UNIT-I

Introduction to internet of Things:

Introduction to internet of Things Introduction, Definition and characteristics of IoT - Physical Design of IoT-Things in IoT, IoT protocols- Logical design of IoT- IoT Functional blocks, IoT Communication Models, IoT Communication APIs- IoT Enabling Technologies- Wireless Sensor Networks, Cloud Computing, Big Data Analytics, Communication protocols, Embedded Systems-IoT Levels and Deployment Templates-Iot Level-1,IoT Level-2, IoT Level-3, IoT Level-4, IoT Level-5, IoT Level-6. Domain Specific IoT.

INTRODUCTION TO IOT

IoT comprises of things that have unique identities and are connected to internet. IoT is not limited to just connecting things to the internet but also allow things to communicate and exchange data.

Definition:
A dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual things that have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into information network, often communicate data associated with users and their environments.

Characteristics:

1) **Dynamic & Self Adapting**: IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user‘s context or sensed environment.
   Eg: the surveillance system is adapting itself based on context and changing conditions.
2) **Self Configuring:** allowing a large number of devices to work together to provide certain functionality.
3) **Inter Operable Communication Protocols:** support a number of interoperable communication protocols and can communicate with other devices and also with infrastructure.
4) **Unique Identity:** Each IoT device has a unique identity and a unique identifier (IP address).
5) **Integrated into Information Network:** that allow them to communicate and exchange data with other devices and systems.

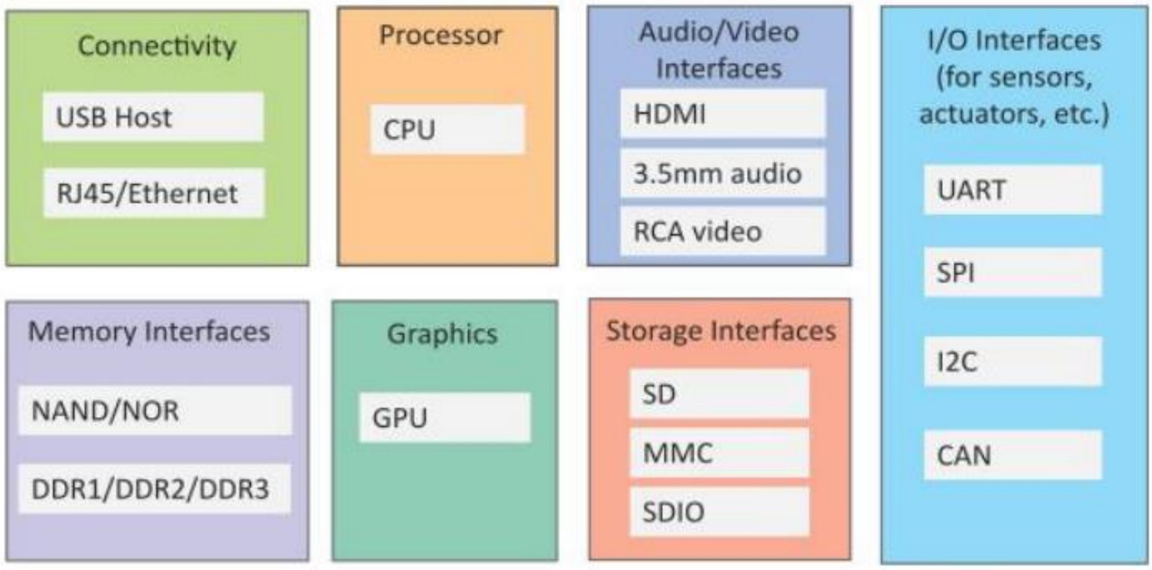
Applications of IoT:

1) Home
2) Cities
3) Environment
4) Energy
5) Retail
6) Logistics
7) Agriculture

8) Industry
9) Health & LifeStyle

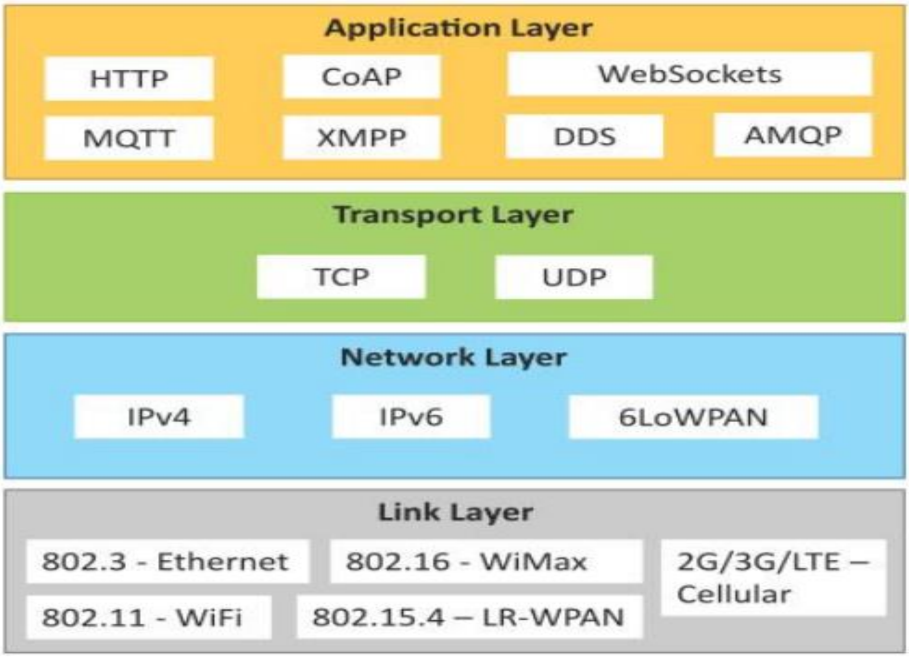
Physical Design Of IoT

1) Things in IoT:



The things in IoT refers to IoT devices which have unique identities and perform remote sensing, actuating and monitoring capabilities. IoT devices can exchange data with other connected devices applications. It collects data from other devices and process data either locally orremotely.
An IoT device may consist of several interfaces for communication to other devices both wired and wireless. These includes (i) I/O interfaces for sensors, (ii) Interfaces for internet connectivity
(iii) memory and storage interfaces and (iv) audio/video interfaces.

2) IoT Protocols:



A) Link Layer : Protocols determine how data is physically sent over the network's physical layer or medium. Local network connect to which host is attached. Hosts on the same link exchange data packets over the link layer using link layer protocols. Link layer determines how packets are coded and signaled by the h/w device over the medium to which the host is attached.

Protocols:

- **802.3-Ethernet**: IEEE802.3 is collection of wired Ethernet standards for the link layer. Eg: 802.3 uses co-axial cable; 802.3i uses copper twisted pair connection; 802.3j uses **fiber optic connection**; 802.3ae uses **Ethernet overfiber**.

- **802.11-WiFi**: IEEE802.11 is a collection of wireless LAN(WLAN) communication standards including extensive description of link layer. Eg: 802.11a operates in 5GHz band, 802.11b and 802.11g operates in 2.4GHz band, 802.11n operates in 2.4/5GHz band, 802.11ac operates in 5GHz band, 802.11ad operates in 60Ghzband.

- **802.16 - WiMax**: IEEE802.16 is a collection of wireless broadband standards including exclusive description of link layer. WiMax provide data rates from 1.5 Mb/s to 1Gb/s.

- **802.15.4-LR-WPAN**: IEEE802.15.4 is a collection of standards for low rate wireless personal area network(LR-WPAN). Basis for high level communication protocols such as ZigBee. Provides data rate from 40kb/s to250kb/s.

- **2G/3G/4G-Mobile Communication**: Data rates from 9.6kb/s(2G) to up to100Mb/s(4G).

B) Network/Internet Layer: Responsible for sending IP datagrams from source n/w to destination n/w. Performs the host addressing and packet routing. Datagrams contains source and destination address.

Protocols:

- **IPv4:** Internet Protocol version4 is used to identify the devices on a n/w using a hierarchical addressing scheme. 32 bit address. Allows total of 2**32addresses.
- **IPv6:** Internet Protocol version6 uses 128 bit address scheme and allows 2**128 addresses.
- **6LOWPAN:**(IPv6overLowpowerWirelessPersonalAreaNetwork) operates in 2.4 GHz frequency range and data transfer 250 kb/s.

- **Transport Layer:** Provides end-to-end message transfer capability independent of theunderlying n/w. Set up on connection with ACK as in TCP and without ACK as in UDP. Provides functions such as error control, segmentation, flow control and congestion control. **Protocols:**

- **TCP:** Transmission Control Protocol used by web browsers(along with HTTP and HTTPS), email(along with SMTP, FTP). Connection oriented and stateless protocol. IP Protocol deals with sending packets, TCP ensures reliable transmission of protocols in order. Avoids n/w congestion and congestion collapse.
- **UDP:** User Datagram Protocol is connectionless protocol. Useful in time sensitive applications, very small data units to exchange. Transaction oriented and stateless protocol. Does not provide guaranteed delivery.

