:**Security in backend refers to implementation of different security mechanisms in the backend for secure cloud resources, systems, files, and infrastructure to end-users.
9. **Internet:**Internet connection acts as the medium or a bridge between frontend and backend and establishes the interaction and communication between frontend and backend.
10. **Database:** Database in backend refers to provide database for storing structured data, such as SQL and NOSQL databases. Example of Databases services include Amazon RDS, Microsoft Azure SQL database and Google CLoud SQL.
11. **Networking:**Networking in backend services that provide networking infrastructure for application in the cloud, such as load balancing, DNS and virtual private networks.
12. **Analytics:**Analytics in backend service that provides analytics capabilities for data in the cloud, such as warehousing, business intelligence and machine learning.

## **Benefits of Cloud Computing Architecture**

* Makes overall cloud computing system simpler.
* Improves data processing requirements.
* Helps in providing high security.
* Makes it more modularized.
* Results in better disaster recovery.
* Gives good user accessibility.
* Reduces IT operating costs.
* Provides high level reliability.
* Scalability.

## Conclusion

Cloud Computing architecture provides a structural framework for designing, implementing and managing cloud-based solutions. Cloud Computing Architecture provides benefits like scalability, flexibility, and cost-effectiveness. It also solve related to security, reliability, and performance.

## Frequently Asked Questions related to Cloud Computing Architecture

### What are the 4 layers of cloud architecture in cloud computing?

*The 4 layer of cloud computing architectures are:*

1. *Physical Layer*
2. *Infrastructure Layer*
3. *Platform Layer*
4. *Application Layer*

### What are the four types of cloud architecture?

*The four type of cloud architecture are:*

1. *Private Cloud*
2. *Public Cloud*
3. *Hybrid Cloud*
4. *Multi Clouds*

# IAAS, PAAS and SAAS

IAAS, PAAS and SAAS are sometimes referred to as cloud service models or cloud computing service models. IaaS (Infrastructure as a Service) gives you virtual hardware like servers and storage. PaaS (Platform as a Service) provides tools for building and managing software applications. SaaS (Software as a Service) delivers ready-to-use software applications over the internet. In this article, we will learn the difference between IAAS, PAAS and SAAS.

## **What is IAAS?**

Infrastructure As A Service (IAAS) is means of delivering computing infrastructure as on-demand services. It is one of the three fundamental cloud service models. The user purchases servers, software data center space, or network equipment and rent those resources through a fully outsourced, on-demand service model. It allows dynamic scaling and the resources are distributed as a service. It generally includes multiple-user on a single piece of hardware.

It totally depends upon the customer to choose its resources wisely and as per need. Also, it provides billing management too.

### Characteristics of IAAS (**Infrastructure as a Service**)

* IAAS is like renting virtual computers and storage space in the cloud.
* You have control over the operating systems, applications, and development frameworks.
* Scaling resources up or down is easy based on your needs.

### Example of IAAS (Infrastructure As A Service)

* Amazon Web Services
* Microsoft Azure
* Google Compute Engine
* Digital Ocean

## **What is PAAS?**

Platform As A Service (PAAS) is a cloud delivery model for applications composed of services managed by a third party. It provides elastic scaling of your application which allows developers to build applications and services over the internet and the deployment models include public, private and hybrid.

Basically, it is a service where a third-party provider provides both software and hardware tools to the cloud computing. The tools which are provided are used by developers. PAAS is also known as Application PAAS. It helps us to organize and maintain useful applications and services. It has a well-equipped management system and is less expensive compared to IAAS.

### Characteristics of PAAS (**Platform as a Service**)

* PAAS is like a toolkit for developers to build and deploy applications without worrying about infrastructure.
* Provides pre-built tools, libraries, and development environments.
* Developers focus on building and managing applications, while the provider handles infrastructure management.
* It speeds up the development process and allows for easy collaboration among developers.

