UNIT – I

Introduction to Internet of Things: Definition & Characteristics of IoT, Physical Design of IoT, Logical Design of IoT, IoT Enabling Technologies, IoT Levels & Deployment Templates Domain Specific IoTs: Home, Cities, Environment, Energy systems, Logistics, Agriculture, Health & Lifestyle.

INTRODUCTION TO INTERNET OF THINGS

Definition:

The Internet of Things has been defined as:

"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" 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.

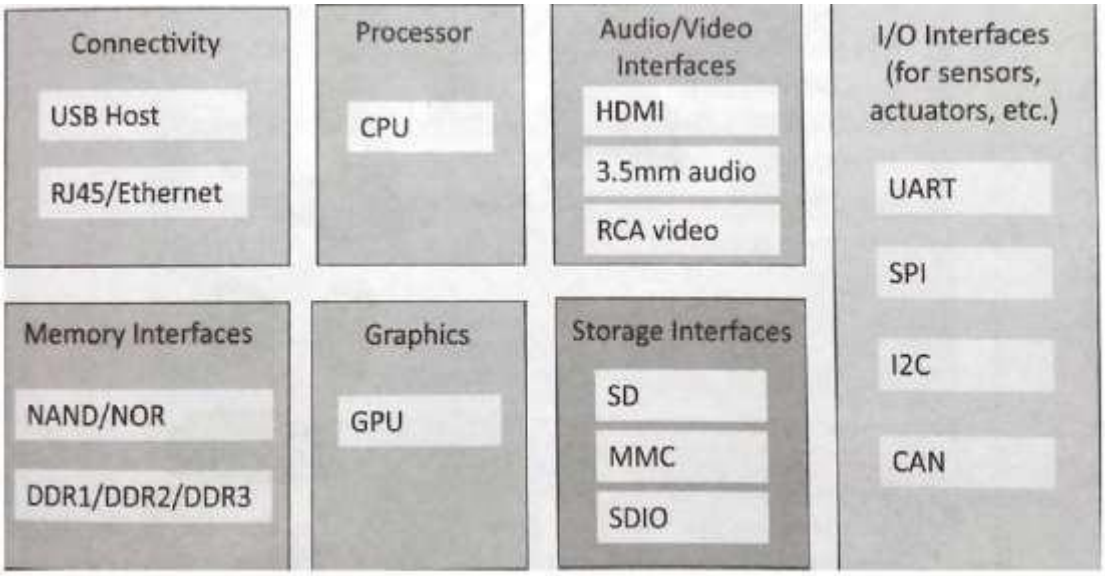
Applications of IoT:

1. Home
2. Cities

3. Environment
4. Energy
5. Retail
6. Logistics
7. Agriculture
8. Industry
9. Health & Life Style

Physical Design of IoT:

1. Things in IoT:

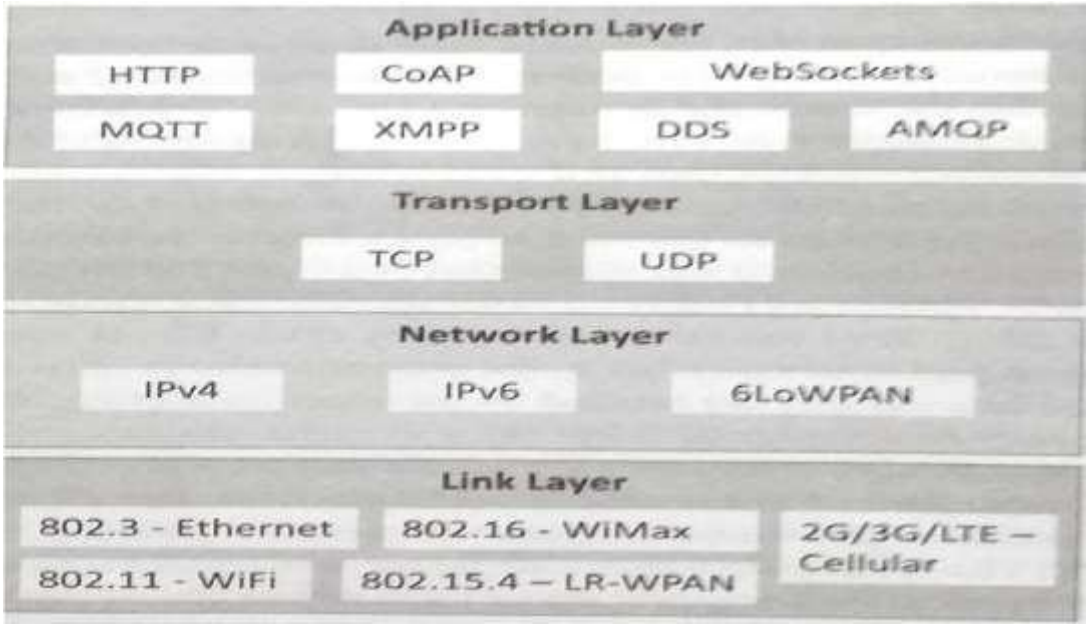


The things in IoT refer to IoT devices which have unique identities and perform remote sensing, actuating and monitoring capabilities. IoT devices can exchange data with other connected devices applications. It collects data from other devices and process data either locally or remotely.