C) Application Layer: Defines how the applications interface with lower layer protocols to send data over the n/w. Enables process-to-process communication using ports.

Protocols:

- **HTTP:** Hyper Text Transfer Protocol that forms foundation of WWW. Follow request-response model Stateless protocol.

- **CoAP:** Constrained Application Protocol for machine-to-machine (M2M) applicationswith constrained devices, constrained environment and constrained n/w. Uses client- server architecture.

- **WebSocket:** allows full duplex communication over a single socket connection.

- **MQTT:** Message Queue Telemetry Transport is light weight messaging protocol based on publish-subscribe model. Uses client server architecture. Well suited for constrained environment.

- **XMPP:** Extensible Message and Presence Protocol for real time communication and streaming XML data between network entities. Support client-server and server-server communication.

- **DDS:** Data Distribution Service is data centric middleware standards for device-to-device or machine-to-machine communication. Uses publish-subscribe model.

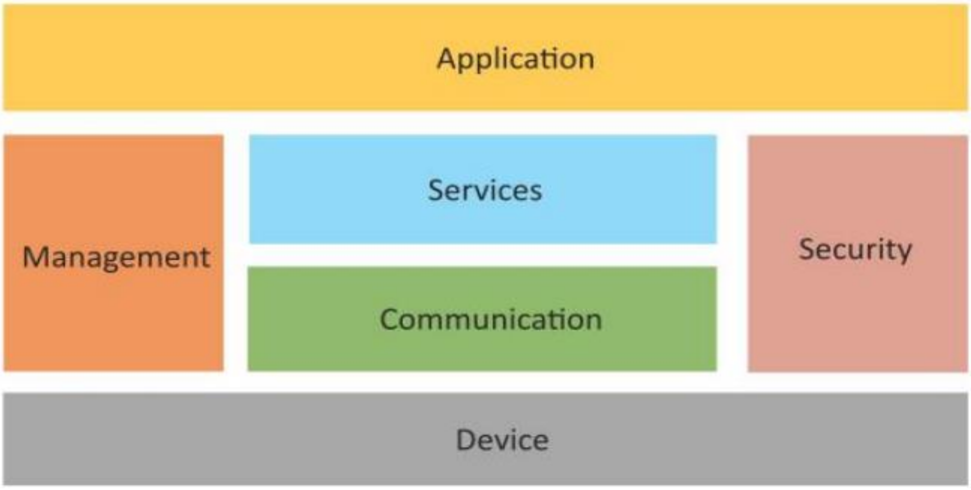
- **AMQP:** Advanced Message Queuing Protocol is open application layer protocol for business messaging. Supports both point-to-point and publish-subscribe model.

LOGICAL DESIGN of IoT

Refers to an abstract represent of entities and processes without going into the low level specifies of implementation.

1) IoT Functional Blocks 2) IoT Communication Models 3) IoT Comm. APIs

1) **IoT Functional Blocks:** Provide the system the capabilities for identification, sensing, actuation, communication and management.



In an IoT system, the primary functional blocks are sensors (data collection), processors (data processing), gateways (communication management), and applications (user interface and data utilization), each playing a crucial role in collecting, processing, transmitting, and presenting data from connected devices across a network; with additional functional blocks including actuators for control actions, connectivity modules for communication, power management, memory storage, and security components depending on the device complexity.

Detailed Explanation of Each Block:

Sensors:

Function: These are the "front-end" of an IoT device, responsible for converting physical phenomena (like temperature, pressure, light) into electrical signals that can be read by the system.

Examples: Temperature sensors, pressure sensors, motion detectors, proximity sensors, humidity sensors.

Processors:

Function: The "brain" of the IoT device, processing raw data collected by sensors, performing calculations, and preparing it for further transmission.

Key aspects: Microcontrollers, embedded systems, digital signal processors (DSPs).

Gateways:

Function: Acts as a bridge between a network of IoT devices and the wider internet, aggregating data from multiple sensors, translating communication protocols, and providing secure access to the cloud.

Features: Data filtering, protocol conversion, security management

Applications:

Function: The user-facing component of an IoT system, presenting processed data through dashboards, alerts, or control interfaces, allowing users to interact with and analyze information from connected devices.

Examples: Smart home applications, industrial monitoring systems, wearable health trackers.

Other Important Functional Blocks:

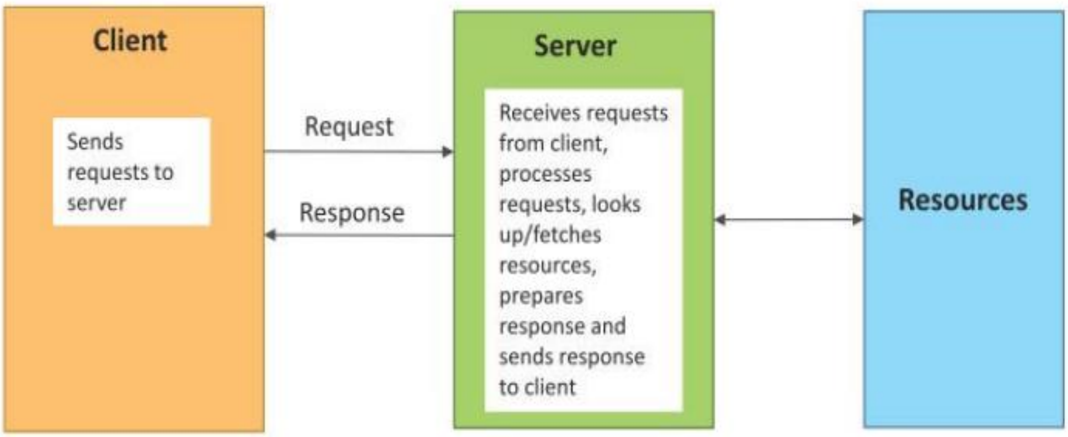
- **Device:** An IoT system comprises of devices that provide sensing, actuation, monitoringand control functions.

- **Communication:** handles the communication for IoT system.
- **Services:** for device monitoring, device control services, data publishing services andservices for device discovery.
- **Management:** Provides various functions to govern the IoT system.
- **Security:** Secures IoT system and priority functions such as authentication, authorization,message and context integrity and data security.
- **Application:** IoT application provide an interface that the users can use to control andmonitor various aspects of IoT system.

2) IoT CommunicationModels:

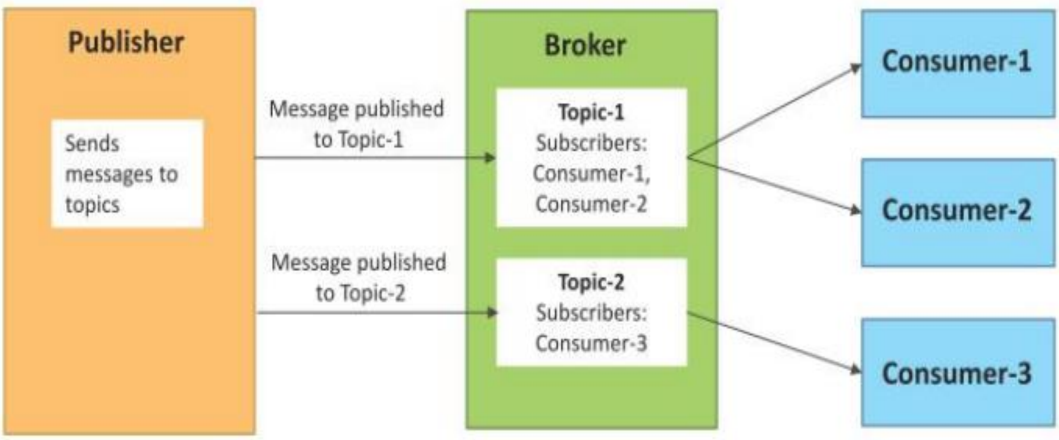
1) Request-Response 2) Publish-Subscribe 3) Push-Pull 4) Exclusive Pair

1) Request-ResponseModel:



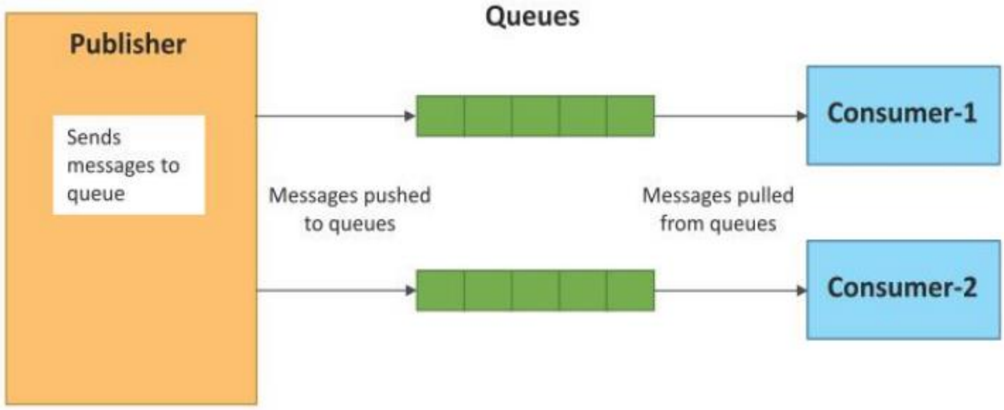
In which the client sends request to the server and the server replies to requests. Is a stateless communication model and each request-response pair is independent of others.