### Examples of PAAS (Platform as a Service)

* AWS Lambda
* Google App Engine
* Google Cloud
* IBM Cloud

## **What is SAAS?**

Software As A Service (SAAS) allows users to run existing online applications and it is a model software that is deployed as a hosting service and is accessed over Output Rephrased/Re-written Text the internet or software delivery model during which software and its associated data are hosted centrally and accessed using their client, usually an online browser over the web. SAAS services are used for the development and deployment of modern applications.

It allows software and its functions to be accessed from anywhere with good internet connection device and a browser. An application is hosted centrally and also provides access to multiple users across various locations via the internet.

### Characteristics of SAAS (Software**as a Service**)

* Applications are ready to use, and updates and maintenance are handled by the provider.
* You access the software through a web browser or app, usually paying a subscription fee.
* It’s convenient and requires minimal technical expertise, ideal for non-technical users.

### Example of SAAS (Software as a Service)

* Salesforce
* Google Workspace apps
* Microsoft 365
* Trello
* Zoom
* Slack
* Adobe Creative Cloud

## **Difference between IAAS, PAAS and SAAS**

| **Basis Of** | **IAAS** | **PAAS** | **SAAS** |
| --- | --- | --- | --- |
| **Stands for** | Infrastructure as a service. | Platform as a service. | Software as a service. |
| **Uses** | IAAS is used by network architects. | PAAS is used by developers. | SAAS is used by the end user. |
| **Access** | IAAS gives access to the resources like virtual machines and virtual storage. | PAAS gives access to run time environment to deployment and development tools for application. | SAAS gives access to the end user. |
| **Model** | It is a service model that provides virtualized computing resources over the internet. | It is a cloud computing model that delivers tools that are used for the development of applications. | It is a service model in cloud computing that hosts software to make it available to clients. |
| **Technical understanding.** | It requires technical knowledge. | Some knowledge is required for the basic setup. | There is no requirement about technicalities company handles everything. |
| **Popularity** | It is popular among developers and researchers. | It is popular among developers who focus on the development of apps and scripts. | It is popular among consumers and companies, such as file sharing, email, and networking. |
| **Percentage rise** | It has around a 12% increment. | It has around 32% increment. | It has about a 27 % rise in the cloud computing model. |
| **Usage** | Used by the skilled developer to develop unique applications. | Used by mid-level developers to build applications. | Used among the users of entertainment. |
| **Cloud services.** | Amazon Web Services, sun, vCloud Express. | Facebook, and Google search engine. | MS Office web, Facebook and Google Apps. |
| **Enterprise services.** | AWS virtual private cloud. | Microsoft Azure. | IBM cloud analysis. |
| **Outsourced cloud services.** | Salesforce | Force.com, Gigaspaces. | AWS, Terremark |
| **User Controls** | Operating System, Runtime, Middleware, and Application data | Data of the application | Nothing |
| **Others** | It is highly scalable and flexible. | It is highly scalable to suit the different businesses according to resources. | It is highly scalable to suit the small, mid and enterprise level business |

## **Advantages of IaaS**

* The resources can be deployed by the provider to a customer’s environment at any given time.
* Its ability to offer the users to scale the business based on their requirements.
* The provider has various options when deploying resources including virtual machines, applications, storage, and networks.
* It has the potential to handle an immense number of users.
* It is easy to expand and saves a lot of money. Companies can afford the huge costs associated with the implementation of advanced technologies.
* Cloud provides the architecture.
* Enhanced scalability and quite flexible.
* Dynamic workloads are supported.

## **Disadvantages of IaaS**

* Security issues are there.
* Service and Network delays are quite a issue in IaaS.

## When to Use IaaS

Choosing Infrastructure as a Service (IaaS) sets businesses up for future success, irrespective of their size. With IaaS, one can easily adjust their resources as your business grows or changes, all without dealing with physical hardware. This means one have to only pay for what they need, keeping costs in check. Plus, they have total control over their setup, allowing them to customize it to fit your needs and keep up with industry standards. If they run into any issues, they can count on support from their provider to help out. And with IaaS, they are always up-to-date with the latest tech advancements, keeping them competitive in the market. So, by using IaaS, businesses can stay flexible, save money, and keep up with the times, paving the way for future innovation and success.

