Unit III -
Introduction & IOT Technologies behind smart and intelligent devices 9hr

IoT Concepts, Introduction to IOT Communications, Telemetry vs IOT, Applications of IOT Communications, People, Processes and Devices.

Automation, asset management, telemetry, transportation, telematics. Telemetry and Telemetric; Report ocation, logistics, tracking and remote assistance; Next generation kiosks, self-service technology; Cellular IOT connectivity services.

Introduction to IoT:

Nowadays, the internet-based information architecture allows the exchange of services and goods between all elements, equipment and objects connected to the network. The IoT refers to the networked interconnection of those everyday objects, which are often equipped with some kind of intelligence.

Definition: Internet of Things (IoT) is a network of devices which can sense, accumulate and transfer data over the internet without any human intervention.

Fig 1. IoT

Internet of things or IoT is a system of connected devices through the internet. It involves mechanical devices, sensors, home appliances, vehicles, etc., apart from desktop, mobile, and laptop. These devices are designed in such a way that they can share data with other devices over the internet. IoT basically provides a platform for devices to interact and collaborate with each other.

The Internet was used for connection-oriented application protocols like HTTP (Hypertext Transfer Protocol) and SMTP (Simple Mail Transfer Protocol). However, nowadays a large number of smart devices communicate between themselves and to other control systems. This concept is known as M2M (Machine-to-Machine communications)

IoT Tutorial: Birth of IoT

The term “The Internet of Things” (IoT) was coined by **Kevin Ashton** in a presentation to Proctor & Gamble in 1999. He is a co-founder of MIT’s Auto-ID Lab. He pioneered RFID (used in bar code detector) for the supply-chain management domain. He also started Zensi, a company that makes energy sensing and monitoring technology. However, IoT was “born” sometime between 2008 and 2009. In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Nowadays there are about 25 billion of devices connected to the IoT. More or less a smart device per person.

The Internet of Things was a common topic used by the media at the beginning of the 21st Century with several major developments paving the way for the future of IoT. LG Electronics introduced the world's first refrigerator connected to the internet in 2000. Allowing consumers to do their food shopping online and make video calls. This invention was followed by a small rabbit-shaped robot in 2005 that could report the latest news, weather forecasts and stock market changes. While the first International Conference on Internet of Things was held in 2008 in Switzerland.

Today there are more than 27 billion devices connected to the Internet of Things, with experts expecting this number to rise to over 100 billion devices by 2030.

HOW IoT Works?

The IoT consists of sensors and devices collecting data from their surroundings. This data is then sent to the cloud by means of Wi-Fi, Bluetooth, LPWAN, satellite, or being connected directly to the internet via ethernet. When the data reaches the cloud, it is then processed by software programs. The information is then made available to the consumer in a user-friendly way. This information is communicated to the user to either check on the system or take action and affect the system.

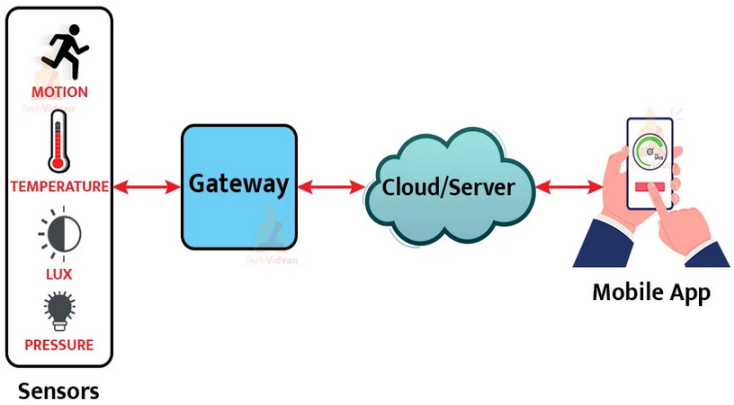


Fig 2 Working of IOT

IoT devices have **sensors embedded** into them. These sensors are capable of sensing their surroundings. The devices store the information in some form of data. These devices include appliances such as mobile phones, coffee machines, microwaves, geysers, fire alarms, Air conditioners, cars and so on.

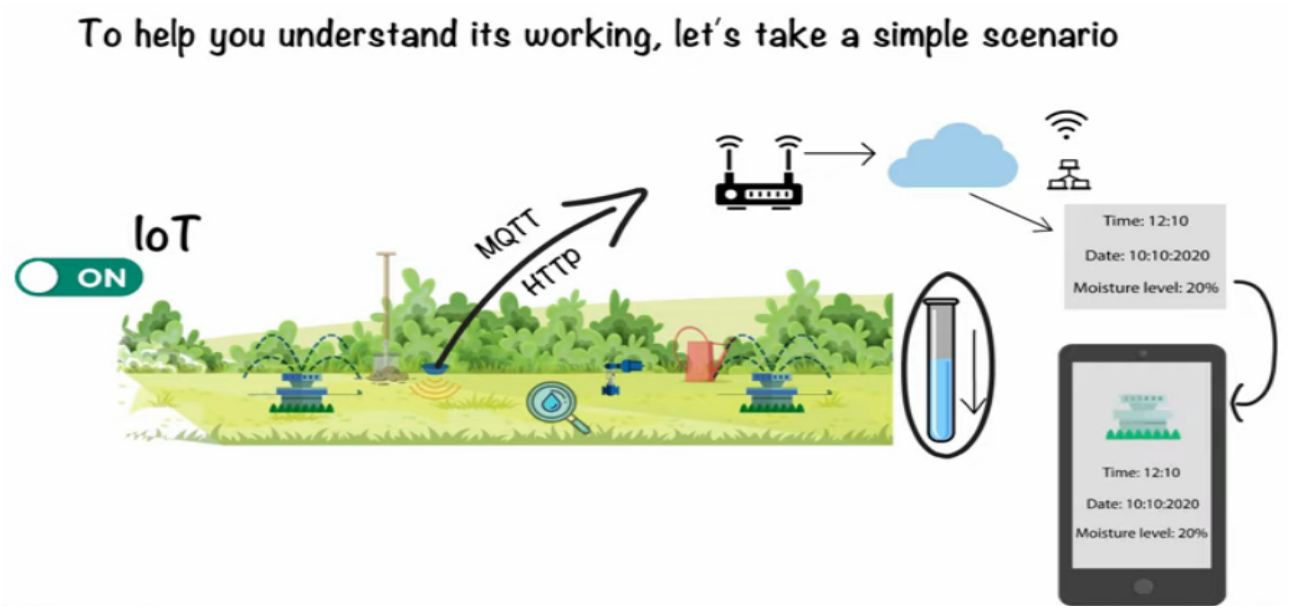
The sensors embedded in these devices **constantly emit data** about the surrounding and on the working information of these devices. **IoT serves as a platform** to dump all the data collected by these devices.

IoT platform includes **cloud servers and large databases**. The IoT platform acts on the data. It integrates and processes the information. Further, the platform analyses the data thoroughly to gather important details. The platform then sends back instructions based on the data provided.

Finally, the **data aggregation is shared with other devices** for better performance in the future. It is also done for improved user experience.

The future of IoT is bright and massive. According to a report generated by Business Insider, 24 billion IoT devices were installed in the year 2020. ITC predicts that IoT revenue will reach 300 billion dollars in the coming years. This generates large amounts of job opportunities in the technological industry and various other industries.

For Example we need to sprinkle water in Garden in specific time or when specific data received as an inout to IoT system. MQTT is an OASIS standard messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network. *HTTP* stands for Hypertext Transfer Protocol. · It is a protocol used to access the data on the World Wide Web (www).



Components of IoT

IoT has 4 components that describe the functioning of most of the IoT systems:

1. ***Sensors/Devices***

Things or Devices are the primary physical objects that are being monitored. Smart sensors attached to these devices are continuously collecting data from the device and transmitting it to next layer i.e. gateway.

Latest advancements in the semiconductor technology can produce micro smart sensors for various applications. For example, there are sensors in your phone such as GPS which track your location and guide you to your destination. Cameras sense human movement to click pictures. Try finding out other sensors in your mobile devices

2. ***Connectivity***

The IoT's major significant trend in recent years is the explosive growth of devices connected and controlled by the internet. The wide range of applications for IoT

technology means that the specifics can be very different from one device to the next, but there are basic characteristics shared by most.

There are many technologies that enable IoT. Crucial to the field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfil.

The sensors can be connected to the cloud through various mediums of communication and transports such as cellular networks, satellite networks, Wi-Fi, Bluetooth, wide-area networks (WAN), low power wide area network and many more.

3. ***Data processing***

*A*nalytics is the process of converting analog data from interconnected smart devices and sensors into usable insights that can be processed, interpreted, and used for detailed analysis. Intelligent analytics is a must for IoT technology for management and improvement of the entire system.

One of the utmost advantages of an efficient IoT system is real-time smart analytics which helps engineers to find out irregularities in the collected data and act fast to prevent an undesired scenario. Service providers can prepare for further steps if the information is collected accurately at the right time.

4. ***User Interface***

User interfaces are the visible, tangible part of the IoT system which can be accessible by users. Designers will have to make sure a well-designed user interface for minimum effort for users and encourage more interactions.

User interface design has higher significance in today's competitive market. Users will be interested in buying new devices or smart gadgets if it is user-friendly and compatible with common connectivity standards.

5. ***System Security***

Security is a critical element of IoT deployment, yet it is too often neglected in the development of systems. Everyday vulnerabilities in IoT are being exploited with malicious intent yet most of them can be prevented simply and cost-effectively. A secure system starts with the practice of eradicating vulnerabilities in IoT devices and equipping them with the means to resist, detect and recover from malicious attacks.

Real time Example of IoT

i. Say, we have an AC in our room, now the temperature sensor installed in it in the room will be integrated with a gateway. A gateway's purpose is to help connect the temperature sensor (inside the AC) to the Internet by making use of a cloud infrastructure.

ii. A Cloud/server infrastructure has detailed records about each and every device connected to it such as device id, a status of the device, what time was the device last accessed, number of times the device has been accessed and much more.

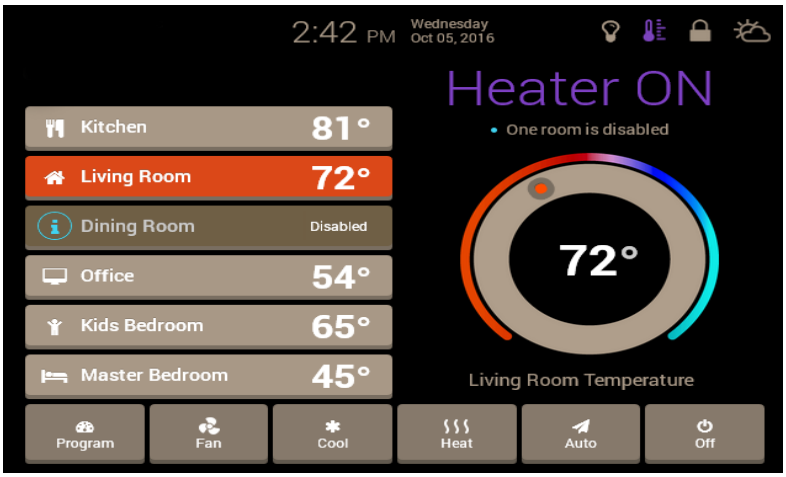
iii. A connection with the cloud then implement by making use of web services such as RESTful.

iv. We in this system, act as end-users and through the mobile app interact with Cloud (and in turn devices installed in our homes). A request will send to the cloud infrastructure with the authentication of the device and device information. It requires authentication of the device to ensure cybersecurity.

v. Once the cloud has authenticated the device, it sends a request to the appropriate sensor network using gateways.

vi. After receiving the request, the temperature sensor inside the AC will read the current temperature in the room and will send the response back to the cloud.

vii. Cloud infrastructure will then identify the particular user who has requested the data and will then push the requested data to the app. So, a user will get the current information about the temperature in the room, pick up through AC's temperature sensors directly on his screen.



Applications of IoT:

Smart Home: Smart homes are the revolution in the technical world. Switching on the lights as someone walks in, switching on AC and adjusting its temperature according to weather. Unlocks door for friends etc., is some of the features of smart homes.

Wearable's: These are the devices that have sensors embedded in them. One can wear them as a watch or specs. It broadly covers fitness and health-related data.

Smart cities: Smart cities are another application of IoT, which includes automated transport, energy management, environmental monitoring. Smart bins will alert municipal services that bins need to be emptied. Some other applications are auto-driven cars, industrial internet, iot in agriculture etc.

Characteristics of IoT

There are six main characteristics. Each characteristic encompasses a set of capabilities that make IoT a success.

1. Intelligence

IoT systems are extensively liked in the market because of their intelligence. A combination of algorithms and computer enables the system to inform change in the

environment and take appropriate actions. For example – Systems are intelligent enough to sense a sudden spike in temperature and trigger an alarm for fire.

2. *Connectivity*

Connectivity is the main characteristic of IoT as it enables the system to send data and stay connected to other devices. It provides system network accessibility and function collaboratively.

3. *Expressing*

IoT is all about interacting intelligently with the outer environment and humans. Expressing enables this interactivity. Expressing allows us to show output into the real world and input from people and the environment.

4. *Sensing*

Sensitivity means aware of the changes around us. Sensor technologies provide us with the means to create an experience that reflects an awareness of changes in the physical world and the people in it. It helps in expressing. This forms the input for the IoT system and provides a better understanding of the complex world around us.

5. *Energy*

Everything in this world is driven by energy. IoT systems are created smart enough to synthesize energy from the outer environment and conserve it. It is also made energy efficient to work for a longer duration.

6. *Security*

Safety and security is the most important feature of any system. If the system is not secure to cyber attack and illegal intervention, nobody will use it. IoT systems deal with personal data; that's why it's an obligation that all safety measure should be taken care of in this system. All IoT systems are secure enough to deal with personal data.

Advantages of IoT

Internet of things facilitates the several advantages in day-to-day life in the business sector. Some of its benefits are given below:

- **Efficient resource utilization:** If we know the functionality and the way that how each device work we definitely increase the efficient resource utilization as well as monitor natural resources.
- **Minimize human effort:** As the devices of IoT interact and communicate with each other and do lot of task for us, then they minimize the human effort.
- **Save time:** As it reduces the human effort then it definitely saves out time. Time is the primary factor which can save through IoT platform.
- **Enhance Data Collection:**
- **Improve security:** Now, if we have a system that all these things are interconnected then we can make the system more secure and efficient.