2) Publish-Subscribe Model:



It involves publishers, brokers and consumers. Publishers are source of data. Publishers send 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 receives data for a topic from the publisher, it sends the data to all the subscribed consumers.

3) **Push-Pull Model:** in which data producers push data to queues and consumers pull data from the queues. Producers do not need to aware of the consumers. Queues help in decoupling the message between the producers and consumers.

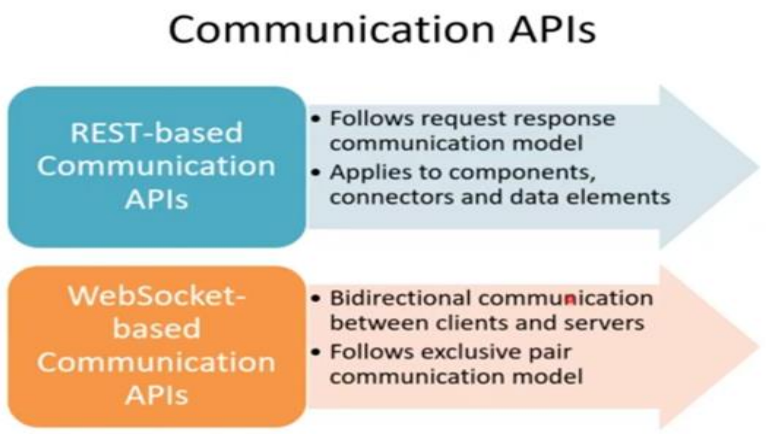


4) **Exclusive Pair:** is bi-directional, fully duplex communication model that uses a persistent connection between the client and server. Once connection is set up it remains open until the client send a request to close the connection. Is a stateful communication model and server is aware of all the open connections.

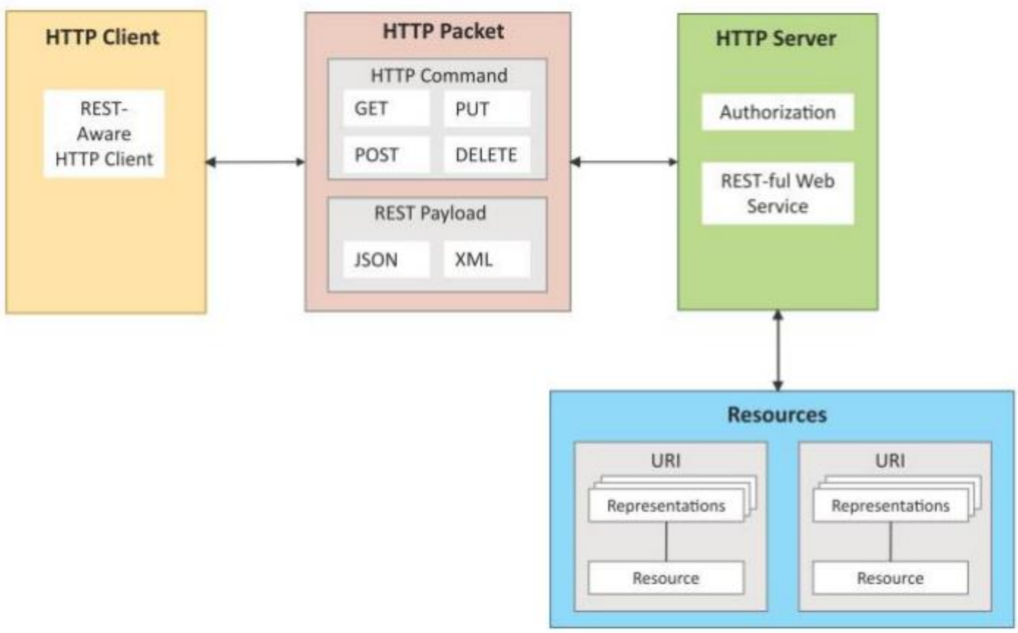
3)IoT Communication APIs:

- **REST based communication APIs(Request-Response Based Model)**
- **WebSocket based Communication APIs(Exclusive Pair Based Model)**

a) REST based communication APIs: Representational State Transfer(REST) is a set of architectural principles by which we can design web services and web APIs that focus on a system's resources and have resource states are addressed and transferred.



The REST architectural constraints: Fig. shows communication between client server with REST APIs.



Client-Server: The principle behind client-server constraint is the separation of concerns. Separation allows client and server to be independently developed and updated.

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.

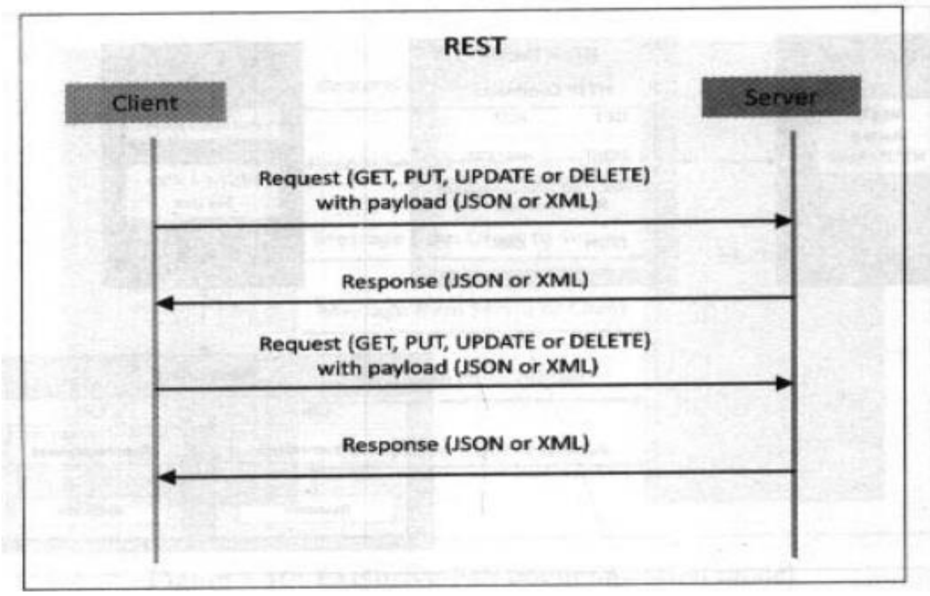
Cache-able: Cache constraint requires that the data within a response to a request be implicitly or explicitly labeled as cache-able or non-cacheable. If a response is cache-able, then a client cache is given the right to reuse that response data for later, equivalent requests.

Layered System: constraints the behavior of components such that each component cannot see beyond the immediate layer with which they are interacting.

User Interface: constraint requires that the method of communication between a client and a server must be uniform.

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.

Request-Response model used by REST:

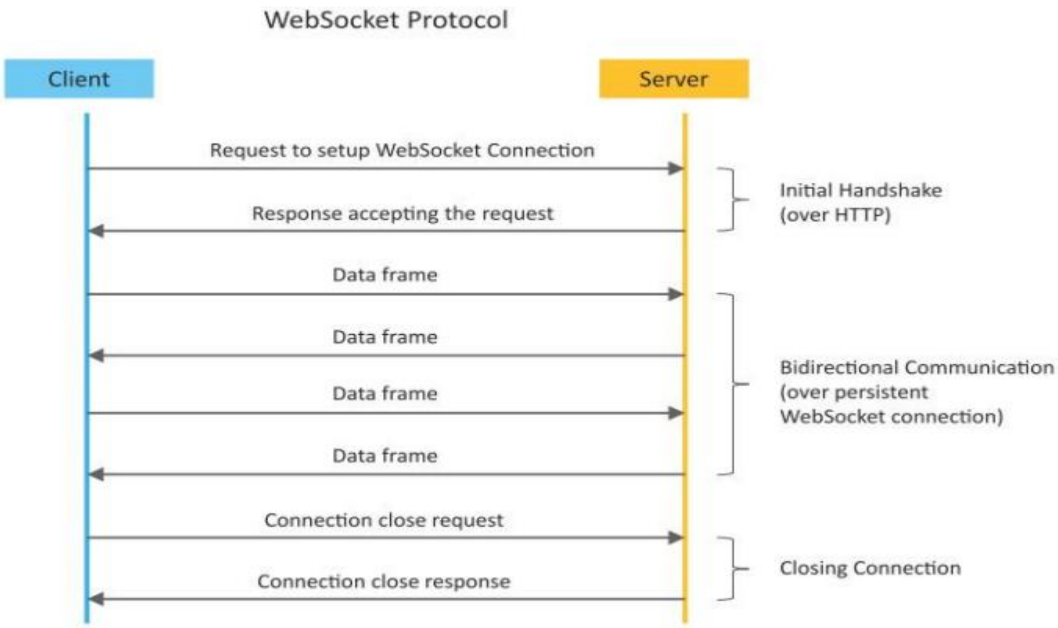


RESTful webservice is a collection of resources which are represented by URIs. RESTful web API has a base URI(e.g: http://example.com/api/tasks/). The clients and requests to these URIs using the methods defined by the HTTP protocol(e.g: GET, PUT, POST or DELETE). ARESTful web service can support various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

b) WebSocket Based Communication APIs: WebSocket API allows us to create web sockets, it is a javascript API that is capable of full-duplex communication using a TCP connection. WebSocket uses port 80 by default.