## **Advantages of PaaS**

* Programmers need not worry about what specific database or language the application has been programmed in.
* It offers developers the to build applications without the overhead of the underlying operating system or infrastructure.
* Provides the freedom to developers to focus on the application’s design while the platform takes care of the language and the database.
* It is flexible and portable.
* It is quite affordable.
* It manages application development phases in the cloud very efficiently.

## **Disadvantages of PaaS**

* Data is not secure and is at big risk.
* As data is stored both in local storage and cloud, there are high chances of data mismatch while integrating the data.

## When to Use PaaS

PaaS is ideal when developers prioritize cost-effectiveness and efficiency in creating unique applications. By unloading tasks like software updates and security patches, PaaS enables developers to focus on the creative aspects of app development, such as designing, testing, and deploying. Use PaaS when you want to streamline development, reduce time spent on maintenance, and maximize focus on innovation.

## **Advantages of SaaS**

* It is a cloud computing service category providing a wide range of hosted capabilities and services. These can be used to build and deploy web-based software applications.
* It provides a lower cost of ownership than on-premises software. The reason is it does not require the purchase or installation of hardware or licenses.
* It can be easily accessed through a browser along a thin client.
* No cost is required for initial setup.
* Low maintenance costs.
* Installation time is less, so time is managed properly.

## **Disadvantages of SaaS**

* Low performance.
* It has limited customization options.
* It has security and data concerns.

## Benefits of Cloud Computing

### Cost Efficiency

Cloud computing eliminate the need for upfront investments in hardware and infrastructure, allowing businesses to pay only for the resources they use on a subscription basis, and reducing overall IT costs.

### 2. Scalability

[Cloud services](https://cloud.synapseindia.com/) can be easily scaled up or down to accommodate fluctuating workloads and business needs, providing organizations with the flexibility to expand or contract resources as required.

### 3. Accessibility

Cloud computing enables remote access to data and applications from anywhere with an internet connection, allowing employees to collaborate effectively and work from any location.

### 4. Reliability and Redundancy

Cloud providers typically offer high levels of reliability and redundancy, with built-in backup and disaster recovery capabilities to ensure data integrity and minimize downtime.

### 5. Security

Cloud providers invest heavily in security measures to protect data, applications, and infrastructure from cyber threats, offering robust encryption, access controls, and compliance certifications to safeguard sensitive information.

### 6. Innovation

Cloud computing enables rapid deployment of new applications and services, allowing businesses to experiment, innovate, and bring products to market faster than traditional IT environments.

Overall, cloud computing services empower businesses to increase agility, reduce costs, improve productivity, and drive innovation in today's digital economy.

## Challenges of Cloud Computing for Businesses

While cloud computing benefits offer numerous businesses, it also comes with Cloud Computing Challenges that organizations need to address:

### 1. Understand App Requirements

Clearly define the functionality you want to add to your app. Identify specific features or capabilities that need to be implemented or improved.

### 2. Prototype and Experiment

Create prototypes or proofs-of-concept using the selected frameworks to evaluate their suitability for your app. Experiment with different frameworks to compare their ease of use, flexibility, and performance.

### 3. Consider Future Scalability and Maintenance

Anticipate future scalability requirements and the potential impact on maintenance and updates. Choose frameworks that align with your app's long-term goals and roadmap.

### 4. Seek Expert Advice

Consult with experienced iOS developers or industry experts to get recommendations and insights based on their expertise and experience.

### 5. Make an Informed Decision

Based on your research, evaluation, and considerations, choose the iOS framework that best meets your app's requirements, development constraints, and long-term objectives.

By following these steps, you can effectively choose the right iOS framework to enhance the functionality of your app and ensure a successful development process.