Disadvantages of IoT

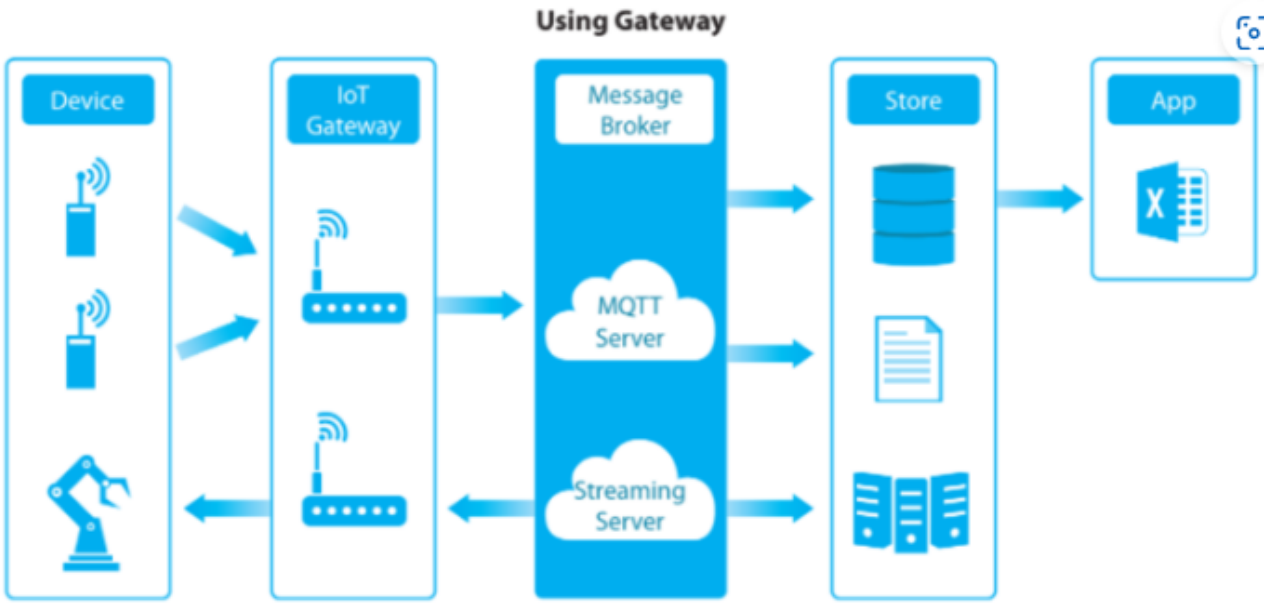
As the Internet of things facilitates a set of benefits, it also creates a significant set of challenges. Some of the IoT challenges are given below:

- ***Security:*** *IoT technology creates an ecosystem of connected devices. However, during this process, the system may offer little authentication control despite sufficient security measures.*
- **Privacy:** The use of IoT, exposes a substantial amount of personal data, in extreme detail, without the user's active participation. This creates lots of privacy issues.
- **Flexibility:** There is a huge concern regarding the flexibility of an IoT system. It is mainly regarding integrating with another system as there are many diverse systems involved in the process.
- **Complexity:** The design of the IoT system is also quite complicated. Moreover, it's deployment and maintenance also not very easy.
- **Compliance:** IoT has its own set of rules and regulations. However, because of its complexity, the task of compliance is quite challenging.

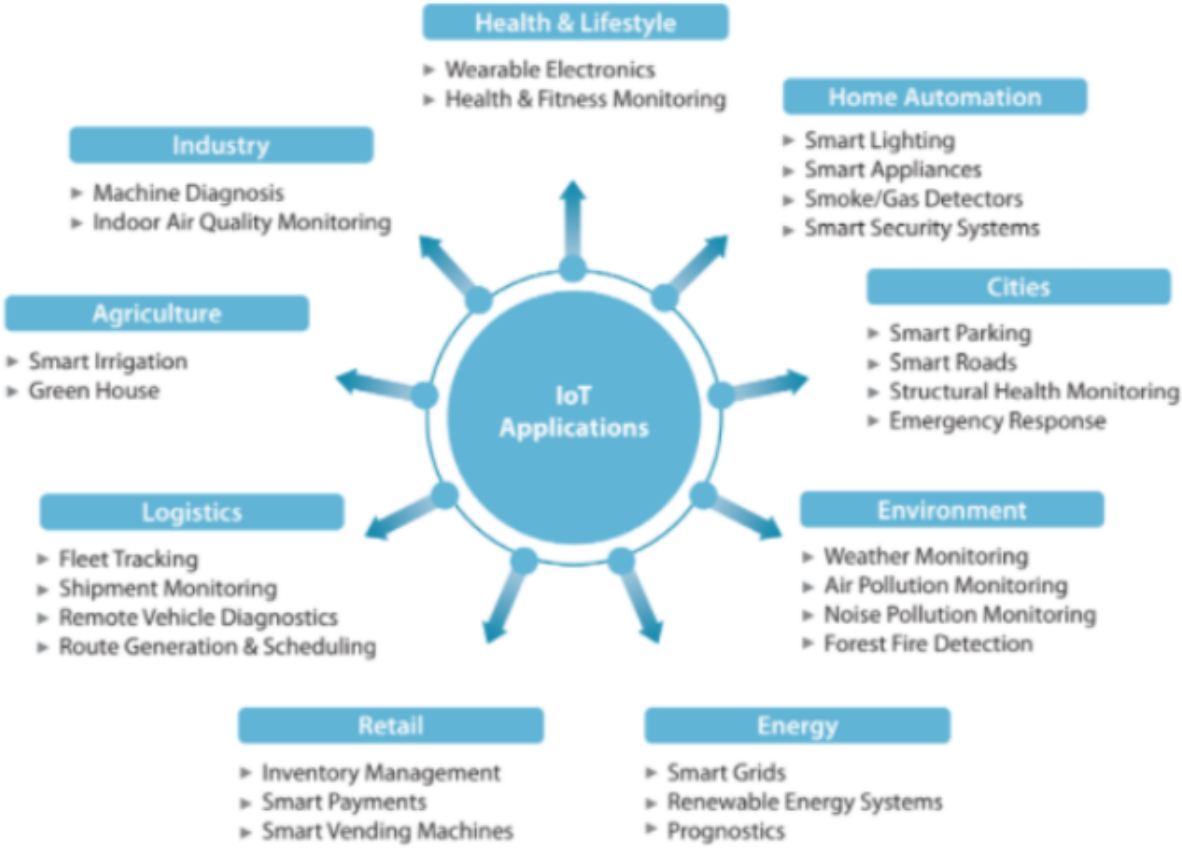
Basic Building Blocks of IoT

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

1. **Sensors** convert a non-electrical input to an electrical signal. Sensors are classified into two types: active and passive sensors. Whereas active sensors use and emit their own energy to collect real-time data (ex.: GPS, X-ray, radars), passive sensors use energy from external sources (ex: cameras). Additionally, sensors differentiate themselves by position, occupancy, and motion, velocity and acceleration, force, pressure, flow, humidity, light, radiation, temperature, etc.
2. **Processors** are the brain, the main part of the IoT system. They process the raw data captured by the sensors and extract valuable information. Examples of processors are microcontrollers and microcomputers
3. **Gateways** are the combination of hardware and software used to connect one network to another. Gateways are responsible for bridging sensor nodes with the external Internet or World Wide Web. The figure below depicts how using gateways works



4. **Applications** provide a user interface and effective utilization of the data collected. The figure above illustrates some examples of IoT applications.



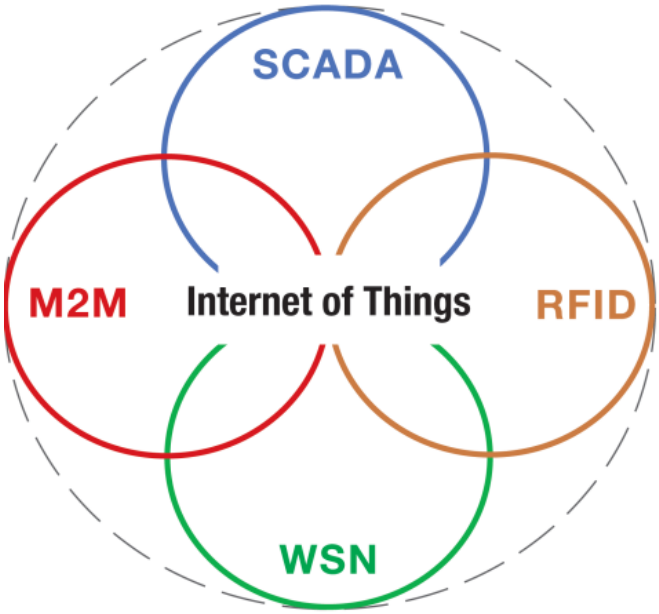
In summary, the IoT architecture comprises four basic building blocks: sensors, processors, gateways, and applications. Sensors are responsible for converting a non-electrical input to an electrical signal; processors “handle” the signals; gateways are used to connect a network to another, and, ultimately, an application offers a user interface and effective utilization of the data collected.

The internet of things (IoT) is the latest buzzword in the tech industry, and for good reason. It's an exciting concept that brings together internet technologies, sensors, and digital services like the cloud to create a global network of everyday objects that can be controlled via apps, websites, or other systems.

There are four pillars that unify the Internet of things. They all help you to communicate and connect with people and devices, and they work together to create a new Internet Age: an Internet Age where we can do things we never thought we could, and where we become more connected than ever before.

1. M2M [Machine to Machine]
2. SCADA [Supervisory Control and Data Acquisition:]
3. WSN [Wireless Sensor Network]
4. RFID [Radio-frequency identification]

Figure shows four pillars that unify the Internet of things

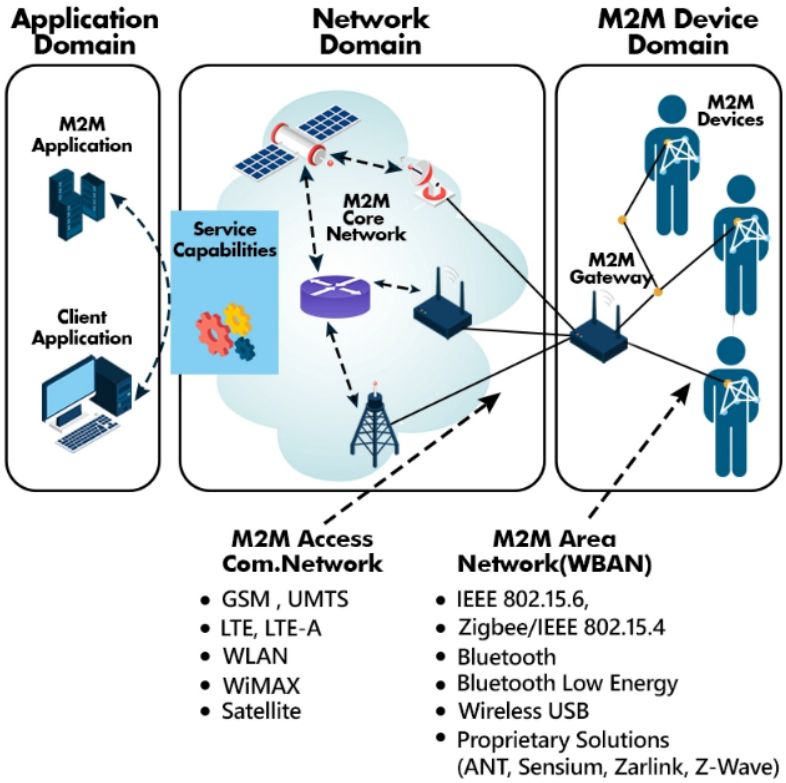


Piller 1: M2M: Machine to Machine

M2M stands for machine-to-machine, mobile-to-machine, and machine-to-mobile Communications. It is about networking the machines and devices that pervade our everyday lives. M2M communications will connect and enable an array of equipment from mainframes to everyday products (e.g., home appliances, vehicles, buildings) in order to unleash new levels of smart services" and commerce.

Machine to Machine (M2M) can be defined as a "direct, point-to-point" communication standard between devices usually of the same type. It's also meant for a specific on-premise application, which can be through wired or "non-Internet"-based wireless methods, such as Zigbee, RFID, Bluetooth, Wi-Fi, BLE, LoRaWAN, Sigfox, 6LoWPAN, and more.

Figure shows the Simple M2M Architecture



In order to develop and deploy an M2M architecture, we follow the latest standards such as ETSI, ANSI C12, and so on. The three main domains of M2M architecture are:

1. M2M application

As the name suggests, the M2M application domain offers applications to use M2M technology conveniently. Examples include server and end-user applications.

2. M2M network domain

M2M network domain acts as a bridge between the M2M application domain and the M2M device domain. It is made of two parts called the M2M core and M2M service capabilities.

3. M2M device domain

M2M device domain contains all the devices that can connect to the M2M network easily. The device domain can also be called the M2M area network. The M2M device domain includes devices that can connect directly over a network, devices that cannot directly connect to a network and may perhaps require an M2M gateway and proprietary devices.

Working of M2M

M2M devices send data across a network by sensing information. In order to send the data the machines use public networks such as cellular and ethernet. M2M comprises components such as RFID, sensors, Wi-Fi communication links and automated computer software programs that translate the incoming data to generate responses or actions.

Telemetry is one of the most renowned M2M communications. It has been in use since the beginning of the last century to transmit data. Developers used telephone lines for

communication and later moved to radio wave transmission signals in order to monitor the performance of the data that is gathered from remote locations.

The arrival of the internet improved the standards of wireless technology and now wireless communication is used in everyday real life applications such as hospitals, cities, stations, roads and so on.

Piller 2 Supervisory Control and Data Acquisition:

Supervisory Control And Data Acquisition (SCADA) is a system that uses computers, networks, and specialized hardware to monitor and control the physical equipment of an industrial process. Or

A SCADA system is a combination of hardware and software that enables the automation of industrial processes by capturing Operational Technology (OT) real-time data.