Features of WebSocket are:

- **Full-Duplex Protocol**: WebSocket is a full-duplex protocol as it allows the application to send and receive data at the same time.
- **Stateful Protocol**: It means the connection between server and client will not be terminated until and unless closed by any one of them either by the client or by the server. Once the connection is terminated from one end it is also closed by another end.
- **3-way handshake**: Websocket uses a 3-way handshake also known as TCP connection for establishing communication between a client and server.



WebSocket protocol, contrary to REST, is stateful while helping two applications in seamless data transmission or information exchange. It's based on port & sockets and works only over a TCP connection. It supports bidirectional communication. By bidirectional, we mean that the same socket/port delivers and receive the data. Hence, a continuous connection is established.

Extensively, WebSocket is used when an application demands ongoing or uninterrupted data delivery. For example, a chat application needs to receive the app all the time. Even if the end-user is not opening the app, the message should be delivered. Only WebSocket can enable such continuous communication. In such unbroken data delivery, using REST will become resource-extensive whereas WebSocket simplifies the job.

Difference Between REST & Websocket APIs

Factor	REST	WebSocket
Cost	High (in comparison)	As ports and sockets are involved, it is cost-effective
Information storage	As REST is stateless, no logs, related to request, is saved or stored	Details like session and port details are used
Communication model	Uses Request-Response communication model	Follows Full Duplex communication model
TCP Connection	Each request needs new connection	Same connection is used throughout
Overheads	Essential for every request	There is no need of overheads

IoT Enabling Technologies

IoT is enabled by several technologies including Wireless Sensor Networks, Cloud Computing, Big Data Analytics, Embedded Systems, Security Protocols and architectures, Communication Protocols, Web Services, Mobile internet and semantic search engines.

1) **Wireless Sensor Network(WSN):** Comprises of distributed devices with sensors which are used to monitor the environmental and physical conditions. Zig Bee is one of the most popular wireless technologies used by WSNs.
   WSNs used in IoT systems are described as follows:
   - **Weather Monitoring System**: in which nodes collect temp, humidity and otherdata, which is aggregated and analyzed.
   - **Indoor air quality monitoring systems:** to collect data on the indoor air quality andconcentration of various gases.
   - **Soil Moisture Monitoring Systems**: to monitor soil moisture at various locations.
   - **Surveillance Systems**: use WSNs for collecting surveillance data(motion datadetection).
   - **Smart Grids** : use WSNs for monitoring grids at various points.
   - **Structural Health Monitoring Systems**: Use WSNs to monitor the health of structures(building, bridges) by collecting vibrations from sensor nodes deployed at various points in the structure.

2) **Cloud Computing:** Cloud computing is another important IoT-enabling technology. Massive amounts of data are generated by IoT devices. Cloud solutions offer scalable and dependable storage and processing for this data. They offer data analysis, remote device administration, and secure access to information from anywhere. The cloud computing industry is dominated by Amazon Web Services (AWS), which provides a wide range of dependable, scalable, and affordable cloud computing services. AWS is a one-stop solution for various cloud services, from data storage to analytics. Services are offered to users in different forms.
   - Infrastructure-as-a-service (IaaS): provides users the ability to provision computing and storage resources. These resources are provided to the users as a virtual machine instances and virtual storage.
   - Platform-as-a-Service (PaaS): provides users the ability to develop and deploy application in cloud using the development tools, APIs, software libraries and services provided by the cloud service provider.
   - Software-as-a-Service (SaaS): provides the user a complete software application or the user interface to the application itself.

3) **Big Data Analytics:**
   Big data analytics is the process of inspecting large volumes of data to reveal valuable insights, patterns, correlations, and trends. Organizations can use this analytical approach to make data-informed decisions. It entails the use of statistical analytic techniques, such as clustering and regression, to large datasets using modern tools and technologies. These analyses can uncover hidden patterns, market trends, consumer behaviours, and other useful information in structured and unstructured data sources, such as streaming and batch data.

   Big data analytics is critical for businesses and industries as it enables data-driven decision-making, develops an understanding of customer preferences, and identifies opportunities and risks. Large volumes of data may be analysed and interpreted to provide businesses with a competitive advantage and increase operational effectiveness.

Some examples of big data generated by IoT are

- Sensor data generated by IoT systems.
- Machine sensor data collected from sensors established in industrial and energy systems.
- Health and fitness data generated IoT devices.
- Data generated by IoT systems for location and tracking vehicles.
- Data generated by retail inventory monitoring systems.

4) **Communication Protocols:** form the back-bone of IoT systems and enable network connectivity and coupling to applications.

IoT devices communicate with each other and with the central systems via communication protocols. These protocols enable efficient and secure data transfer in IoT networks. IoT (Internet of Things) communication protocols are required for devices to connect and share data in the IoT ecosystem. There are several popular IoT communication protocols, each with unique advantages and applications. Several important IoT communication protocols are listed below:

- Message Queue Telemetry Transport (MQTT)
- Hypertext Transfer Protocol (HTTP)
- Constrained Application Protocol (CoAP)
- Bluetooth
- Zigbee
- Bluetooth Low Energy (BLE)
- Wi-Fi
- Z-Wave

These were the important IoT enabling technologies. Wireless Sensor Networks (WSN) for data collection, Cloud Computing for storage and processing, Big Data Analytics for insights, Embedded Systems to analyse sensor data, and different Communication Protocols for device connectivity are key supporting technologies. Together, these technologies enable IoT to transform businesses by giving devices more intelligence and data-driven capabilities.

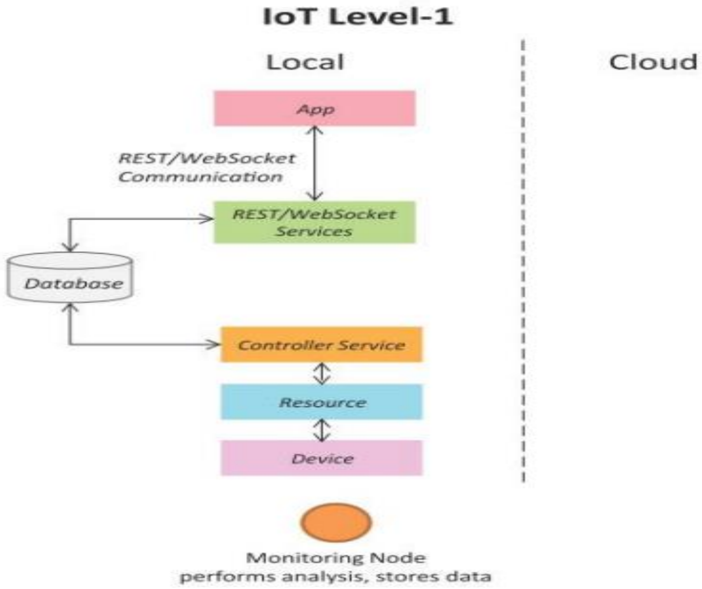
5) **Embedded Systems:** is a computer system that has computer hardware and software embedded to perform specific tasks. Embedded System range from low cost miniaturized devices such as digital watches to devices such as digital cameras, POS terminals, vending machines, appliances etc.,

Embedded systems, such as microcontrollers and other hardware components, are critical in processing sensor data. The information gathered by these sensors isn't immediately usable. Instead, the embedded system intervenes to make it useful.