### 1. Security Concerns

Security remains a top concern for businesses considering [cloud computing services](https://www.synapseindia.com/article/cloud-solutions-of-synapseindia-ensures-smooth-business-operations) adoption. Data breaches, compliance issues, and unauthorized access are potential risks associated with storing sensitive information in cloud computing security.

### 2. Data Privacy

Businesses must ensure that their data is protected and compliant with relevant regulations, such as GDPR or HIPAA, when stored or processed in the cloud. Maintaining data privacy and confidentiality is critical to maintaining trust with customers and stakeholders.

### 3. Compliance Requirements

Different industries have specific regulatory requirements governing data storage, processing, and transmission. Businesses must ensure that their cloud computing service providers comply with relevant regulations to avoid penalties and legal issues.

### 4. Downtime and Reliability

Cloud service outages or downtime can disrupt business operations and impact productivity. Organizations need to consider the reliability and uptime guarantees offered by cloud providers and have contingency plans in place to mitigate potential disruptions.

### 5. Vendor Lock-In

Businesses may face challenges if they decide to switch cloud computing providers due to vendor lock-in. Migrating data and applications between cloud platforms can be complex, time-consuming, and costly, limiting flexibility and hindering innovation.

**Introduction to cloud based IoT Platforms like IBM, Thingspeak, AWS**

### **1. Amazon Web Services (AWS)**

AWS has the largest number of services compared to other IoT platforms. It is, however, the most expensive of all the platforms in our IoT platforms comparison. AWS provides IoT services for both the cloud and edge software.

With edge software, developers are able to collect data, connect devices, and make the right decisions with their applications even when they do not have an internet connection.

On the other hand, they can securely connect different devices or a group of devices, make sure that they are secure and healthy, and detect and respond to any action or alert raised by other Internet of Things (IoT) sensors and applications

#### The edge software solutions provided by AWS include;

* **Amazon FreeRTOS**: This is an operating system provided by AWS and used by microcontrollers. It is used primarily for making low-power and small edge devices easy to use, program, connect, secure, deploy, and manage. It integrates different software libraries with the FreeRTOS kernel – this is one of the most popular open-source OS used for microcontrollers. With Amazon FreeRTOS, developers can connect small devices to the AWS cloud services.
* **AWS IoT edge software**: You cannot have an IoT platform comparison without talking about AWS IoT edge software due to its ability to bring computing power closer to the data generation source. It makes it possible for applications to eliminate over-reliance on a centralized cloud when it comes to data processing.
* **AWS IoT Greengrass**: This solution plays a crucial role when it comes to ensuring that devices use the data they generate locally while at the same time relying on the cloud for services such as analytics, management, and storage.

#### The cloud services for IoT provided by AWS include;

* **AWS IoT Core**: This is a managed cloud service whose responsibility is to allow connected devices to interact with other devices as well as cloud applications securely. It can support many devices at the same time and route messages to endpoints securely and reliably.
* **AWS IoT Device Defender**: This is also a managed service that is used for securing IoT devices. Its main purpose is to audit all IoT configurations to ensure that they abide by IoT [security practices](https://www.31west.net/blog/cyber-security-it-security-and-data-security-a-complete-guide/).
* **AWS IoT Device Management**: This service is used for remotely managing, monitoring, and organizing IoT devices. Developers have the option to either register devices in bulk or individually and manage all permissions to ensure that the devices are secure all the time.
* **AWS IoT Analytics**: Just like the others above, the AWS IoT Analytics service is fully managed and is used for analyzing large volumes of data from IoT devices. With this service, developers do not have to worry about making the right decisions for their IoT applications as well as machine learning.
* **AWS Partner Device Catalog**: Developers can use this service to find hardware and other devices that help them build, explore, and get their IoT solutions to the market.
* **AWS IoT SiteWise**: This is a managed service used for organizing and collecting data from large industrial devices and equipment.
* **AWS IoT Things Graph**: This is a service used for connecting web services and devices visually when building IoT applications.
* **AWS IoT Events**: This service is used to help developers detect events generated by IoT applications and sensors and then respond to them.