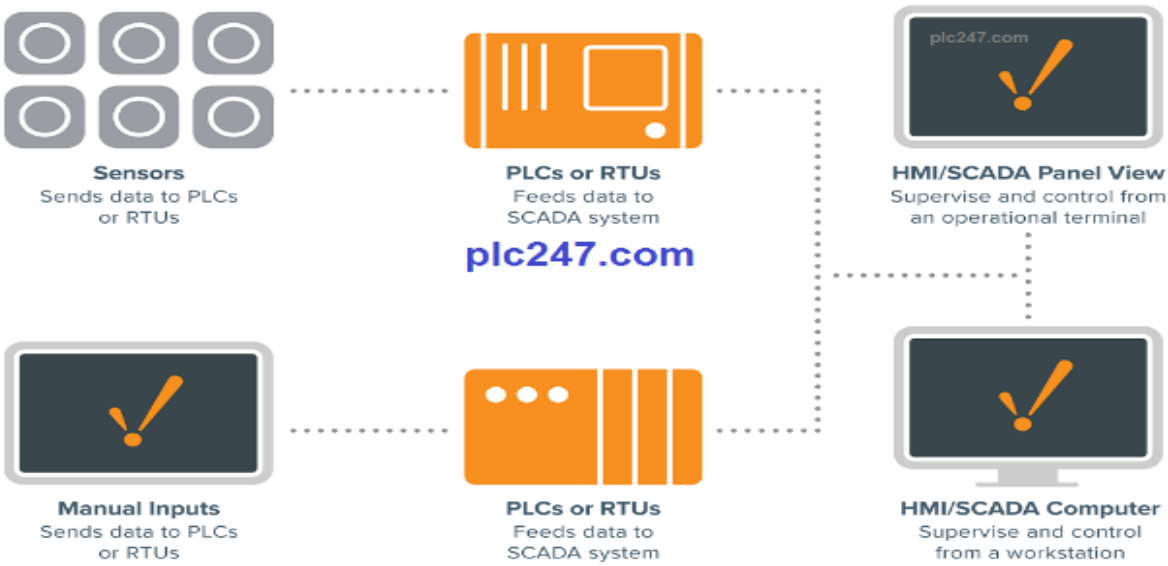
SCADA connects the sensors that monitor equipment like motors, pumps, and valves to an onsite or remote server. A SCADA system empowers organizations to:

1. Control processes locally or at remote locations
2. Acquire, analyze and display real-time data
3. Directly interact with industrial equipment such as sensors, valves, pumps, and motors
4. Record and archive events for future reference or report creation.

Basic Structure of SCADA:

All SCADA systems have the following main components:

1. Peripherals: including sensors, measuring devices, converters and actuators.
2. Intermediate data collection stations: are remote terminal units RTU (Remote Terminal Units) or PLC (Programmable Logic Controllers) that communicate with actuators.
3. Communication system: includes industrial communication networks, telecommunication equipment and multiplexing converters that transmit field-level data to control blocks and servers.
4. Monitoring control system: includes SCADA software and HMI (Human Machine Interface).



In the SCADA system, the data collection process is performed first in the process of RTUs scanning information obtained from actuators connected to them. The time taken to perform this task is called the internal scan time. Servers scan the RTUs (at a slower rate) to collect data from these RTUs.For control, the server sends the request signal to the RTU, thereby allowing the RTU to send the control signal directly to the device executing the task.

Examples of a SCADA system

1. Smart City
2. Smart Manufacturing

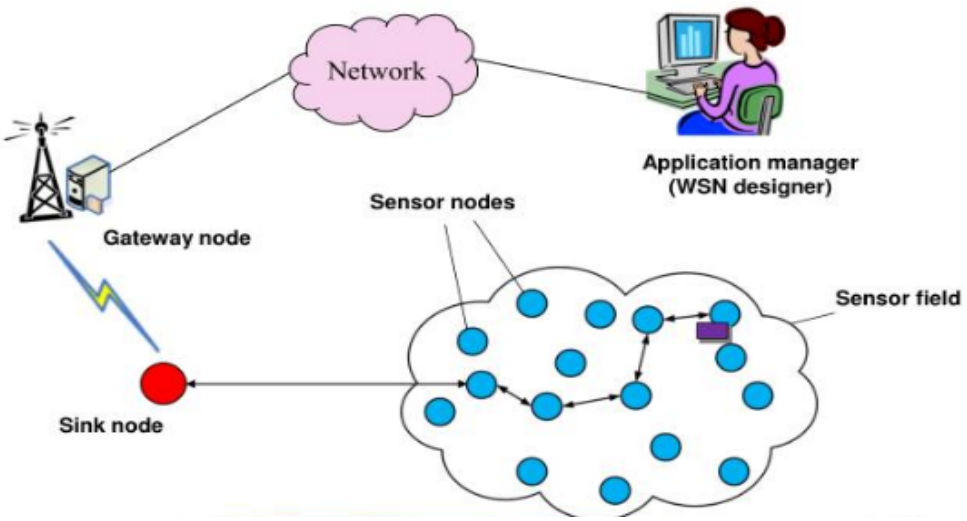
Piller 3: WSN: Wireless Server Network

A wireless sensor network (WSN) is a wireless network that contains distributed independent sensor devices that are meant to monitor physical or environmental conditions. A WSN consists of a set of connected tiny sensor nodes, which communicate with each other and exchange information and data. These nodes obtain information on the environment such as temperature, pressure, humidity or pollutant, and send this information to a base station. The latter sends the info to a wired network or activates an alarm or an action, depending on the type and magnitude of data monitored.

Typical applications include weather and forest monitoring, battlefield surveillance, physical monitoring of environmental conditions such as pressure, temperature, vibration, pollutants, or tracing human and animal movement in forests and borders.

They use the same transmission medium (which is air) for wireless transmission as wireless local area networks (WLANs). For nodes in a local area network to communicate properly, standard access protocols like IEEE 802.11 are available. However, this and the other protocols cannot be directly applied to WSNs.

Figure showing general working of WSN.



Piller 4:RFID : Radio-frequency identification

RFID (radio frequency identification) 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.

RFID belongs to a group of technologies referred to as Automatic Identification and Data Capture (AIDC). AIDC methods automatically identify objects, collect data about them, and enter those data directly into computer systems with little or no human intervention. RFID methods utilize radio waves to accomplish this. At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader (also called an interrogator). The reader then converts the radio waves to a more usable form of data. Information collected from the tags is then transferred through a communications interface to a host computer system, where the data can be stored in a database and analyzed at a later time.

There are two types of RFID :

1. Passive RFID – 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 125-134MHZ as low frequency, 13.56MHZ as a high frequency and 856MHZ to 960MHZ as ultra-high frequency.
2. 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.

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. Counterfeit prevention (e.g., in the pharmaceutical industry).

These 4 Pillars are used in making any IOT application.

Introduction to IOT Communications Model

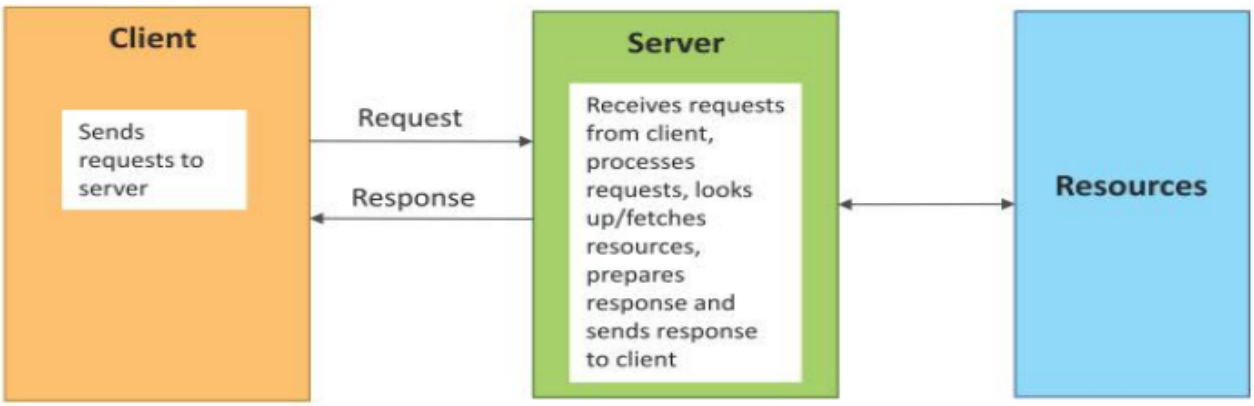
There are 4 communication model i) Request-Response ii) Publish-Subscribe iii)Push-Pull iv) Exclusive Pair

1. Request-Response:

Request-response model is communication model in which the client sends requests to the server and the server responds to the requests. When the server receives a request, it decides how to respond, fetches the data, retrieves resource representation, prepares the response, and then sends the response to the client.

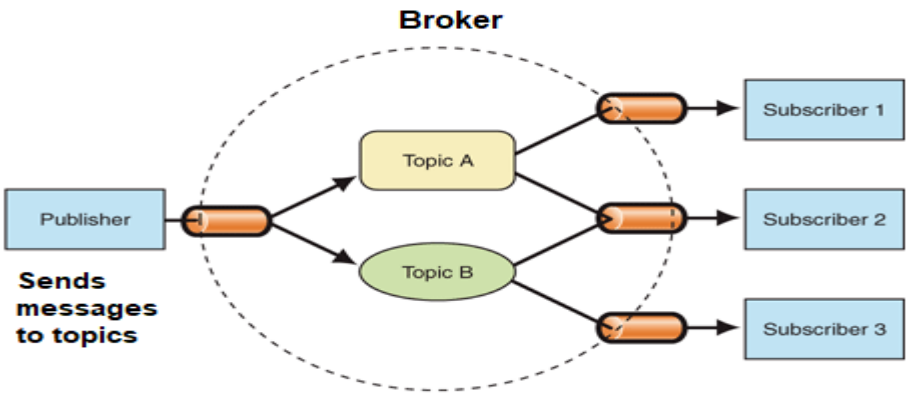
HTTP works as a request-response protocol between a client and server. A web browser may be the client, and an application on a computer that hosts a web site may be the server. Example: A client (browser) submits an HTTP request to the server; then the server returns a response to the client. The response contains status information about the request and may also contain the requested content.

Example: Sending a spreadsheet to the printer — the spreadsheet program is the client.



2. Publish-Subscribe

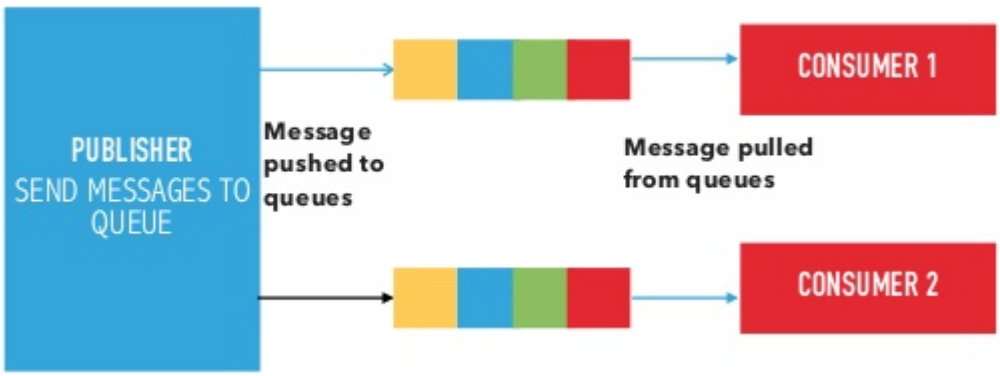
Publish-Subscribe is a communication model that involves publishers, brokers and consumers. Publishers are the source of data. Publishers send the data to the topics which are managed by the broker. Publishers are not aware of the consumers. Consumers subscribe to the topics which are managed by the broker. When the broker receive data for a topic from the publisher, it sends the data to all the subscribed consumers. Example: Public sensors with a massive base of uniform users that will use the data



3. Push-Pull

Push-Pull is a communication model in which the data producers push the data to queues and the consumers Pull the data from the Queues. Producers do not need to be aware of the consumers. Queues help in decoupling the messaging between the Producers and Consumers. Queues also act as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate rate at which the consumer pull data

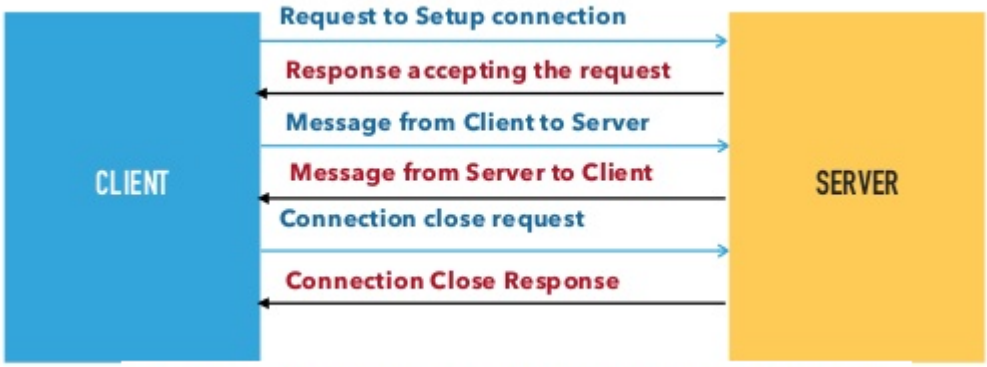
Example: Queues help in decoupling the messaging between the producers and consumers.



4. Exclusive Pair

Exclusive Pair is a bidirectional, fully duplex communication model that uses a persistent connection between the client and server. Connection is setup it remains open until the client sends a request to close the connection. Client and server can send messages to each other after connection setup. Exclusive pair is stateful communication model and the server is aware of all the open connections.

Example: The WebSocket-based communication API.