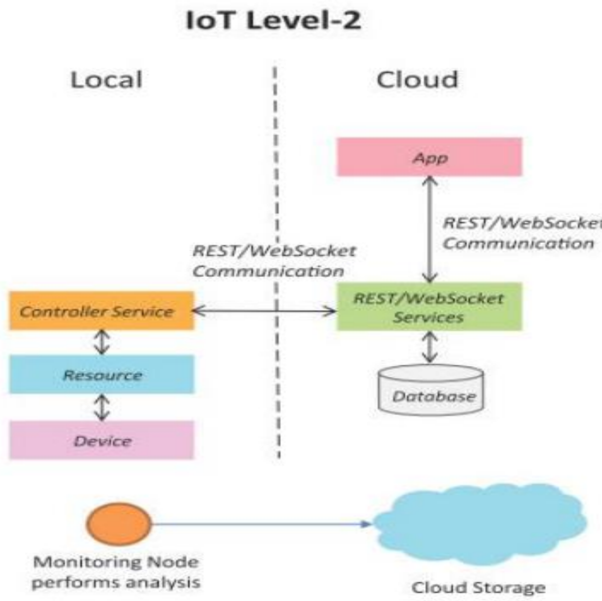
Here's how it works in simpler terms: Suppose you have several sensors that collect information like temperature or motion. This data is analogous to raw components in a recipe. The embedded system is like the chef, taking those raw ingredients (data), following a recipe (algorithm), and turning it into something meaningful. So, embedded systems are like the smart chefs of the technology world, turning sensor data into useful information and actions.

IoT Levels and Deployment Templates

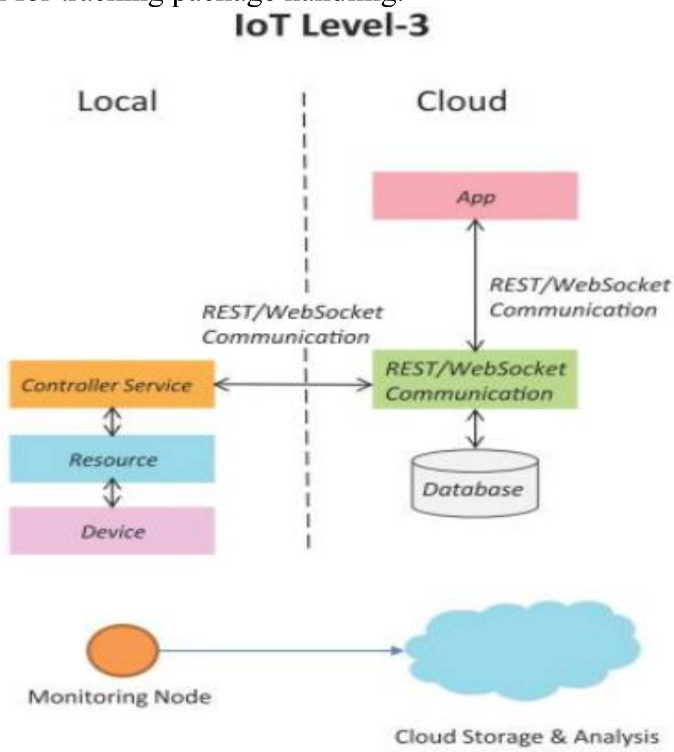
1) **IoT Level1:** System has a single node that performs sensing and/or actuation, stores data, performs analysis and host the application as shown in fig. Suitable for modeling low cost and low complexity solutions where the data involved is not big and analysisrequirement are not computationally intensive. An e.g., of IoT Level1 is Home automation.



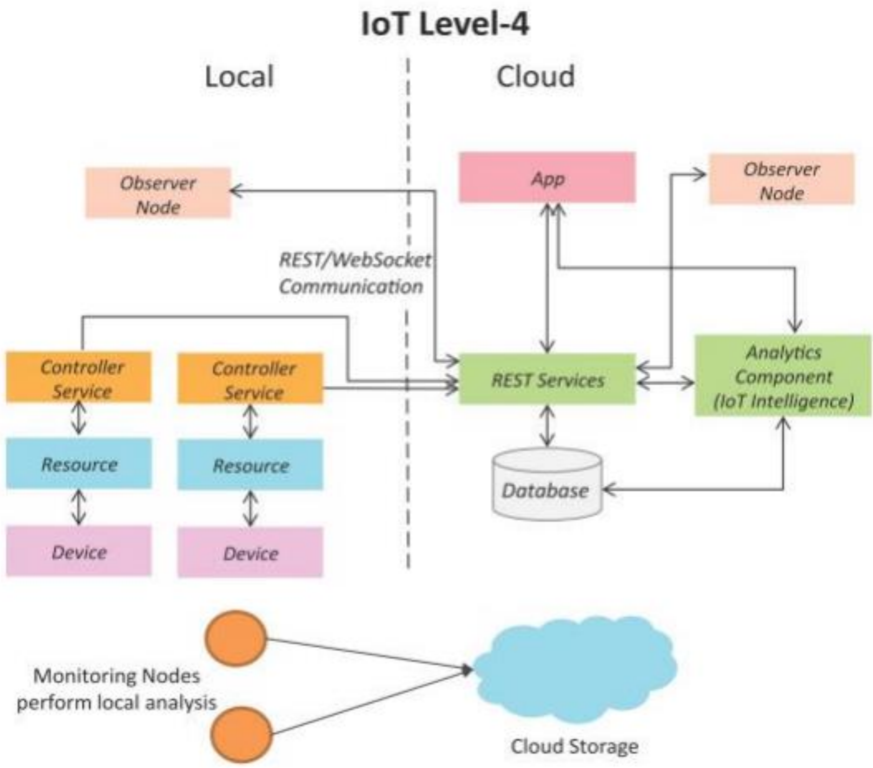
2) **IoT Level2:** has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not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



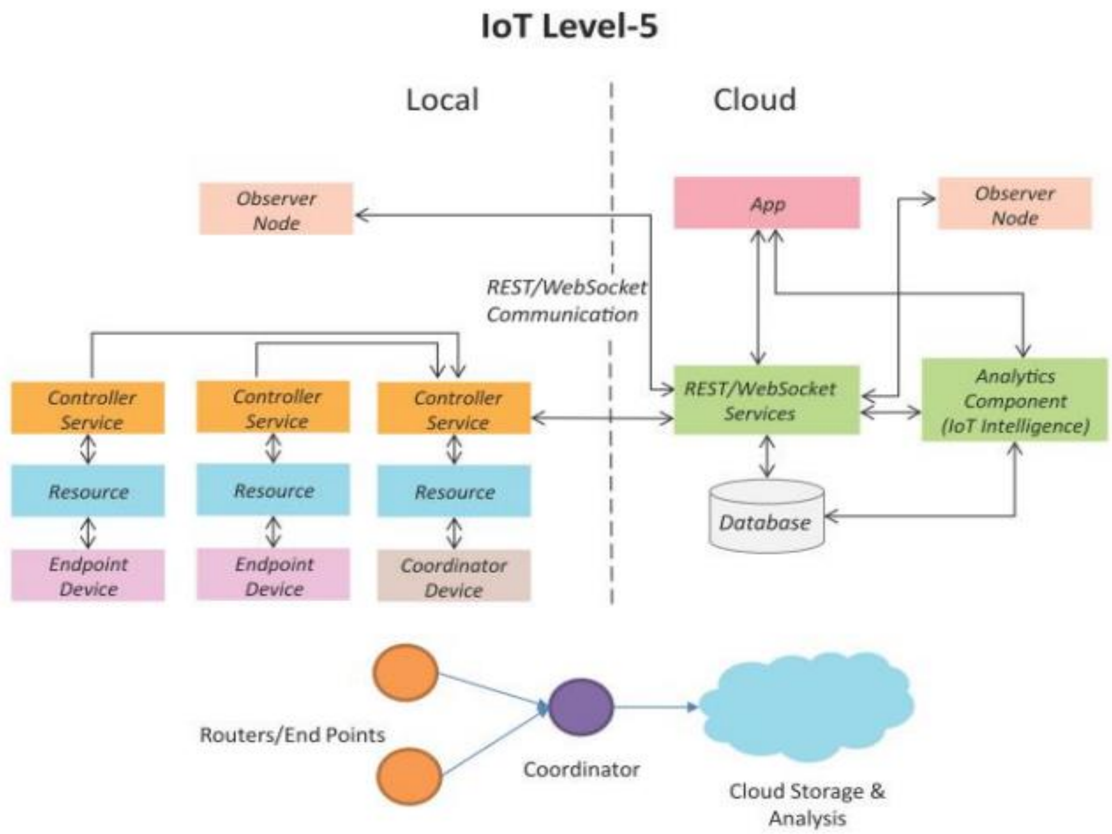
3) **IoT Level3:** system has a single node. Data is stored and analyzed in the cloud application is cloud based as shown in fig. Level3 IoT systems are suitable for solutions where the data involved is big and analysis requirements are computationally intensive. An example of IoT level3 system for tracking package handling.