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 over fiber.
- 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 network to destination network 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 network using a hierarchical addressing scheme. 32 bit address. Allows total of 2**32 addresses.

- IPv6: Internet Protocol version6 uses 128 bit address scheme and allows 2**128 addresses.
- 6LOWPAN: (IPv6 over Low power Wireless Personal Area Network) operates in 2.4 GHz frequency range and data transfer 250 kb/s.

c) Transport Layer: Provides end-to-end message transfer capability independent of the underlying 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 network 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.

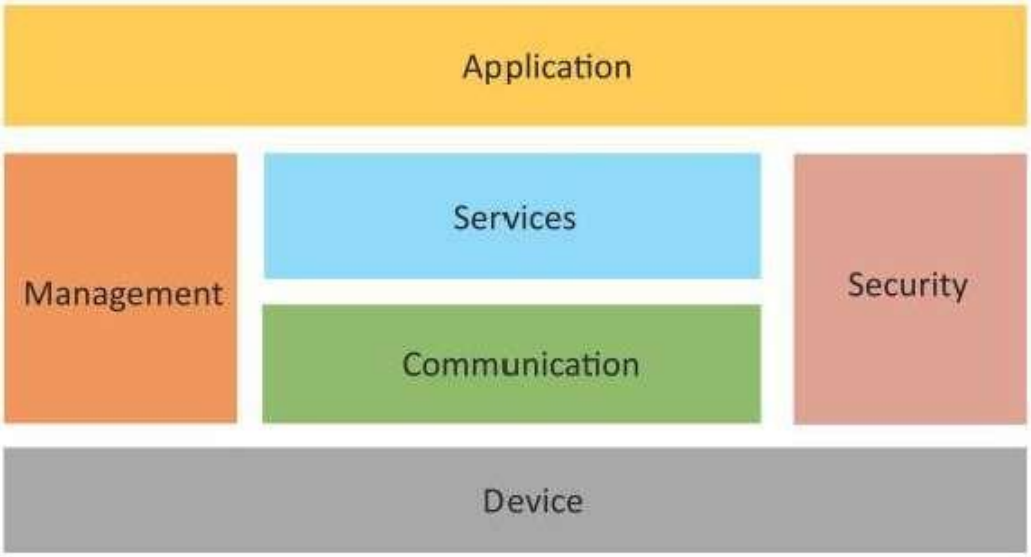
- **HTTP:** Hyper Text Transfer Protocol that forms foundation of WWW. Follow request- response model Stateless protocol.
- **CoAP:** Constrained Application Protocol for machine-to-machine (M2M) applications with constrained devices, constrained environment and constrained n/w. Uses client- server architecture.
- **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:

This system refers to an abstract represent of entities and processes without going into the low level specifies of implementation. The steps in logical design are:

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.

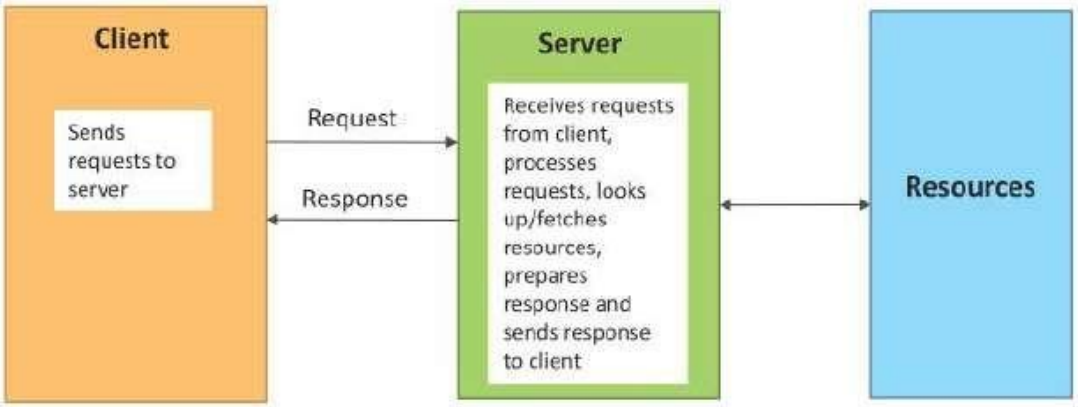


- Device: An IoT system comprises of devices that provide sensing, actuation, and monitoring and control functions.
- Communication: handles the communication for IoT system.
- Services: for device monitoring, device control services, data publishing services and services for device discovery.
- Management: 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 provides an interface that the users can use to control and monitor various aspects of IoT system.