IOT Communication API's

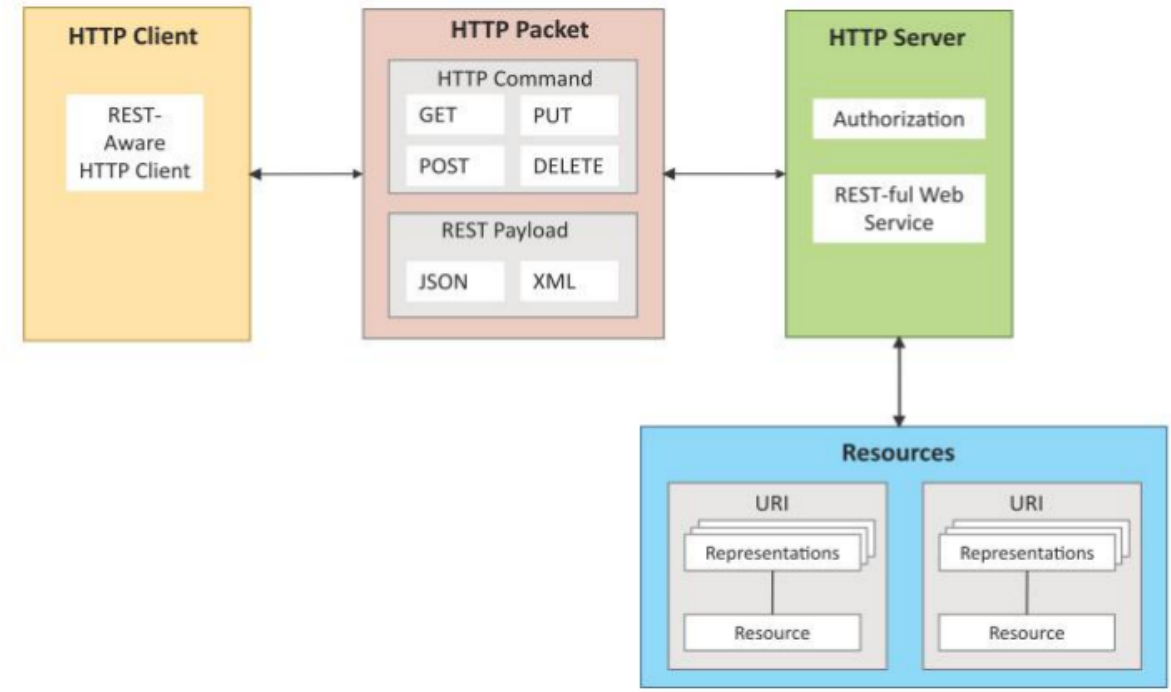
IoT APIs are the points of interaction between an IoT device and the internet and/or other elements within the network. As API management company Axway puts it, "APIs are tightly linked with IoT because they allow you to securely expose connected devices to customers, go-to-market channels and other applications in your IT infrastructure."

There are two types of API support

i) REST based communication APIs (Request-Response BasedModel)

ii) WebSocket based Communication APIs (Exclusive PairBasedModel)

REST is acronym for Representational State Transfer. It follows request response model. Representational State Transfer (REST) is a set of architectural principles by which you can design web services and web APIs that focus on a system's resources and how resource states are addressed and transferred. The REST architectural constraints are as follows:
The below figure shows the communication between client server with REST APIs



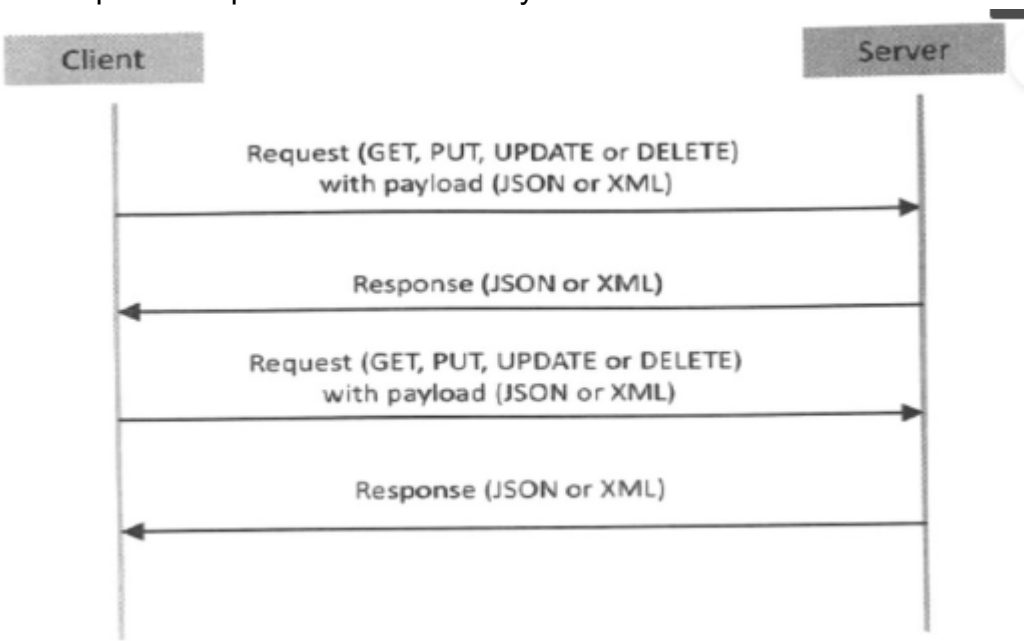
REST architecture constraints are as follows:

1. Client-Server: The principle behind client-server constraint is the separation of concerns. Separation allows client and server to be independently developed and updated.
2. Stateless: Each request from client to server must contain all the info. Necessary to understand the request, and cannot take advantage of any stored context on the server.
3. Cache-able: Cache constraint requires that the data within a response to a request be implicitly or explicitly labeled as cache-able or non-cacheable. If a response is

cacheable, then a client cache is given the right to reuse that response data for later, equivalent requests.

4. Layered System: constraints the behavior of components such that each component cannot see beyond the immediate layer with which they are interacting.
5. User Interface: constraint requires that the method of communication between a client and a server must be uniform.
6. Code on Demand: Servers can provide executable code or scripts for clients to execute in their context. This constraint is the only one that is optional.

The Request-Response model used by REST:



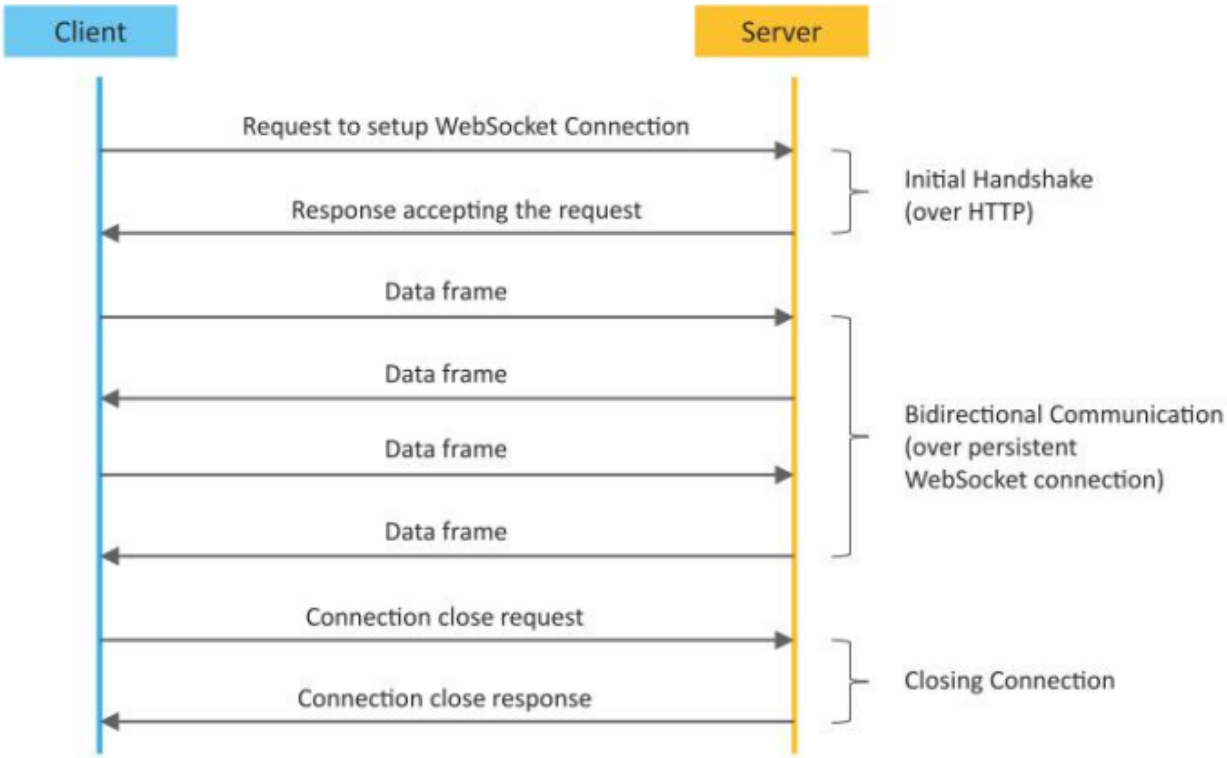
RESTful web service is a collection of resources which are represented by URIs. RESTful web API has a base URI(e.g: http://example.com/api/tasks/). The clients and requests to these URIs using the methods defined by the HTTP protocol(e.g: GET, PUT, POST or DELETE). A RESTful web service can support various internet media types Following table showing HTTP request method and action

HTTP Method	Resource Type	Action	Example
GET	Collection URI	List all the resources in a collection	http://example.com/api/tasks/ (list all tasks)
GET	Element URI	Get information about a resource	http://example.com/api/tasks/1/ (get information on task-1)
POST	Collection URI	Create a new resource	http://example.com/api/tasks/ (create a new task from data provided in the request)
POST	Element URI	Generally not used	
PUT	Collection URI	Replace the entire collection with another collection	http://example.com/api/tasks/ (replace entire collection with data provided in the request)
PUT	Element URI	Update a resource	http://example.com/api/tasks/1/ (update task-1 with data provided in the request)
DELETE	Collection URI	Delete the entire collection	http://example.com/api/tasks/ (delete all tasks)
DELETE	Element URI	Delete a resource	http://example.com/api/tasks/1/ (delete task-1)

B) WebSocket Based Communication APIs:

WebSocket APIs allow bi-directional, full duplex communication between clients and servers. WebSocket APIs follow the exclusive pair communication model. WebSocket APIs allow full duplex communication and do not require new connection to be setup for each message to be sent.

WebSocket communication begins with a connection setup request sent by the client to server. This request (is known as WebSocket handshake) is sent over the HTTP and server interprets it as an upgrade request. If server supports this websocket protocol, then it responds to the WebSocket handshake response. After connection setup, the client and server can send data/message to each other in full-duplex mode. This API is used to reduce network traffic and latency as there is no overhead for connection setup and termination request for each message. It suitable in IoT application that has low latency and high throughput requirements.


Client
Server
Request to setup WebSocket Connection
Response accepting the request
Initial Handshake
(over HTTP)
Data frame
Data frame
Data frame
Data frame
Bidirectional Communication
(over persistent
WebSocket connection)
Connection close request
Connection close response
Closing Connection

IoT Levels & Deployment Template

Developing an IoT Level Template system consists of the following components:

1. **Device:** These may be sensors or actuators capable of identifying, remote sensing, or monitoring.
2. **Resources:** These are software components on IoT devices for accessing and processing. storing software components or controlling actuators connected to the device. Resources also include software components that enable network access.
3. **Controller Service:** It is a service that runs on the device and interacts with web services. The controller service sends data from the device to the web service and receives commands from the application via web services for controlling the device.
4. **Database**: Stores data generated from the device. Database can be either local or in the cloud and stores the data generated by the IoT device.
5. **Web Service:** It provides a link between IoT devices, applications, databases, and analysis components. Web services serve as a link between the IoT device, application, database and analysis components. Web service can be either implemented using HTTP and REST principles (REST service) or using WebSocket protocol (WebSocket service).
6. **Analysis Component:** It performs an analysis of the data generated by the lol device and generates results in a form which are easy for the user to understand. .
7. **Application:** It provides a system for the user to view the system status and view product data. It also allows users to control and monitor various aspects of the IoT system. IoT applications provide an interface that the users can use to control and monitor various aspects of the IoT system. Applications also allow users to view the system status and view the processed

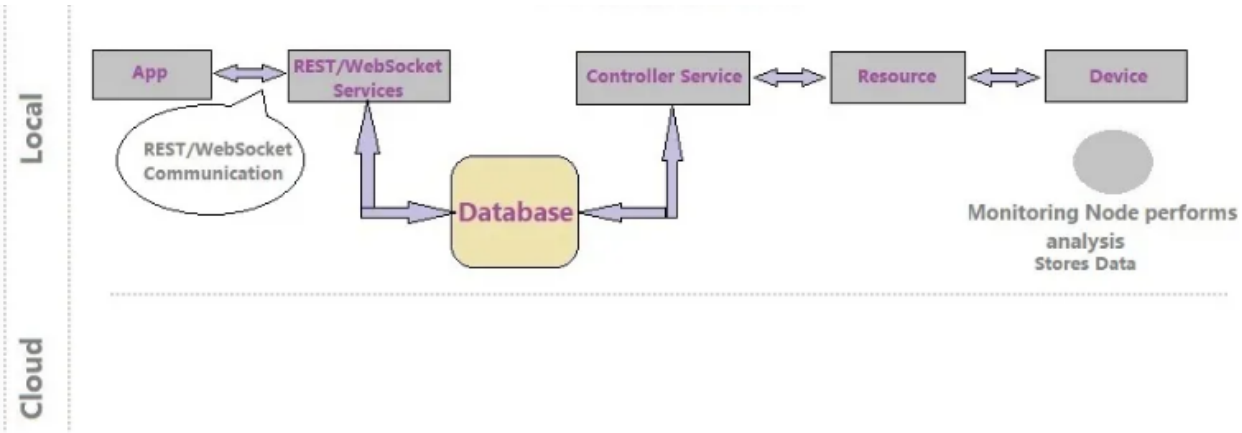
IoT Level-1

Level-1 IoT systems have a single node that performs sensing and/or actuation, stores data, performs analysis and host the application. Suitable for modelling low cost and low complexity solutions where the data involved is not big and analysis requirement are not computationally intensive. An e.g., of IoT Level1 is Home automation.

Example1: The system consist of a single node that allows controlling the lights and appliances in a home the device used in this system interfaces with the lights and appliances using electronic relay switches. The status information of each light or appliances is maintained in a local database. REST services deployed locally allow retrieving and updating the state of each lighter appliance in the status database. The controller service continuously monitors the state of each light or appliance by retrieving the light from the database.

Example2: We can understand with the help of an eg. let's look at the IoT device that monitors the lights in a house. The lights are controlled through switches. The database has maintained the status of each light and also REST services deployed locally allow retrieving and updating the state of

each light and trigger the switches accordingly. For controlling the lights and applications, the application has an interface. The device is connected to the internet and hence the application can be accessed remotely as well.



IoT Level-2

IoT Level2 has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself. An e,g., of Level2 IoT system for Smart Irrigation.