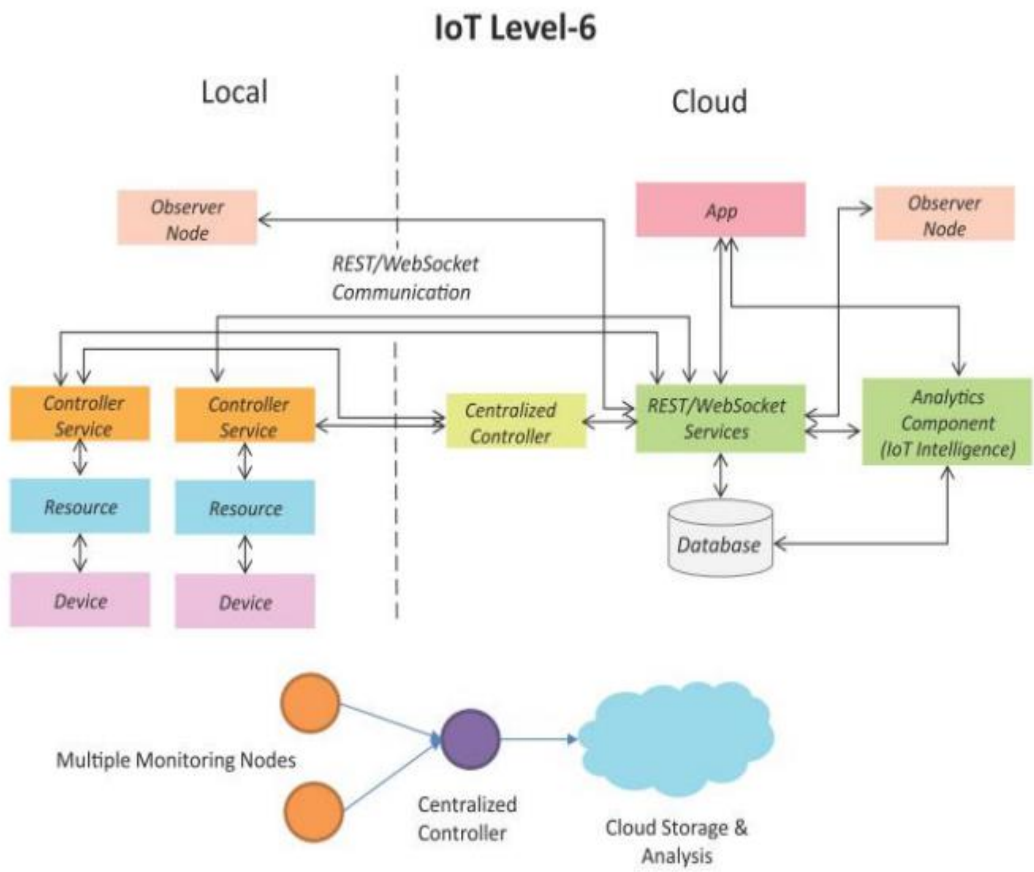
4) **IoT Level4:** System has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud based as shown in fig. Level4 contains local and cloud based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices. An example of a Level4 IoT system for Noise Monitoring.



5) **IoT Level5:** System has multiple end nodes and one coordinator node as shown in fig. The end nodes that perform sensing and/or actuation. Coordinator node collects data fromthe end nodes and sends to the cloud. Data is stored and analyzed in the cloud and the application is cloud based. Level5 IoT systems are suitable for solution based on wireless sensor network, in which data involved is big and analysis requirements arecomputationally intensive. An example of Level5 system for Forest Fire Detection.



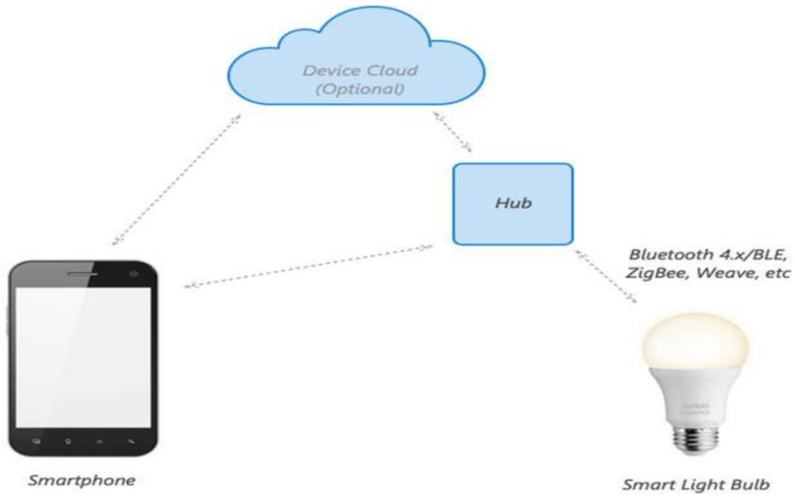
6) **IoT Level6:** System has multiple independent end nodes that perform sensing and/or actuation and sensed data to the cloud. Data is stored in the cloud and application is cloud based as shown in fig. The analytics component analyses the data and stores the result in the cloud data base. The results are visualized with cloud based application. The centralized controller is aware of the status of all the end nodes and sends controlcommands to nodes. An example of a Level6 IoT system for Weather Monitoring System.



DOMAIN SPECIFIC IoTs

1) **Home Automation:**

   a) **Smart Lighting:** helps in saving energy by adapting the lighting to the ambient conditions and switching on/off or diming the light when needed. Key enabling Technologies includes solid state lighting (Such as LED lights) and IP enabled lights. Wireless enabled and internet connected lights can be controlled remotely from IOT applications such as mobile or web applications. Smart lights with sensors for occupancy, temperature, lux level can be configured to adapt the lighting based on the ambient conditions sensed, in order to provide good ambience.



b) **Smart Appliances:** make the management easier and also provide status information to the users remotely. Modern homes have a number of appliances such as TVs Refrigerators, Music Systems Washing machine etc., Managing and controlling these appliances is difficult with their own remote controls. Smart Appliances make the management easier and also provide status information remotely.

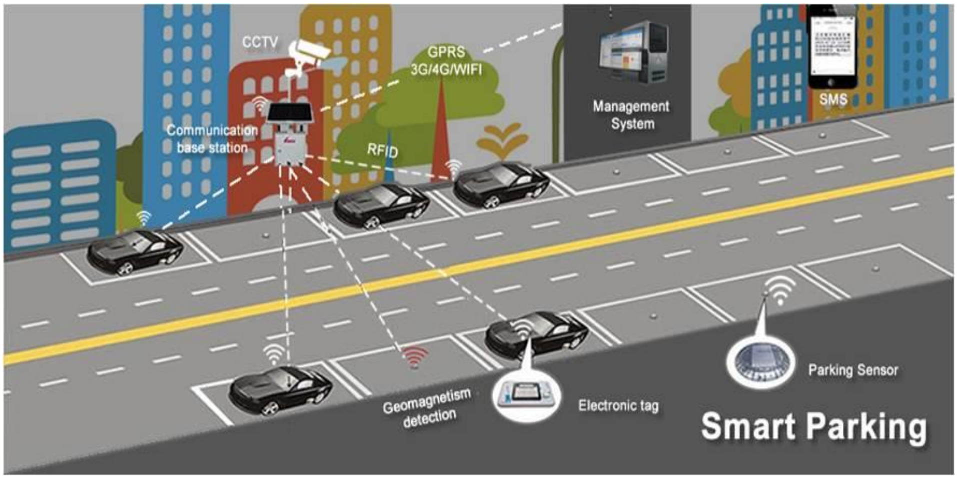
For example washing machine can be monitored remotely when washing cycle is completed. Smart thermostat (A/C) allow controlling the temperature remotely and can learn the user preferences. Smart refrigerators can keep track of the items stored and send updates to the user when an item is low on stock. Smart TVs allows users to search and stream videos and movies from the internet and search TV channel schedules and fetch news. With Open Remote users can control various appliances using mobile or web applications.

c) **Intrusion Detection:** use security cameras and sensors(PIR sensors and door sensors)to detect intrusion and raise alerts. Alerts can be in the form of SMS or email sent to the user. Advanced systems even send detailed alerts such as an image grab or a short video clip sent as an email attachment. The system uses image processing to recognize the intrusion and can extract the intrusion subject and generate Universal – Plug- and –Play instant messaging and alert.

d) **Smoke/Gas Detectors:** Smoke detectors are installed in homes and buildings todetect smoke that is typically an early sign of fire. Alerts raised by smoke detectors can be in the form of signals to a fire alarm system. Gas detectors can detect the presence of harmful gases such as CO, LPG etc., It can raise alerts in human voice describing where the problem is, send an SMS, email to user or local fire safety and provide visual feedback on its status. It can detect gas leakage and smoke and gives visual level indication also.