Looking at the IoT platforms comparison in this article, you will realize that AWS provides the highest number of services. It is also one of the best platforms for developers who do not mind its cost.

### **2. Microsoft Azure**

Microsoft Azure IoT platform is composed of multiple cloud services used for connecting, monitoring, and controlling IoT devices and other assets. It is managed by Microsoft. It makes it to our IoT platforms comparison article because it is the second-largest platform after AWS. It is also cheaper than Google and AWS.

Microsoft Azure IoT solution is composed of IoT devices and back-end services that run in the cloud and communicate with each other. Developers get two options to build their solutions. These include PaaS (Platform as a Service) and SaaS (Software as a Service).

#### The SaaS solutions provided by Microsoft Azure include;

* **Azure IoT Cloud Services**: Azure provides developers with Azure IoT Cloud Services to connect their devices to the cloud and analyze data from their IoT devices.
* **Azure IoT Central**: This solution helps developers connect, manage, and monitor their IoT devices. They even get the option to choose a device type template and then test a basic IoT application for the operators of the device. This solution also allows developers to provision new devices. They can track its performance with SolarWinds. You do not require programming knowledge to use this service, something that has made it very popular.
* **IoT Hub Device Provisioning Service**: This works like a helper for the IoT Hub discussed below. It helps developers securely provision their devices to the Hub. They can even provision multiple devices at the same time instead of doing it individually.
* **IoT Hub**: Using this service, developers can connect different IoT devices with an IoT hub. The hub controls and monitors a large number of IoT devices. It also plays a crucial role when it comes to the bi-directional communication between the back-end and IoT devices.
* **Azure Maps**: Developers looking for geographic information for their mobile and web applications can use the Azure Maps service. It uses a set of APIs to create applications that run well on both mobile and desktop applications.
* **Time Series Insights**: This is a service used for visualizing, storing, and querying data that is collected or generated by IoT devices.
* **IoT Edge**: Working together with the IoT Hub, this service is used for analyzing data directly on the IoT devices instead of doing it in the cloud.

#### The PaaS solutions from Azure include;

* **Azure Digital Twins**: With this service, developers can create models that look like the physical environment. They can model the interactions and relationships between devices, spaces, and even people.
* **Azure IoT Solutions Accelerators**: This is composed of a number of PaaS solutions used for accelerating the development of IoT solutions. Developers can customize the provided IoT solution to match their requirements. This requires JavaScript and .NET skills to customize the visualization and back-end respectively.

### **3. IBM Watson IoT Cloud**

When it comes to IoT platforms comparison, IBM is known best for its support for industrial IoT solutions. This is the main reason why IBM is among the top five IoT platforms we have today. Its platform is known as the IBM Watson IoT platform.

The platform comes as a managed service that is hosted in the cloud to ensure that there is secure management, connection, and processing of data collected by IoT devices.

Together with the power brought by IoT, the IBM Watson IoT platform leverages other technologies such as blockchain, APIs (Applications Programming Interfaces), and artificial intelligence to ensure that enterprises can collect data from machines, equipment, and other devices and [implement secure API test cases](https://rapidapi.com/blog/api-testing/). This data can be used to gain insights into operations for better decision-making.

The service is built on the IBM cloud to make sure that it is scalable enough to adapt to changing business needs and allow them to expand without any problems. To ensure that there is instant processing of data collected from IoT devices, this service uses artificial intelligence for data analytics. This makes it easy for enterprises to get valuable insights from the data.

This platform is popular among companies, especially those manufacturing machines, appliances, and home devices. You will also find this solution in home appliances such as ovens, dishwashers, and washing machines.