Example1: The system consists of a single node that monitors the soil moisture level and controls the irrigation system. The device used system collects soil moisture data from sensors. The controller service continuously monitors the moisture level. A cloud based REST web service is used for storing and retrieving moisture data which is stored in a cloud database. A cloud based application is used for visualizing the moisture level over a period of time which can help in making decision about irrigation schedule.

Example2 : Cloud-based application is used for monitoring and controlling the IoT system A single node monitors the soil moisture in the field Which is sent to the database on the cloud using REST APIS. The controller service continuously monitors moisture levels.

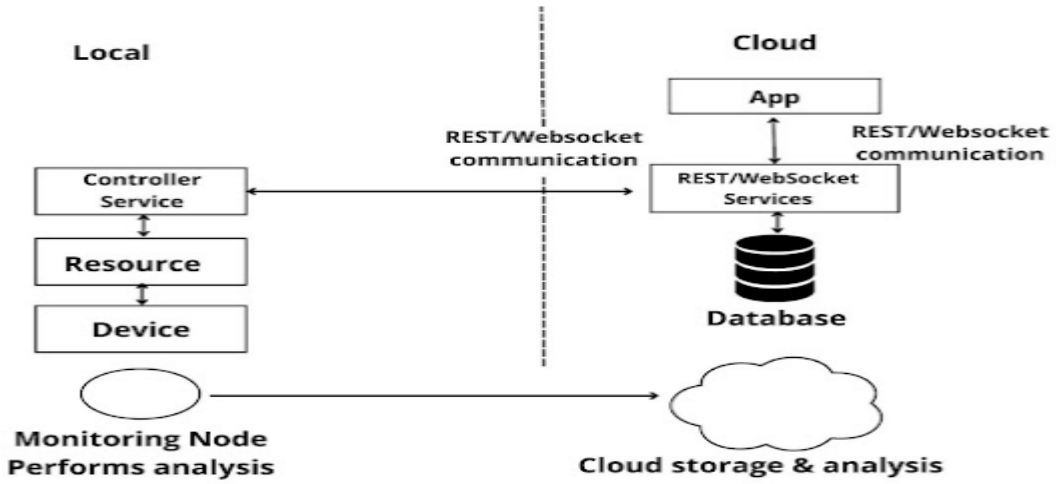


Fig. **IoT Level-2**

IoT Level-3

This System has a single node. Data is stored and analyzed in the cloud application is cloud based as shown in fig. Level3 IoT systems are suitable for solutions where the data involved is big and analysis requirements are computationally intensive.

Example: The system consists of a single node that monitors the vibration levels for the package being shipped. The device in this system uses accelerometer and gyroscope sensor for monitoring vibration levels. The controller serves in the sensor data to the cloud in a real time using a websocket service. The data is stored in the cloud and also visualizing the cloud based applications . The analysis components in the cloud can trigger alerts if the vibration level becomes greater than the threshold.

Example: A node is monitoring a package using devices like an accelerometer and gyroscope. These devices track vibration levels. Controller service sends sensor data to the cloud in the rear time using WebSocket APL. Data is stored in the cloud and visualized using a cloud-based application. The analysis component triggers an alert if vibration levels cross a threshold.

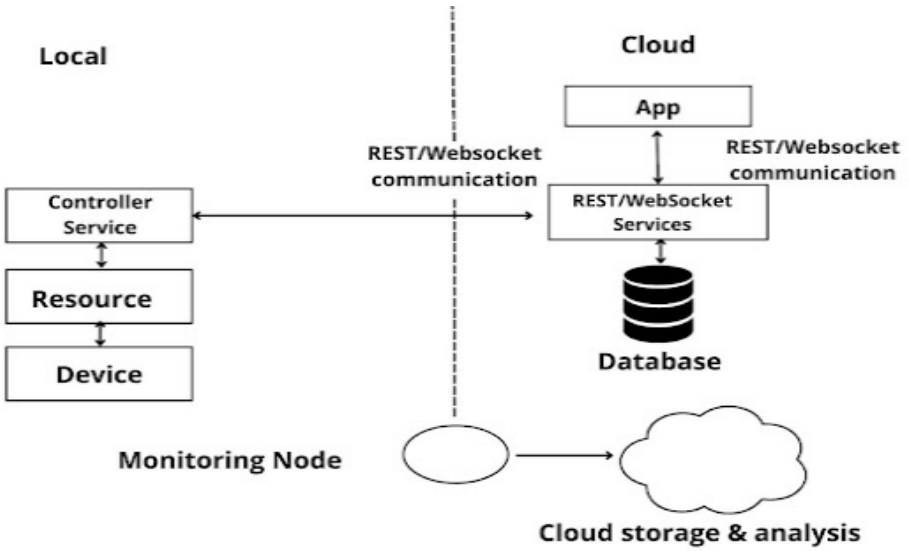


Fig. **IoT Level-3**

IoT Level-4

At this level, multiple nodes collect information and store it in the cloud. Local and rent server nodes are used to grant and receive information collected in the cloud from various devices. Observer nodes can process information and use it for applications but not perform control functions, this level is the best solution where data involvement is big, requirement analysis is comprehensive and multiple nodes are required,

Example: IoT System for Noise Monitoring. The system consists of multiple nodes placed in different locations for monitoring noise levels in an area. The nodes in this example are equipped with sound sensors. Nodes are independent of each other. Each node runs its owner controller service that sends the data to the cloud. The data is stored in cloud database. The analysis of data collected from a number of nodes is done in the cloud. A cloud based application is used for visualizing the aggregated data.

Example: Analysis is done on the cloud and the entire IoT system has monitored the cloud using an application. Noise monitoring of an area requires various nodes to function independently of each other. Each has its own controller service. Data is stored in a cloud database.

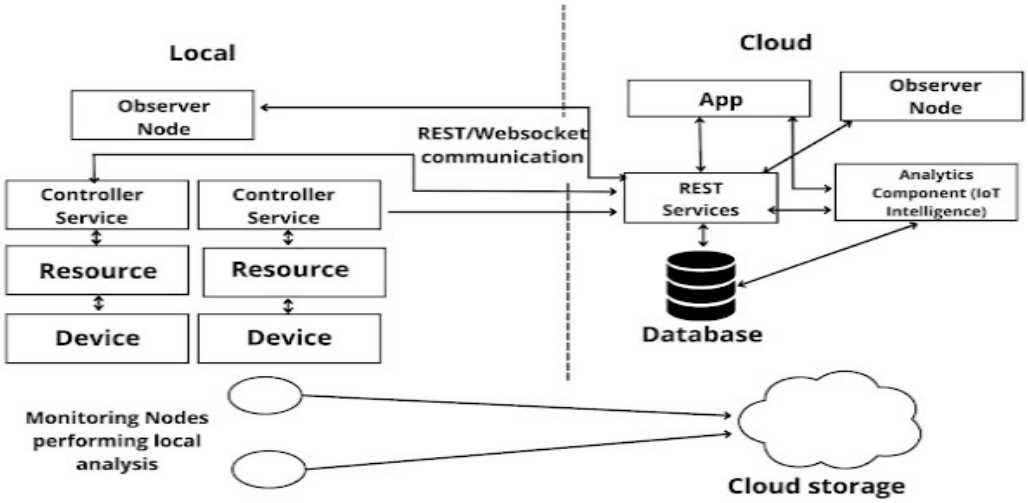


Fig. **IoT Level-4**

IoT Level-5

In this level Nodes present locally are of two types end odes and coordinator nodes End nodes collect data and perform sensing or actuation or both. Coordinator nodes collect data from end nodes and send it to the cloud. Data is stored and analyzed in the cloud. This level is best for WSN, where the data involved is big and the requirement analysis is comprehensive.

Example : IoT system for Forest Fire Detection. The system consists of multiple nodes placed in different locations for monitoring temperature, humidity and CO2 levels in a forest. The end nodes in this example are equipped with various sensors such as temperature, humidity and CO2. The coordinator node collects the data from the end nodes and act as a gateway that provides internet connectivity to the IoT system. The controller service on the coordinator device sends the collected data to the cloud. The data is stores in a cloud database. The analysis of data is done in the computing cloud to aggregate the data and make predictions. A cloud based applications is used for visualizing the data

Example: A monitoring system has various components: end nodes collect various data from the environment and send it to the coordinator node. The coordinator node acts as a gateway and allows the data to be transferred to cloud storage using REST API. The controller service on the coordinator node sends data to the cloud.

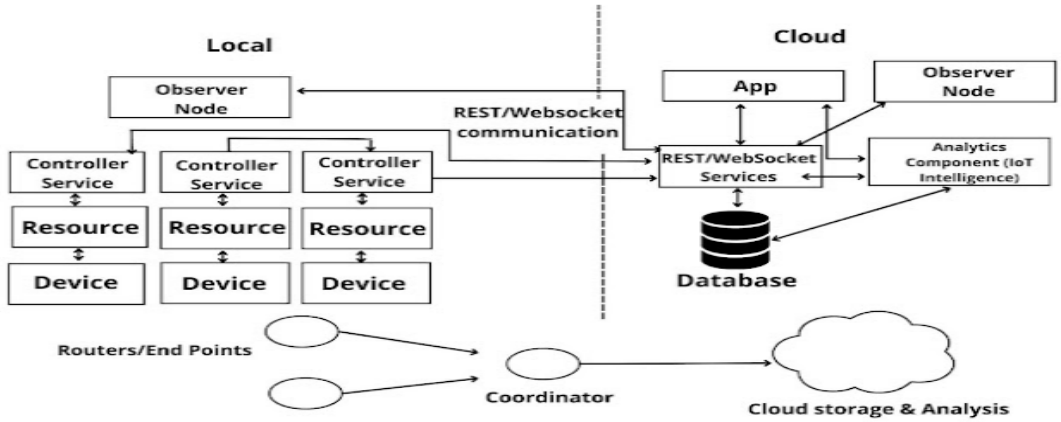


Fig. **IoT Level-5**

IoT Level-6

At this level, the application is also cloud-based and data is stored in the cloud-like of levels. Multiple independent end nodes perform sensing and actuation and send d to the cloud. The analytics components analyze the data and store the results in the cloud database. The results are visualized with a cloud-based application. The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes.

Example weather monitoring system The system consists of multiple nodes placed in different locations for monitoring temperatures,humidity and pressure in an area.the end nodes are equipped with various sensors(such as temperature,humidity and pressure).the end nodes send the data to the cloud realtime using a websocket service.the data is stored in a cloud database. The analysis of data is done in a cloud to aggregate a data and make predictions.a cloud based application is used for visualizing the data.

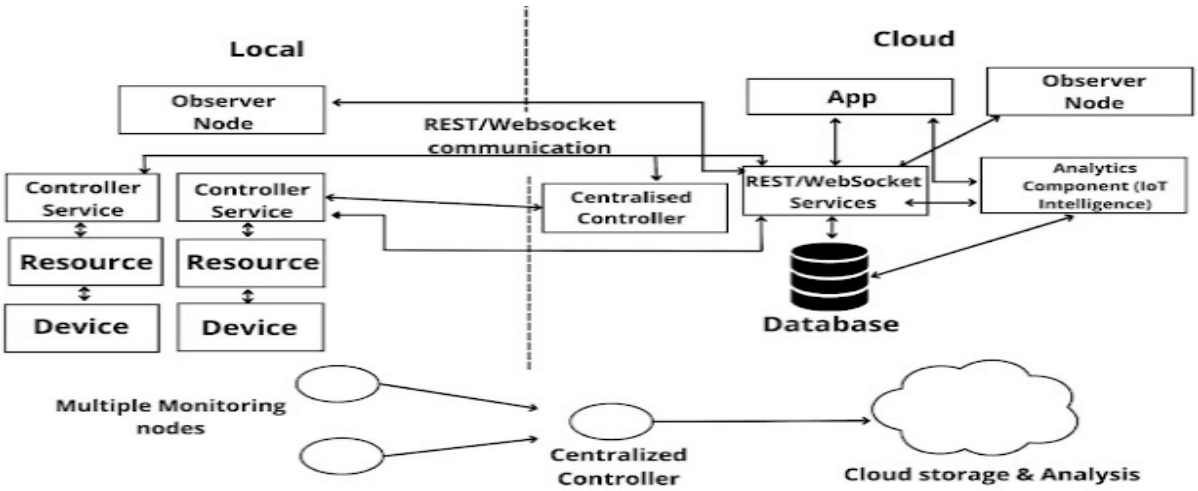


Fig. **IoT Level-6**

1. Define IOT and explain the characteristics of IoT.
2. Explain IoT component with suitable diagram [oct 2022]
3. Make note on IoT Functional Blocks
4. Make note on IoT communication APIs. [oct 2022]
5. Explain IoT Communication model with suitable diagram
6. Elaborate the functions of IoT Level3 with diagram
7. Explain the functions of IoT Level5 with diagram

8. Describe the functions IoT Level6 with block diagram.

What is telematics?

Telematics is a term that combines the words telecommunications and informatics to describe the use of communications and IT to transmit, store and receive information from devices to remote objects over a network.

Telecommunications and informatics are combined in the term telematics. It is frequently defined as “the integration of computer and Wi-Fi information and communication technologies to effectively communicate across vast systems to bolster a range of services.”

Presently, the meaning of telematics is widely associated with its application in vehicle detection and investments when having up-to-date data on their location is required for everyday business operations. GPS tracking is an instance of telematics in contemporary fleet management.

Further, telematics can improve fleet control and visibility for managers through aftermarket solutions that capture data from diverse fleets. Passenger-load vehicle fleet managers can accurately see how many passengers are in each vehicle. They can also maintain surveillance systems inside the cars. Video feeds inside the vehicles can also be stored for litigation or driver coaching. And finally, IoT-enabled telematics can reduce insurance costs while improving rider experiences.