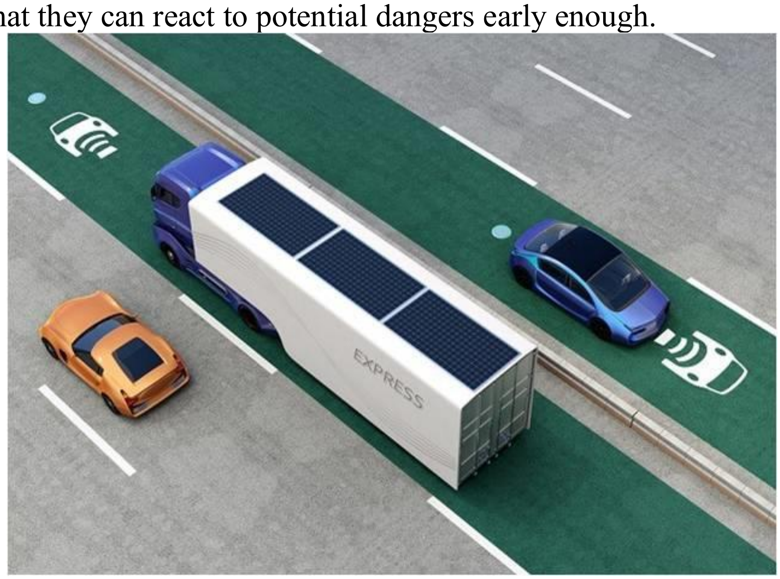
2) Cities:

a) **Smart Parking:** make the search for parking space easier and convenient for drivers. Smart parking are powered by IoT systems that detect the no. of empty parking slots and send information over internet to smart application back ends. These applications can be accessed by drivers from smart phones, tablets and in-car navigation system. In the smart parking sensors are used for each parking slot to detect whether the slot is empty or occupied. This information is aggregated by a local controller and then sent over the internet to the data base. In some applications, parking reservation and dynamic pricing also available.

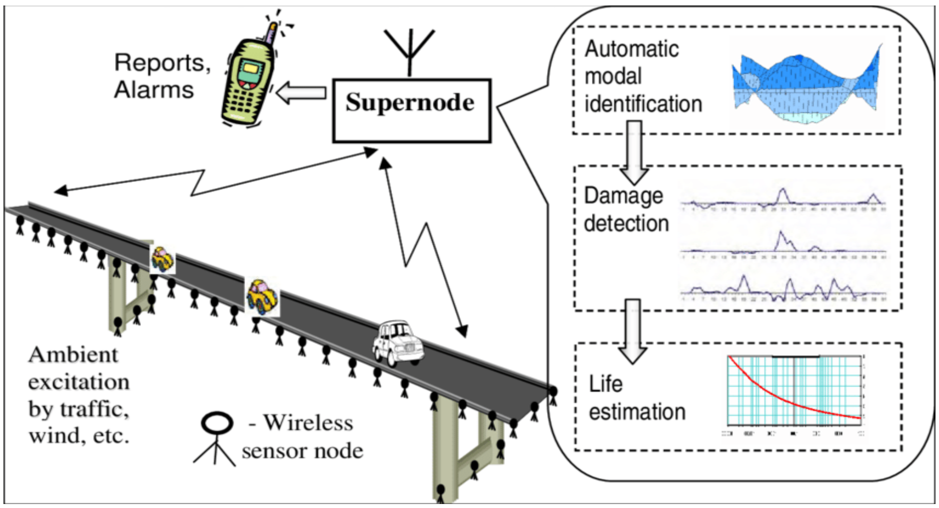


b) **Smart Lighting:** for roads, parks and buildings can help in saving energy. It allows lighting to be dynamically controlled and also adaptive to the ambient conditions. It can be controlled remotely to configure lighting schedules and lighting intensity. Smart lights equipped with sensors can communicate other lights and exchange information on the sensed ambient conditions to adapt the lighting.

c) **Smart Roads:** Equipped with sensors can provide information on driving condition, travel time estimating and alert in case of poor driving conditions, traffic condition and accidents. Such applications help in reducing traffic jams. Information sensed can be communicated via internet to cloud based applications and social media and disseminated to the drivers who subscribe it, and it also provide road situation a few hundred meters ahead of them, so that they can react to potential dangers early enough.



d) **Structural Health Monitoring:** uses a network of sensors to monitor the vibration levels in the structures such as bridges and buildings. By analyzing the data it is possible to detect cracks and mechanical breakdowns. It can locate the damages and estimate the remaining life of the structure. Using this type of applications, can give advance warnings in case of imminent failures. Since Structural health monitoring system use large number of wireless sensor nodes which are powered by traditional batteries, researchers are exploring energy harvesting technologies.



e) **Surveillance: Public transport and events in city is required to ensure safety and security. City wide surveillance infrastructure comprising of large number of distributed and internet connected video cameras are created.** The video feeds from surveillance cameras can be aggregated in cloud based scalable storage solution. Cloud based video analytics applications can be deployed to search for patterns or specific events from the videos 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. Response to such alerts generated by systems sent to the public, rerouting of traffic, evacuations of the affected areas etc., The system adapts by dynamically adjusting traffic lights, changing related driving policies, applying essential security controls and can reduce the latency of emergency services such as ambulances and police cars.

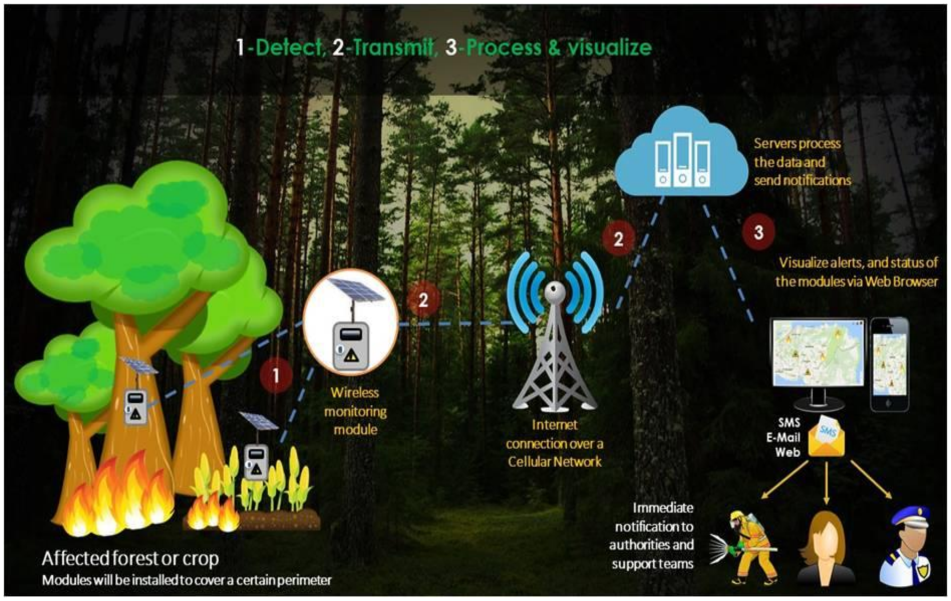
3) Environment:

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. Weather alerts can be sent to the subscribers.

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. This air pollution monitoring system integrates a single chip microcontroller, several air pollution sensors, GPRS modem and a GPS module.

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.

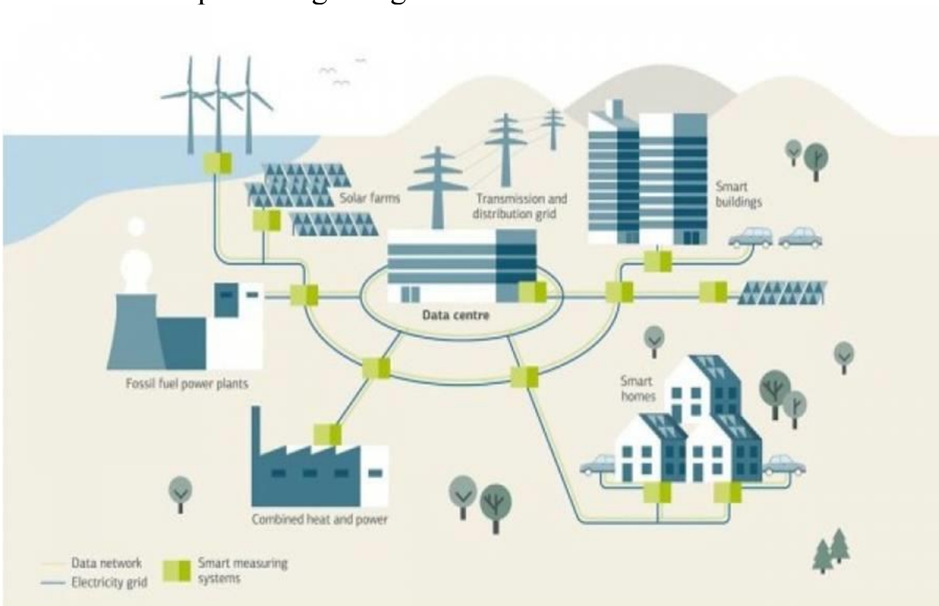
d) **Forest Fire Detection:** Forest fire can cause damage to natural resources, property and human life. There can be different causes such as lightning, human negligence, volcanic eruptions and sparks from rock falls. Early detection of forest fire can help in minimizing damage. IOT system use a number of monitoring nodes deployed at different locations, which collects measurements on ambient conditions. This system provide early warning and estimates the scale and intensity of the fire.