#### IBM Watson IoT Cloud’s solutions include;

* **IBM IoT Blockchain Service**: This service is tasked with making sure that IoT devices and IoT, in general, integrate well with all business services in an immutable and shared ledger. With this service, IoT devices can send data and respond to events coming from business processes through a blockchain ledger. This ledger is shared by the business network. The Blockchain Service allows developers to provide analysis, improve visibility, and engage their users.
* **IBM IoT Analytics Service**: Again, IoT platforms comparison cannot lack analytics. This explains the reason why the top IoT platforms have an analytics service. This service allows developers to gain real-time data analytics with simplified data curation and ingestion. Developers can deploy this service in a hybrid environment, on-premise, or on the cloud.
* **IBM IoT Connection Service**: This solution works by integrating different services to make a multi-tenant, public SaaS solution.

### **4. Google IoT Cloud Platform**

Google is one of the top and most successful tech companies in the world today. When it comes to IoT platforms comparison, Google stands tall with the number of services provided. The best IoT solution from Google is the Cloud IoT Core. It is used to create innovative and secure solutions. It is the second most expensive IoT platform after AWS.

#### Some of the best IoT solutions from Google IoT Cloud Platform include;

* **Cloud IoT Core**: This is a managed solution used for managing, connecting, and consuming data collected from different connected devices. Developers get a complete solution with Cloud IoT Core, where they can collect, analyze, process, and visualize data. This happens in real-time. The Cloud IoT Core solution is integrated with other services such as Google Cloud Data Analytics to make it easy for developers to use IoT data for things like machine learning, visualization, and advanced analytics. It also comes with a device manager (used for configuring and managing individual devices), a database performance monitoring tool, and a protocol bridge (used for providing connection endpoints with load balancing.
* **Firebase**: Firebase can be described as an IoT and mobile development platform. It supports messaging over XMPP and HTTP from cloud to device and device to cloud. Developers get SDKs for Android, JavaScript, C++, and iOS.
* **Cloud IoT Edge**: This is an IoT solution tasked with extending the machine learning and data processing capabilities of Google Cloud in edge devices such as robotic arms, oil rigs, and wind turbines, among others. With this solution, these devices can make decisions locally instead of relying on the cloud. It runs on Linux and Android operating systems.
* **Cloud Pub/Sub**: Every IoT platforms comparison needs to include an analytics program. Google Cloud provides the Cloud Pub/Sub for analyzing scenarios involving device-to-cloud connections. It works by ingesting event streams and then ensuring that they are delivered for processing. With the delivery of data being handled by Cloud Pub/Sub, developers can focus on other areas of their IoT applications. It comes with client libraries for Python, Ruby, PHP, Objective-C for iOS, JavaScript, .NET, Java for Android, and Go.

### **5. Cisco IoT Cloud Connect**

Cisco is one of the best-performing companies when it comes to providing businesses with IT services. They promise to ensure that companies can seize the technology opportunities of tomorrow to expand and streamline their operations. Cisco believes that the cloud possesses all the opportunities that businesses need to expand.

Their IoT solutions are geared towards strengthening the relationship between customers and businesses. They also try to provide solutions that can help businesses make more money – a statement that you will rarely find with any other IoT platform. That is one of the reasons we cannot forget Cisco IoT Cloud Connect when talking about IoT platforms comparison.

The Cisco IoT Cloud Connect platform comes with several robust features that make it stand out from the rest. Some of these features include a centralized data management solution, edge computing, advanced security, and other industry cloud features. The platform is popular among developers working in the financial, predictive maintenance, healthcare, and home security industries.

#### Cisco is best known for its two solutions, namely IoT Control Center and the Kinetic IoT Operations Platform.

* **IoT Control Center**: The IoT Control Center services thousands of enterprise-grade customers and millions of mobile devices across the globe, making it the largest platform when it comes to cellular connectivity. It is also the best service provider when it comes to smart cars. This means that Cisco cannot be left behind when talking about IoT platforms comparison. Today, there are millions of devices being added to this service every day, especially because of its connectivity features such as 5G readiness, eSIM as a service, and machine learning.
* **Kinetic IoT Operations Platform**: This platform uses three components to connect different types of devices. It also manages data both in the cloud and at the network’s edge. Apart from this platform being fully compatible with the hardware from Cisco, it can also work with other products, as long as they are recommended by Cisco.