Telematics Control Unit & IoT Cloud Connectivity

An automotive telematics solution fundamentally has four building blocks:

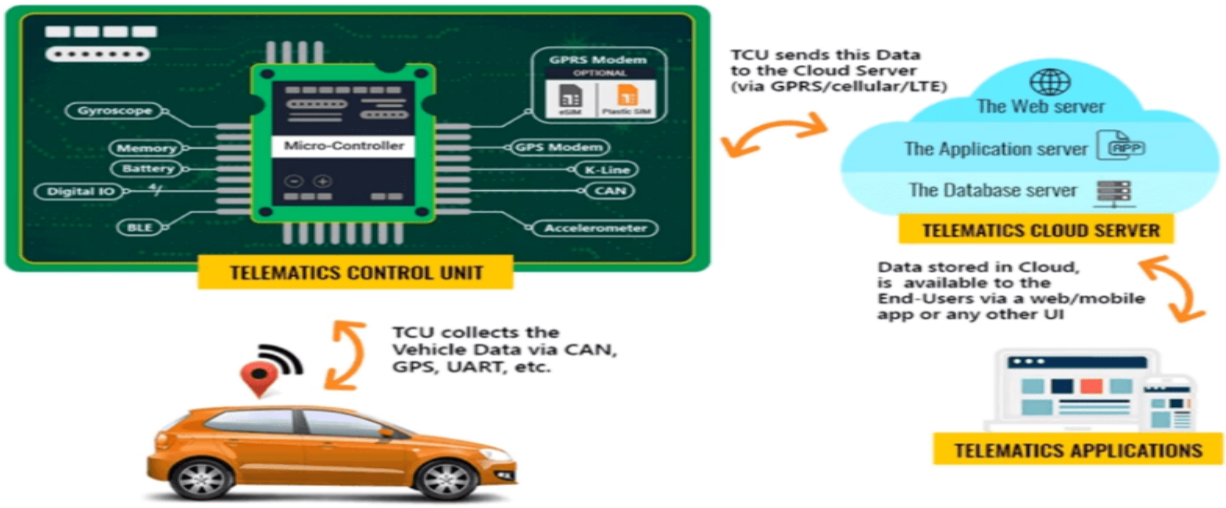
1. Vehicle ECU Network – Inside the vehicle, there is an interconnected network of automotive ECUs, which are small super computers. These ECUs help the Telematics Control Unit to collect vehicle data such as engine temperature, vehicle speed, diagnostics information, etc.
2. Telematics Control Unit (TCU) – This control unit is the heart of the telematics device in the vehicle. It has communication interfaces with the vehicle’s CAN bus and the IoT cloud server. The telematics control unit collects vehicle data such as diagnostics information, vehicle speed and real-time location and transmits this information to the IoT cloud. The communication with the cloud server is established through a cellular, LTE or GPRS network. This information is stored in the IoT cloud and can be accessed by connected mobile or web apps in the IoT ecosystem.

   The TCU also manages the memory and battery of the telematics device. Additionally, it streamlines the data that is shared with the driver through the Human Machine Interface (HMI) device or dashboard.
3. IoT Cloud Server – The information that is collected by the telematics control unit is shared with the cloud-based telematics server through a highly secure GPRS or cellular network. These data packets are also configured as MQTT messages before they are transmitted to the IoT cloud.

   On the IoT cloud platform, the data is extracted and stored in databases for processing.

4. Telematics Applications – The data from the cloud-based telematics server can be accessed by authorized personnel through a web, desktop or mobile application connected to the IoT ecosystem. This data can also be fed into a business intelligence system for further analysis and reporting.

Working of Telematics:
A telematics system operates by integrating a machine into an asset, including a tracking device or other real-time monitoring tools. The device then gathers critical asset performance information. Once the information is collected, the device sends it to a computer system, where it will be compiled, interpreted, and reviewed.
Data is collected using various methods, including hard-wired or self-fit gadgets and smartphone apps. The system considers multiple factors, such as natural conditions.
For example: When we say that a vehicle is integrated with telematics, it essentially means that it is fitted with a crash-resistant black box with a complex electronic control unit inside. This black-box, also referred to as the T-Box in automotive engineering parlance, is a telematics control unit.



As indicated in the image above, the telematics device collects data from within the vehicle and relays it back to the IoT cloud through the communication channel. This information is then pushed to the telematics applications/back-office systems where it is analyzed, and business intelligence decisions are made.

Likewise, the back-end applications send data to the telematics control unit from IoT cloud through the same communication channel.

Benefits of Telematics

The concept of telematics is not a recent introduction in the automotive industry. It was prevalent from 1996, but remained an untapped technology at that time due to the high investment cost for infrastructure setup and lack of consumer demand. However, the rise in popularity of vehicle connectivity has given telematics a new leash of life!

Some of the key benefits offered by the implementation of telematics are:

1. Navigation – Telematics provides turn-by-turn navigation assistance to guide drivers easily to their locations. When drivers are able to access shortest routes to destinations, they are also able to save on fuel costs.
2. Safety – Telematics devices collect safety-related information such as call for assistance during a crisis, emergency requests, stolen vehicle tracking, etc. and provide timely help to the vehicle occupants. Telematics also collects driving

behavior data such as sharp braking, acceleration, etc. This information can be used to educate drivers so that they stay safe on the roads.

3. Vehicle Performance – Users receive important vehicle health reports through the telematics system. This information can be very useful for fleet managers, as they can then schedule vehicle maintenance accordingly.
4. Vehicle Visibility – Telematics empowers organizations so that they can track the location of their vehicles. Fleet managers can use the vehicle location data to make timely route adjustments while responding to traffic congestion, weather conditions, etc. This way, they can switch resources around and ensure that there is no delay in deliveries.
5. Connectivity to Internet – The driver and passengers in the vehicle can utilize live weather forecasts, news bulletins and even information from social networking apps.
6. Reduced Administrative Costs – Administration and compliance is simplified as telematics devices can be integrated with third-party apps that generate various types of reports.

Challenges of Telematics

1. Power dependency: Vehicle GPS trackers must be powered to function. Nevertheless, both battery-powered and complex-wired tools have drawbacks. One must charge battery-powered devices regularly to prevent being stuck in an urgent situation with no way to summon help. Hard-wired car trackers power up from the battery pack and can drain it if the wires are not correctly installed.
2. Privacy concerns: People are understandably worried about their moves being tracked and recorded on a remote server. Before placing a GPS tracker in a car used by anyone except yourself – whether it's your wife, kid, or employee – make sure to address any privacy issues they may have by clarifying why you want to configure a tracker and how you plan to use the data.
3. Jamming: Sadly, GPS signals can be clogged by devices that interrupt GPS satellite messages. The only way to avoid this is to invest in a telematics system capable of detecting and reporting signal jamming.
4. System installation can take some time: Mounting telematics may take roughly 15 minutes to a day. This is because the process may require dismantling and rebuilding the dashboards. Therefore, you should allow specialists to carry out this task on your behalf.
5. Cost: Mounting a telematics system is costly, even if the consumer has the skill to do so, since one must purchase hardware and software. Prices vary depending on the global navigation satellite system (GNSS) and GPS. Cellular tracking is the least expensive, costing around $700. Nevertheless, the user must pay approximately $35 per month for online data. In passive wireless monitoring, the hardware costs $700, and the directory and network costs $800. Moreover, the average cost of satellite-based real-time tracking ranges between $5 and $100.

Top 10 Applications of Telematics

1. Safety monitoring
2. Communication in real-time
3. Detect harsh acceleration or braking
4. Vehicle maintenance
5. A risk assessment by insurance companies
6. Logging fuel consumption

7. Monitoring weather conditions
8. Assist with performance and training
9. Monitoring trailers and quasi assets
10. Beyond standard geofencing

What is Telemetry:

Telemetry automatically collects, transmits and measures data from remote sources, using sensors and other devices to collect data. It uses communication systems to transmit the data back to a central location. Subsequently, the data is analyzed to monitor and control the remote system.

Telemetry data helps improve customer experiences and monitor security, application health, quality and performance. Although telemetry refers to wireless data transfer mechanisms such as radio, ultrasonic, or infrared systems, it is not limited and includes data transferred over other media such as optical links, telephones, computer networks, and other wired communications. Telemetry data can be transferred through radio, GSM, satellite, infrared, ultrasonic, and cable. In other cases, telemetry refers to the data collected by tech companies on user activity, tracking things like usage, uptime, crashes, software installed, and more.

Traditional examples of telemetry are:

1. Monitoring data from space crafts
2. Animal tracking devices
3. Automobile sensors for fuel level, engine heat, vehicle speed and more
4. Heart monitors (EKG)
5. Convicted felon ankle bracelets
6. Wearables such as Fitbit health monitoring devices

Telemetry provides the ability to access data from remote locations. Very often, these locations are difficult or expensive to get to and have limited access to power and physical networks.

IoT Telemetry Protocols

IoT devices communicate using several network protocols. IoT devices used for telemetry such as remote sensors have the following requirements:

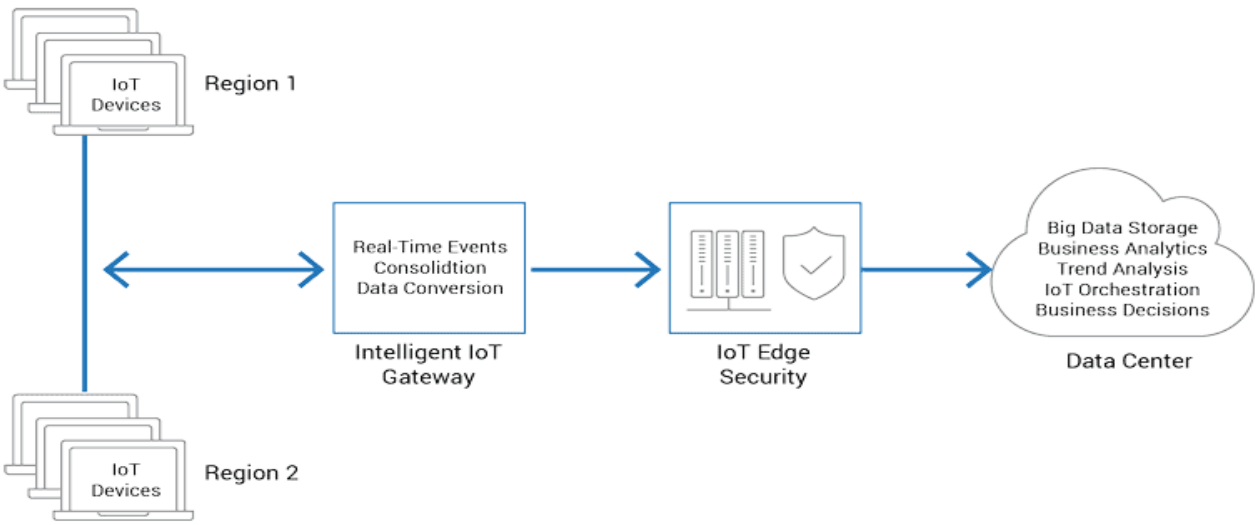
- Low Power – Many IoT devices are powered from an embedded battery. New battery technologies have life expectancies of 10 to 20 years.
- Low-Code Footprint – IoT devices are required to be as small as possible. This requires lightweight protocols that do not need heavy computing or wireless transmission power requirements.
- Low Bandwidth – Higher bandwidth transmissions require higher power and additional hardware footprints.
- Local Intelligent IoT Gateways – The closer this system is to the IoT device, the lower the power required to transmit to this receiving system.

IoT telemetry communications between the devices and the receiving system are performed by several protocols. Each protocol has benefits and flaws.

- MQTT – The Message Queuing Telemetry Transport (MQTT) protocol runs over TCP/IP and was designed for embedded hardware devices with limited embedded components and low power requirements. This protocol uses a publish-subscribe approach, which is inactive between transmissions and data retrievals. MQTT requires an intelligent IoT gateway.
- CoAP – Constrained Application Protocol (CoAP) was designed to run on devices constrained by low power and lossy networks. The protocol runs on UDP and is easily translatable to HTTP. CoAP can be routed over IP networks and supports IP multicast for M2M communications between other IoT devices.
- HTTP – This protocol is often combined with the Restful API protocol and is routable across the internet but is insecure.
- HTTPS – This protocol is secure and robust but has high power and processing requirements to encrypt data traffic and requires remote management of certificates.
- Alternative protocols
    - XMPP – IM-based protocol, simple addressing scheme
    - Advanced Message Queuing Protocol (AMQP) – Server to Server
    - Streaming Text-Oriented Messaging Protocol (STOMP)
    - Data Distribution Service (DDS) – Device to Device
    - OPC UA
    - Web Application Messaging Protocol (WAMP)

IoT telemetry architecture

IoT telemetry architecture includes the components shown below.



- IoT Devices – IoT devices are independent network nodes that communicate across IP networks or often directly with IoT gateway systems.

- M2M IoT – Protocols communicate with the local IoT gateway or alternately with central data enter or cloud locations.
- IoT Gateway – the intelligent IoT gateway performs a set of functions including,
    - Protocol translation between M2M IoT protocols and central datacenter and cloud applications
    - Consolidation of upstream IoT communications to WAN-optimized data communications
    - Near real-time analytics and event management. IoT devices communicate with the gateway with low-latency network connections. Compute and other resource-intensive analytics can be performed locally for time-critical events
    - IoT gateways communicate using secure and encrypted protocols.
- IoT Edge Security – IoT devices are exposed and vulnerable (by design) and require security technologies including firewall deep-packet inspection and others. IoT devices that have been compromised should be detected and quarantined as soon as possible. Edge security for IoT devices should be provided both at the IoT gateway and at the ingestion point of the central datacenters or clouds.
- Datacenter – IoT data ingested is often processed by:
    - Business applications that monitor and act upon the telemetry data. IoT data from multiple locations are analyzed centrally with a complete view of all deployed devices.
    - Storing the incoming data stream in various big-data repositories for long-term storage and analysis
    - IoT device management software systems that provide orchestrations, software/firmware updates, health monitoring and overall management. New IoT devices can be deployed and on-boarded with centralized systems.

IOT Domain Wise Applications

In this topic we are going to learn about domain specific IOT applications like smart lighting, weather monitoring, etc.

IoT applications span a wide range of domains like:

1. Home Automation
2. Smart Cities
3. Environment
4. Energy systems
5. Retail
6. Logistics
7. Industry
8. Agriculture
9. Health

Home Automation

Home sweet home—there's nothing like it! Our homes can be made smarter using the Internet of Things (IoT)—a system in which computing devices are connected over a network using unique identifiers (UIDs), and which can transfer data without the need for any human-to-human or human-to-computer interactions. These IoT devices can be used to automate our homes also.

IoT applications for smart homes:

- *Smart Lighting*
- *Smart Appliances*
- *Intrusion Detection*
- *Smoke / Gas Detectors*

1. **Smart Lighting:** Smart lighting for homes helps in saving energy by adapting the lighting to the ambient condition and switching on/off or dimming the lights when needed. Smart lighting is a technology driven concept that links three main features of solid state lighting (SSL) technologies, universal communication interfaces and advanced control.