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. ofsensor nodes that monitor the water level and flow rate sensors and raise alerts when rapid increase in water level and flow rate.

4) **Energy:**

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 healthof equipment and integrity of the grid can be evaluated. Smartgrids use high speed two- way communication technologies for real time information and power exchange. Smart meters captures almost real time consumption, remotely control the consumption, and remotely switch off the consumption when required. Storage collection and analysis of smart grids data in the cloud can help in dynamic optimization of system operations, maintenance and planning. It can also help in detecting faults and predicting outages.

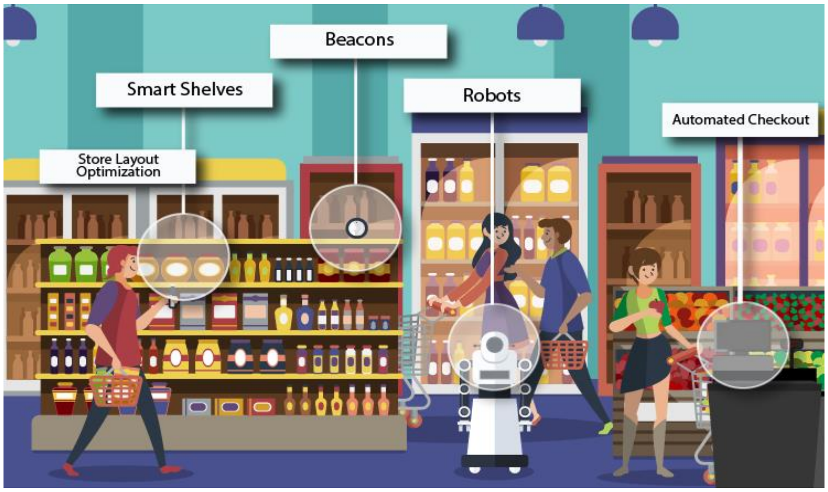


b) **Renewable Energy Systems:** IoT based systems integrated with the transformers at the point of interconnection measure the electrical variables and how much power is fed into the grid. For wind energy systems, closed-loop controls can be used to regulate the voltage at point of interconnection which coordinate wind turbine outputsand 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 thesubstations. The information received from PMUs must be monitored in real-time for estimating the state of the system and for predicting failures.

5) Retail:

a) **Inventory Management:** In the Retail business, over stocking results in additional storage expenses and risk incase of perishable products, under stocking can lead to loss of revenue. RFID tags attached to the products allow them to be tracked in real time, so that the inventory levels can be determined accurately. IoT systems enable remote monitoring of inventory using data collected by RFID (Radio Frequency Identifier) readers.



b) **Smart Payments:** Solutions such as contact-less payments powered by technologiessuch as Near Field Communication (NFC) and Bluetooth. NFC may be used in combination with bluetooth, where NFC initiates initial pairing of devices to establish a Bluetooth connection while the actual data transfer takes place through Bluetooth.

c) **Smart Vending Machines:** Sensors in smart vending machines monitors its operations and send the data to cloud which can be used for predictive maintenance. Smart vending machines connected to the internet allow remote monitoring of inventory levels, elastic pricing of products, promotions and contact less payments. It can also allow user preferences to be remembered and learned with time. When user moves from one vending machine to another and pairs the smart phones with the vending machines, a user specific interface is presented.

6) **Logistics:**

a) **Route generation & scheduling:** IoT based system backed by cloud can provide firstresponse to the route generation queries and can be scaled up to serve a large transportation network. Data Driven Transportation system can provide services such as advanced route guidance, dynamic vehicle routing, anticipating customer demands for picking up and delivery problem for instance.

b) **Fleet Tracking:** Use GPS to track locations of vehicles in real-time. Cloud based fleet traking system can be scaled up on demand to handle large number of vehicles. Alerts can be generated in case of deviations in planned routes. The vehicle location and route data can be aggregated and analyzed for detecting bottlenecks in the supply chain such as traffic congetion and generation of alternative routes.

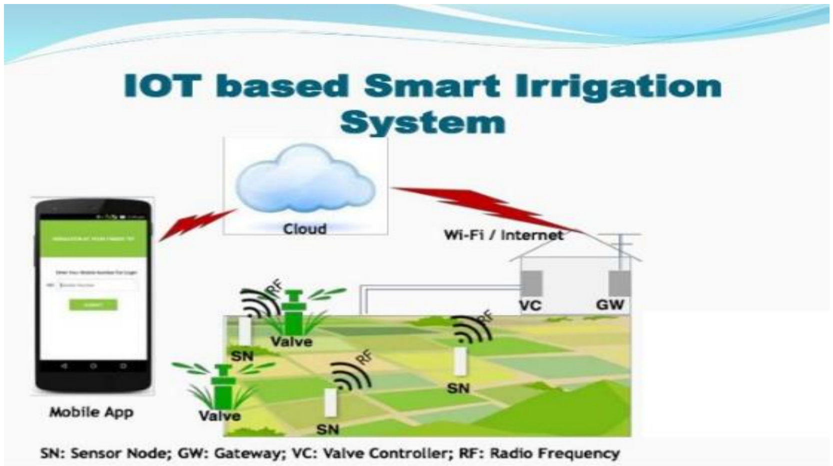
c) **Shipment Monitoring:** IoT based shipment monitoring systems use sensors such as temp, humidity, to monitor the conditions and send data to cloud, where it can be analyzed to detect food spoilage. The analysis and interpretation of data on the environmental conditions inside the containers and food truck positioning can enable more effective routing decisions in real time. For fragile products, vibration levels during shipments can be tracked using accelerometer and gyroscope sensors attached to IOT devices.

d) **Remote Vehicle Diagnostics:** Systems use on-board IoT devices for collecting dataon Vehicle operations (speed, RPMetc.,) and status of various vehicle subsystems. Such data are can be captured by integrating on-board diagnostic systems with IOT devices using protocols such as CAN bus. These systems can send diagnostic data to a centralized servers or the cloud where it can be analysed to generate alerts and suggest remedial actions.

7) **Agriculture:**

a) Smart Irrigation:

Smart irrigation system can improve crop yields while saving water. Smart irrigation systems use IoT devices with soil moisture sensors to determine the amount of moisture on the soil and release the flow of the water through the irrigation pipes only when the moisture levels go below a predefined threshold. It also collects moisture level measurements on the server on in the cloud where the collected data can be analyzed to plan watering schedules. Cultivar's Rain Could is a device for smart irrigation that uses water valves, soil sensors, and a WiFi enabled programmable computer.



a) **Green House Control:** Green Houses are structure with glass or plastic roofs that provide conducive environment for growth of plants. The climatological conditions inside a Green House can be monitored and controlled to provide the best conditions for growth of plants. The temperature, humidity, soil moisture, lightens, Carbon-di Oxide levels are monitored using sensors. IoT systems play an importance role in green house control and help in improving productivity. The data collected from various sensors is stored on centralized servers or in the cloud where analysis is performed to optimize the control strategies and also correlate the productivity with different control strategies.

1) **Industry:**

a) **Machine diagnosis and prognosis**: Machine prognosis refers to predicting the performance of a machine by analyzing the data on the current operating conditions and how much deviation exists from the normal conditions. Machine diagnosis refers to determining the cause of a machine fault. Industrial machines have a large number of components that must function correctly for the machine to perform its operations.

b) **Indoor Air Quality Monitoring:** is very important for health and safety of the workers. Harmful and toxic gases such as Carbon monoxide, Nitrogen dioxide, Nitrogen Monoxide etc., can cause serious health problems. Wireless sensor based IOT devices can identify the hazardous zones, so that the corrective measures can be taken to ensure proper ventilation.

2) Health and LifeStyle:

a) Health & Fitness Monitoring: Wearable IOT devices that allow non-invasive and continuous monitoring of physiological parameters can help in continuous health and fitness monitoring. Health care providers can analyze the collected data to determine any health conditions or abnormalities. Commonly uses body sensors like body temperature, heart rate, pulse oximeter, blood pressure, electrocardiogram etc.

b) Wearable Electronics: Wearable gadgets and fashion electronics such as smart watches, smart glasses , smart shoes, smart wrist bands etc., provide various functions and features to assist us in our daily activities and making us to lead healthy lifestyles.