Modern smart lighting systems are based on Light Emitting Diode (LED) technology and involve advanced technology drivers. Now the lighting systems are evolving to support different wireless communications interfaces well suited with the IoT environment. Market propensity of SSL systems forecast the accelerated growth of connected IoT lighting control systems in different markets from smart homes to industrial lighting systems. These systems offer advanced features such as spectral control of the light source and also, the inclusion of several communication interfaces.

2. **Smart Appliances:** Smart appliances make the management easier and also provide status information to the users remotely. For example, a smart refrigerator can keep track of items and notify the user when a item is low on stock. Examples of smart appliances are TVs, refrigerators, music systems, washing machines, etc.

3. **Intrusion Detection:** Home intrusion detection systems use cameras and sensors to detect intrusions and for raising alerts. Alerts can be sound, SMS or email sent to the user. An advanced system can even send an image or a short video clip related to the intrusion event.

4. **Smoke/Gas Detectors:** Smoke detectors installed at home can detect smoke and alert the users. Smoke detectors use optical detection, ionization, or air sampling techniques to detect smoke. Gas detectors can detect harmful gases like CO or LPG. These detectors can send alerts in the form of email, SMS, or voice.

2. Smart Cities

a) **Smart Parking:** Smart parking makes the search for parking space easier and convenient for drivers. In smart parking, sensors are used for each parking slot, to detect whether the slot is occupied or not. This information is aggregated by local controllers and sent over the Internet to the database. Drivers can use an application to know about empty parking slots.

b) **Smart Lighting:** Smart lighting systems for roads, parks, and buildings can help in saving energy. Smart lighting allows lighting to be dynamically controlled and also adaptive to the ambient conditions. Smart lights connected to the Internet can be controlled remotely to configure lighting intensity and lighting schedule.

c) **Smart Roads:** Smart roads equipped with sensors can alert the users about poor driving conditions, traffic congestion, and accidents. Information sensed from the roads can be sent via Internet to applications or social media. This helps in reducing traffic jams.

d) **Structural Health Monitoring:** A network of sensors are used to monitor the vibration levels in the structures. Data from the sensors is analyzed to assess the health of the structures. By analyzing the data it is possible to detect cracks, locate damages to the structures and also calculate the remaining life of the structure.

e) **Surveillance:** The video feeds from surveillance cameras can be aggregated in cloud based scalable storage solution. Surveillance of infrastructure, public transport and events in cities is required to ensure safety and security. City wide surveillance requires a

large network of connected cameras. The video feeds from the cameras can be aggregated in cloud-based storage. Video analytics applications can be used to search for specific patterns in the collected feeds.

f) **Emergency Response:** IoT systems for fire detection, gas and water leakage detection can help in generating alerts and minimizing their effects on the critical infrastructures. IoT systems can be used to monitor buildings, gas and water pipelines, public transport and power substations. These systems provides alerts and helps in mitigating disasters. Along with cloud-based applications IoT systems helps to provide near real-time detection of adverse events.

3. Environment

IoT applications for smart environments:

1. *Weather Monitoring*
2. *Air Pollution Monitoring*
3. *Noise Pollution Monitoring*
4. *Forest Fire Detection*
5. *River Flood Detection*

a) **Weather Monitoring:** Systems collect data from a no. of sensors attached and send the data to cloud based applications and storage back ends. The data collected in cloud can then be analyzed and visualized by cloud based applications.

b) **Air Pollution Monitoring:** System can monitor emission of harmful gases (CO2, CO, NO, NO2 etc.,) by factories and automobiles using gaseous and meteorological sensors. The collected data can be analyzed to make informed decisions on pollutions control approaches.

c) **Noise Pollution Monitoring:** Due to growing urban development, noise levels in cities have increased and even become alarmingly high in some cities. IoT based noise pollution monitoring systems use a no. of noise monitoring systems that are deployed at different places in a city. The data on noise levels from the station is collected on servers or in the cloud. The collected data is then aggregated to generate noise maps.

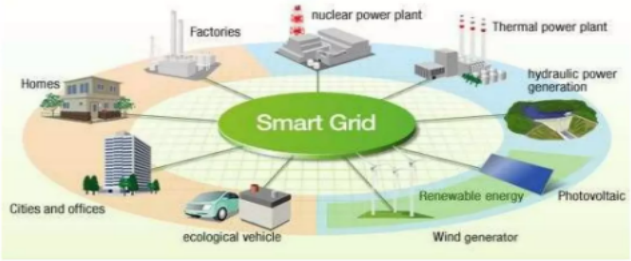
d) **Forest Fire Detection:** Forest fire can cause damage to natural resources, property and human life. Early detection of forest fire can help in minimizing damage.

e) **River Flood Detection:** River floods can cause damage to natural and human resources and human life. Early warnings of floods can be given by monitoring the water level and flow rate. IoT based river flood monitoring system uses a no. of sensor nodes that monitor the water level and flow rate sensors.

4. Energy System

IoT applications for smart energy systems:

1. *Smart Grid*
2. *Renewable Energy Systems*
3. *Prognostics*



a) **Smart Grids:** is a data communication network integrated with the electrical grids that collects and analyze data captured in near-real-time about power transmission, distribution and consumption. Smart grid technology provides predictive information and recommendations to utilities, their suppliers, and their customers on how best to manage power. By using IoT based sensing and measurement technologies, the health of equipment and integrity of the grid can be evaluated.

b) **Renewable Energy Systems:** IoT based systems integrated with the transformers at the point of interconnection measure the electrical variables and how much power is fed into the grid. For wind energy systems, closed-loop controls can be used to regulate the voltage at point of interconnection which coordinate wind turbine outputs and provides power support.

c) **Prognostics:** In systems such as power grids, real-time information is collected using specialized electrical sensors called Phasor Measurment Units(PMUs) at the substations. The information received from PMUs must be monitored in real-time for estimating the state of the system and for predicting failures

5. Retail

IoT applications in smart retail systems:

1. *Inventory Management*
2. *Smart Payments*
3. *Smart Vending Machines*

a) **Inventory Management:** IoT systems enable remote monitoring of inventory using data collected by RFIDreaders. The inventory in a store or warehouse can be managed by using IoT. The products or items in the store can be attached with RFID tags. By using the RFID tags, the RFID reader or software can automatically show the number of items in the store or warehouse. If a product goes out of stock a notification can be sent to the store owner automatically.

b) **Smart Payments:** Solutions such as contact-less payments powered by technologies such as Near Field Communication(NFC) and Bluetooth. Now-a-days new types of payments are coming into picture like QR codes, NFC, contact less technologies etc. These technologies enables smart payments.

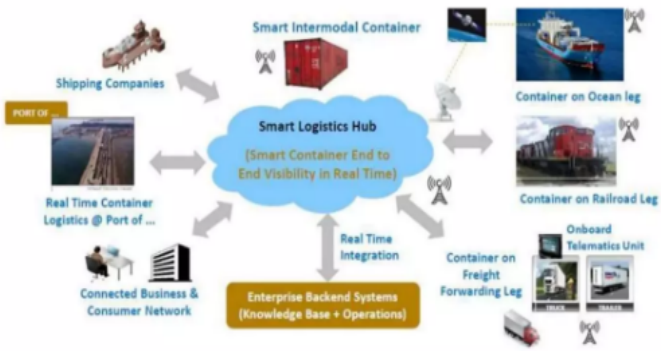
c) **Smart Vending Machines:** Sensors in a smart vending machines monitors its operations and send the data to cloud which can be used for predictive maintenance A smart vending machine contains several items. A consumer can insert money and get the item they want as shown in the image below. Several sensors can be attached to these vending machines such that whenever an item quantity is less, the owner of that machine will be automatically notified so that the owner can be arrangements to get that item beforehand.

Also, the vending machines can maintain the history of the consumers. So, when a consumer visits the vending machine next day, it can suggest the same item that the consumer purchased before.

6. Logistics

IoT applications for smart logistic systems:

1. *Fleet Tracking*
2. *Shipment Monitoring*
3. *Remote Vehicle Diagnostics*



a) **Route generation & scheduling:** While delivering packages to various locations, different sensors can be fixed in those routes and they can be monitored remotely through an application. By looking at the data sent by the sensors, the delivery company can automatically know which routes are less congested and schedule the delivery of packages in such routes.

b) **Fleet Tracking:** Use GPS to track locations of vehicles inreal-time. A delivery company will have several delivery personnel working with them. Different people will use different vehicles for delivering the packages. Sensors can be fixed to those vehicles and their location can be tracked to know how long will it take to deliver the package.

c) **Shipment Monitoring:** IoT based shipment monitoring systems use sensors such as temp, humidity, to monitor the conditions and send data to cloud, where it can be analyzed to detect foods poilage. The packages can be fixed with RFID tags or other form of remote tracking sensors to send data periodically to a server via Internet. The delivery company can use that data to track where the package is and update the user about the remaining time that will be needed to deliver the package.

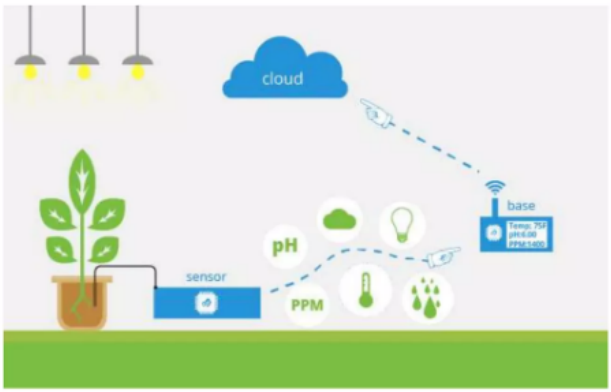
d) **Remote Vehicle Diagnostics:** Systems use on-board IoT devices for collecting data on Vehicle operations(speed, RPMetc.,) and status of various vehicle subsystems. A vehicle rental company can fix sensors into the vehicles before giving them for rent to the customers. The company can check the data sent by the sensors to know the current location of the vehicle and easily track them.

7 Agriculture:

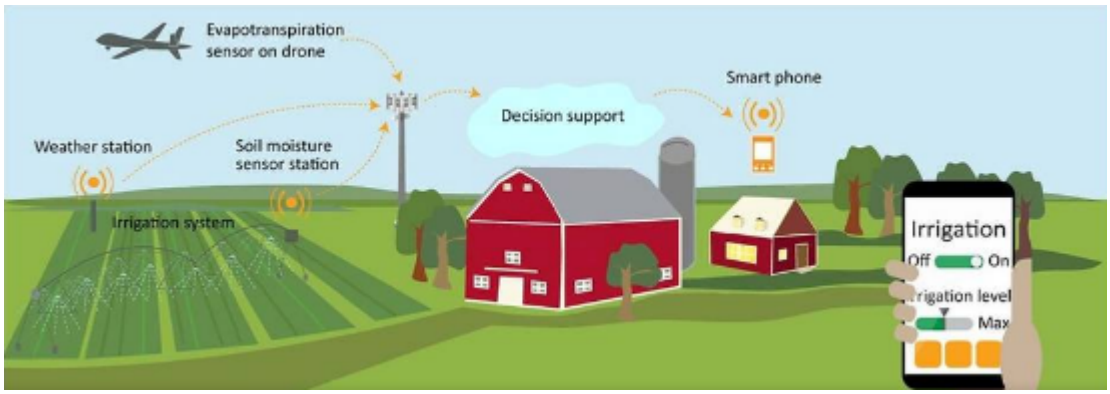
IoT applications for smart agriculture:

1. Smart Irrigation

2. Green House Control



Smart Irrigation: Irrigation refers to the watering of plants. By using different sensors like temperature sensor, humidity sensor, soil moisture sensor, etc., data can be collected about the soil and the environment and let the framer know when to turn on the water sprinklers to provide water to the plants. This process is illustrated in the figure given below.



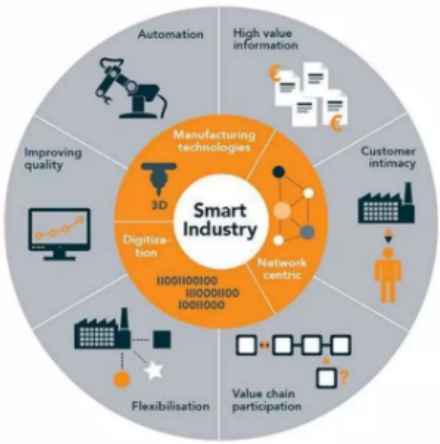
Green House Control: A green house is an artificial field that can be grown inside buildings or on the roof tops. It is a controlled environment in which several types of sensors are fixed to gather data about the soil, environment and other parameters.

The data from the green house is aggregated at a local gateway and sent to the server via Internet. The data at the server is analyzed and appropriate alerts are sent to the owner of the green house. This process is illustrated in the figure below.

8. Industry:

IoT applications in smart industry:

1. *Machine Diagnosis & Prognosis*
2. *Indoor Air Quality Monitoring*



Machine Diagnosis & Prognosis: The machines used in the industry can be fixed with sensors. The data from the sensors can be used to diagnose the machines. We can know if the machine is working up to the expected performance or not. The data analysis will also let the owner of the machine know when the life of machine will be over.

Indoor Air Quality Monitoring: The quality of air for the working personnel inside the industry is also important. Often times leakage of dangerous gases leads to the death of industry personnel. Sensors can be fixed at different location to monitor the working environment for any leakage of hazardous gases and notify the appropriate personnel to deal with it.

9. Health and lifestyle

IoT applications in smart health & lifestyle:

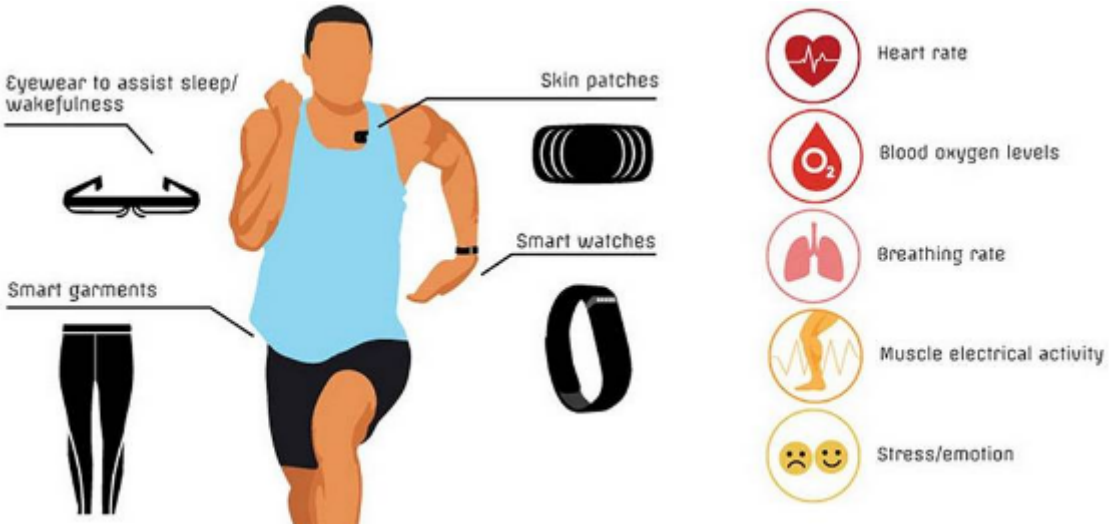
1. Health & Fitness Monitoring

2. Wearable Electronics

Health and Fitness Monitoring: With the advent of IoT remote healthcare has become an viable option for attending to patients. There is no need for patient to visit hospital for every minor health problem.

The doctor can attend to such patients from a remote location. Different sensors can be fixed on near the patient to monitor the health vitals of that patient. The data sent by the sensors is monitored by the doctor and appropriate decisions are made.

Wearable Electronics: Now-a-days there are different types of wearables available in the market to monitor health and lifestyles. Some examples of such wearables are smart watches, smart glasses, smart patches, smart garments, etc., as shown in the below figure.

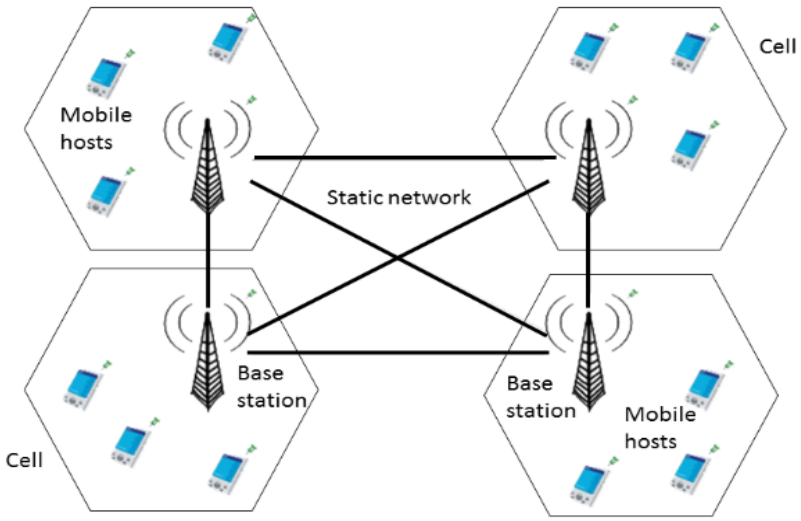


Cellular IoT

Cellular IoT allows a wide variety of machines and devices to communicate with each other, via a mobile data connection provided by cellular networks. Cellular IoT technologies allow physical devices (e.g. sensors, actuators, and their host microcontrollers or single-board computers) to connect to a private network or the public Internet for the purpose of transmitting data. Cellular IoT connects physical objects by piggybacking on the cellular networks.

Piggybacking: In general, piggybacking involves the unauthorized use of resources, whether that is wireless access, a user session, or even processing power. "piggybacking" refers to a situation where an unauthorized party gains access to some system in connection with an authorized party. This can happen in several ways, including piggybacking on public wireless networks, and piggybacking into a password-protected system.

Cellular IoT is used to define IoT devices that are connected to the internet through cellular networks, similar to the ones used by your smartphone. Instead of using Wi-Fi, Bluetooth, or other forms of connectivity, IoT devices can connect to the internet through cellular networks.



Cellular IoT is one of the most popular types of Internet of Things connectivity, primarily because it:

- Has excellent coverage
- Simplifies global deployment
- Works right out of the box
- Establishes secure connections
- Performs well in mobile, indoor, and outdoor applications
- Supports low and high bandwidth applications

While cellular networks were designed for phones, they're highly versatile, and cellular technology has evolved to accommodate a wider range of devices and use cases over time. Like smartphones and other mobile devices, cellular IoT devices can use 2G, 3G, 4G, and 5G networks. But they don't use data the same way as phones, and with billions of low-power devices relying on cellular technology, specialized cellular networks have also been developed specifically for IoT: LTE-M and NB-IoT.

What is LTE-M?

You can probably hazard a guess that LTE-M is closely related to the popular LTE (Long-Term Evolution) wireless standard. The countries that support LTE encompass a vast list primarily comprised of the Americas and parts of Europe.

LTE-M effectively stands for "Long-Term Evolution for Machines" and allows for IoT devices to piggyback on existing LTE networks. It was designed in a power-conscious manner for applications that require low-to-medium data throughput. With a bandwidth of 1.4 MHz (compared to 20 MHz for LTE), LTE-M provides great range but less throughput than LTE (approximately 375KB down and 300KB up). LTE-M also offers cell tower handoff features, making it a great mobility solution (even across multiple regions).

Asset tracking, wearables, home security, and home/business monitoring are all great examples of use cases for LTE-M in the IoT.

What is NB-IoT?

Considering the Internet of Things is literally part of the name, NB-IoT was designed for the IoT. NB-IoT stands for "Narrowband-IoT" and is great for areas without robust LTE coverage or when bandwidth requirements are relatively minimal. Again, per its name, NB-IoT uses just a narrow band of the full bandwidth available.

Available globally where GSM is the flag-bearer (such as much of Europe, Africa, and Asia), NB-IoT devices consume very little power and provide less data throughout than LTE-M (approximately 60KB down and 30KB up). Compared to LTE-M's bandwidth of 1.4 MHz, NB-IoT operates on 200 KHz, providing longer range and better indoor penetration.

Certain use cases like smart cities (e.g. parking meters, utility monitoring), parking garages, indoor deployments, and agricultural settings are great examples of suitable NB-IoT implementations.

Cellular IoT Benefits:

The advantages of cellular connectivity with IoT are extensive:

1. Coverage: Cellular networks are ubiquitous, mature, and reliable.

2. Global Reach: There is no other network technology with the reach of cellular.
3. Security: SIM-based authentication and utilization of VPN tunnels makes cellular the most secure option.
4. Installation: Works out-of-the-box without requiring local installation or technical expertise.
5. Low/No power: Cellular modules can consume ~8mA of power and networks are still available in the case of a power outage.

When it comes to security, coverage, and usability, it’s hard to compete with cellular.

Next generation kiosks, self-service technology

A kiosk is a digital machine that businesses can utilize to give customers the ability to make purchases independently. This provides an excellent opportunity for companies looking forward to improving their customer and business relations, not to mention allowing them to generate more income and valuable information about their market. This article will look at how setting up a kiosk in your store, or parking spaces can provide long-term benefits. We will also learn about types of kiosks with examples. So, let's not waste our precious time and cut to the chase!

A kiosk refers to a booth, which is small in size, used for marketing purposes. It is generally manned by one or two persons or styled for self-use by customers electronically. Kiosks help in test marketing new products in a low-cost manner. Kiosks can be operated through a small space inside a shopping mall or in the compound.

Kiosks are set up in areas or places which see a large footfall of customers. Different types of products can be displayed, such as food products offered to taste, mobile phones, cars, and so on. In the case of services, a person at the kiosk helps explain the service offerings, such as fine dining offers of a hotel, services of an e-commerce or fintech platform, insurance products, and so on.

Small kiosks are also set up within an existing space or franchisee shop to display new products or services. Example of such offering includes skincare products launched by a company traditionally selling hair care products, insurance cum investment (ULIP) products offered by a traditional insurance company.

They also include self-service kiosks, which are operated as interactive computer terminals that help customers update their information or personal records. For example, updating personal data of change in address, mobile phone number in kiosks set up by banks which allow customers to update their records without human intervention and long-standing queues.

The owners of a kiosk, malls, or other lessors who sub-let space for kiosks charge a rent for the space let-out. The rent is less in comparison to high rent charged for a larger outlet or showroom. The low rent also suits the business which may be in its early stages and not able to pay for a larger space.

Types of Kiosks

There are many types of kiosks, and those can be best used for several different applications. Some might seem futuristic or high-tech, but they are not uncommon in many places throughout the world, and there are lots of varieties. These kiosks can help customers find their way around an establishment, place orders, make payments, or gain access to Internet connectivity. Regardless of how these kiosks were developed, they play a significant role when it comes to interacting directly with customers since they facilitate quick and easy ways to interact with employees (or machines).

In years past, business owners relied on big-box stores for all their electronic needs. Today, however, we have our pick of packaging and distribution methods for the kiosks we

choose. That is set to change even further as technology has the potential to fundamentally increase efficiency in various retail settings. There are essentially two kinds of options: non-interactive and interactive kiosks.

1. Non-Interactive Kiosks

The use of non-interactive kiosks has helped to improve shopping experiences. These are stand-alone displays that deliver a variety of messages and can be used in countless ways to provide important information while conveying information as well. These kiosks are basically to convey only information related to a product, brand, and so forth. Some examples of non-interactive kiosks are as follows:

1. **Informational Kiosks** : This is a computer-like device combining specialized hardware, software and connectivity options, designed to provide certain information to people in public places.
2. **Products Kiosks**: the product kiosk, which is specifically used to showcase a new product.
3. **Promotional Kiosks**: Promotional Kiosk are a folding, reusable kiosk structures used majorly for Promotional Activities. The Promotional Kiosk are highly used due to its portability, reusability and stability.

2. Interactive Kiosks

Interactive kiosks are those that customers can use in different ways to access a specific resource or avail of something, usually at shopping centres, malls, parking areas, etc. Because these kiosks function on user interaction and demand, these devices are available to a wide variety of businesses and businesses-in-general, including restaurants, service providers, and even destinations such as malls and airports. Interactive kiosks have different usages depending on what they provide access to. These functions can range from wayfinding and navigation, self-checkout, purchases, or even internet access – all at the user's behest!

Types of Interactive Kiosks

Wayfinding Kiosks A wayfinding kiosk is a type of information display that helps people find their way through spaces. This includes providing things such as maps, directories, and directional displays with the goal of getting patrons from one location to another. Unlike the information display found at most malls and big box stores today, a wayfinding kiosk contains a touch-screen feature that allows users to search or explore maps to help them reach their destinations without any problems whatsoever.

1. **Self-Service kiosks:** Another kind of interactive kiosk is a self-service kiosk that customers can use to complete tasks and transactions by themselves. This has already become very popular, and its popularity is continuously increasing in many shopping centres because customers find it efficient and simpler to use. Using this type of kiosk instead of a store associate could help reduce long lines and wait

times. However, it utterly depends on personal preference; some people are more fond of using this type of screen than asking a professional to get them what they need, while others prefer speaking with an individual as they find it very helpful when they need something specific or unique. However, the fact can't be ignored that self-service kiosks are excellent and valuable devices.

2. **Internet Kiosks:** Without sounding like a broken record, internet kiosks are still as popular and valuable as they were back in the day. These devices continue to be installed in public places such as airports, hotels, and other hospitality businesses. Internet kiosks are essentially digital displays that provide visitors with an outlet for entertainment while also offering them an easy way to browse the internet or at least search for specific services which might be helpful when travelling or visiting unfamiliar cities or states, for example. Unfortunately for some people, this alternative source of exposure has caused many to rely too much on internet kiosk-related information and thus become lazy. However, these devices are handy, and their popularity is rapidly increasing.
3. **Parking Kiosks:** One of the most popular interactive kiosks is parking kiosks; these devices have become an indispensable tool for the parking industry. These are basically payment terminals that help motorists efficiently & quickly make payments and pay their parking fees without needing to stand in a long queue in a parking lot. Additionally, parking kiosks reduce the stress of car park owners managing parking lots. These machines are highly accurate, efficient, and user-friendly, reducing traffic congestion in a parking lot, improving customers' parking experience, and saving time.

Well, if you explore, you will discover that several other kinds of interactive kiosks are also there, such as shoppable kiosks and more. However, we will now learn how these kiosks are benefiting us.

Benefits of Kiosks

Now that we have reviewed the various types of kiosks, so it's time to discuss why they are worth purchasing or renting. They are an investment, aren't they? After all, whichever option you choose, you will be investing in the maintenance or development of your brand. That being said, let's understand why they are worth buying!

1. **Save Money:** Interactive kiosks are suitable for customers. They don't ask for a salary and can provide customers with any information they might need. And since you're not paying to hire people, which means more money to buy even more products! Kiosks also reduce overhead costs because you don't have to pay rent or hire people to run the business. Placing a vending machine outside is an excellent way of getting noticed and attracting sales. Interactive kiosks can eliminate the need for staffing; you won't have to worry about red tape, sick leave, maternity leave, or firing someone if they don't work out; after all, these machines are made for that exact purpose!

2. **Increase Reach:** While most people think of kiosks as a way to promote their products and services, they're not just for in-store shopping but are increasingly being installed outside retail establishments, such as hotels. This is for two reasons: one, many companies want to extend the reach of their advertising efforts; and two, these can be operated by trained professionals who know how to perform various tasks efficiently. So, having a kiosk can increase customer reach and significantly benefit your business.
3. **Improve Customer Experience:** A great thing about having a kiosk in a retail store or parking lot is that it considerably improves the customer experience. Most people have a sense of freedom and superiority when they are not interrupted while making a purchase, and that's what a kiosk provides them with. Remember, improved customer experience means more customer revisits, so every business owner should consider installing a kiosk to gain more profits.

Challenges

When considering the hardware to manage your Kiosk you want to consider a few main points:

1. Remote access – the ability to access your Kiosks remotely allows you to manage your kiosks without spending any additional time or money sending someone out to the field.
2. Display – with screen resolution always improving, you want to ensure that your display output can at minimum handle 4K resolution.
3. External Devices – some kiosks such as ones used for pay stations and self-service ordering require the integration of a credit card reader.
4. Software Compatibility – Some kiosks run multiple software applications, you also want to ensure that the hardware running your kiosks is compatible with the major Operating Systems.