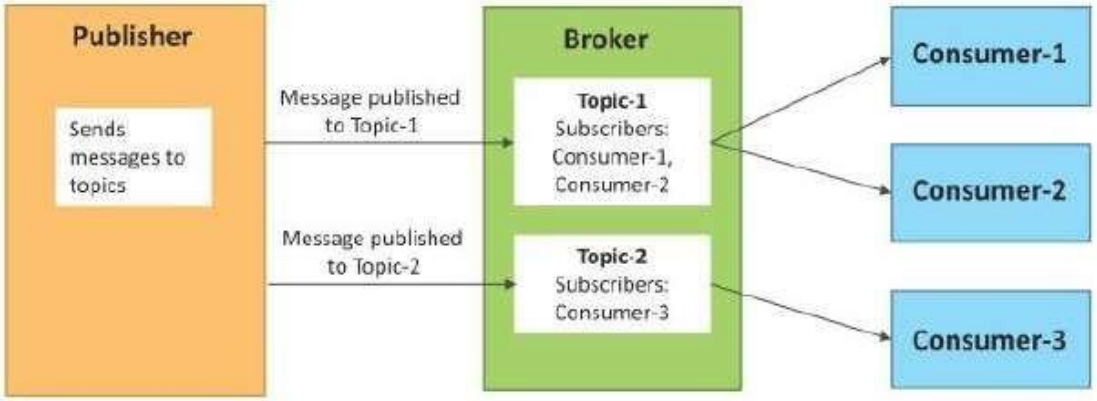
2. IoT Communication Models:

a) Request-Response b) Publish-Subscribe c) Push-Pull d) Exclusive Pair

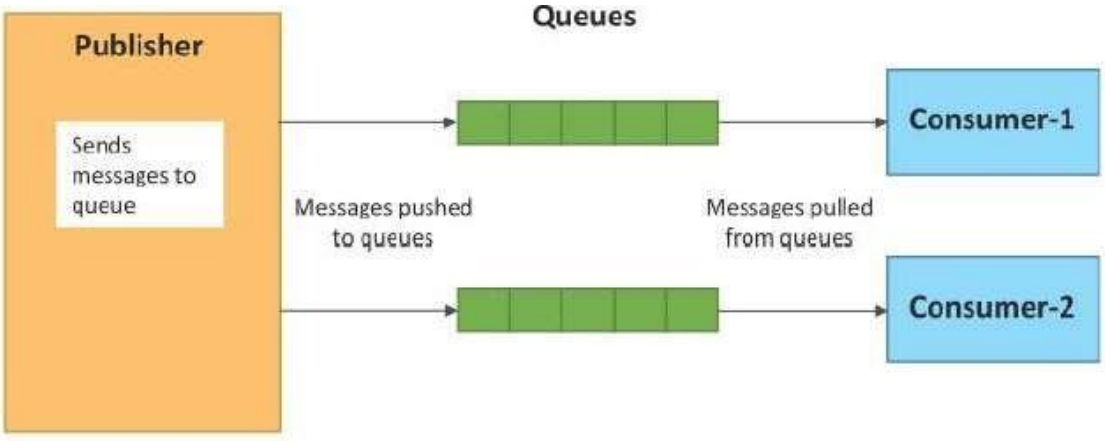
a) Request-Response Model: In which the client sends request to the server and the server replies to requests. Is a stateless communication model and each request-response pair is independent of others.



b) Publish-Subscribe Model: 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.

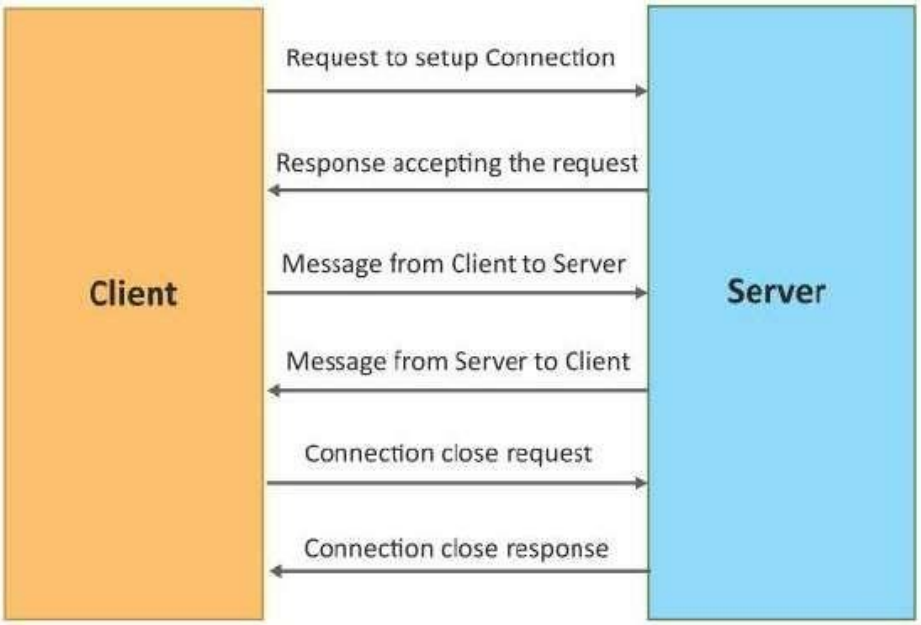


c) Push-Pull: In which data producers push data to queues and consumers pull data from the queues. Producers do not need to aware of the consumers. Queues help in decoupling the message between the producers and consumers.



d) Exclusive Pair: This 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.



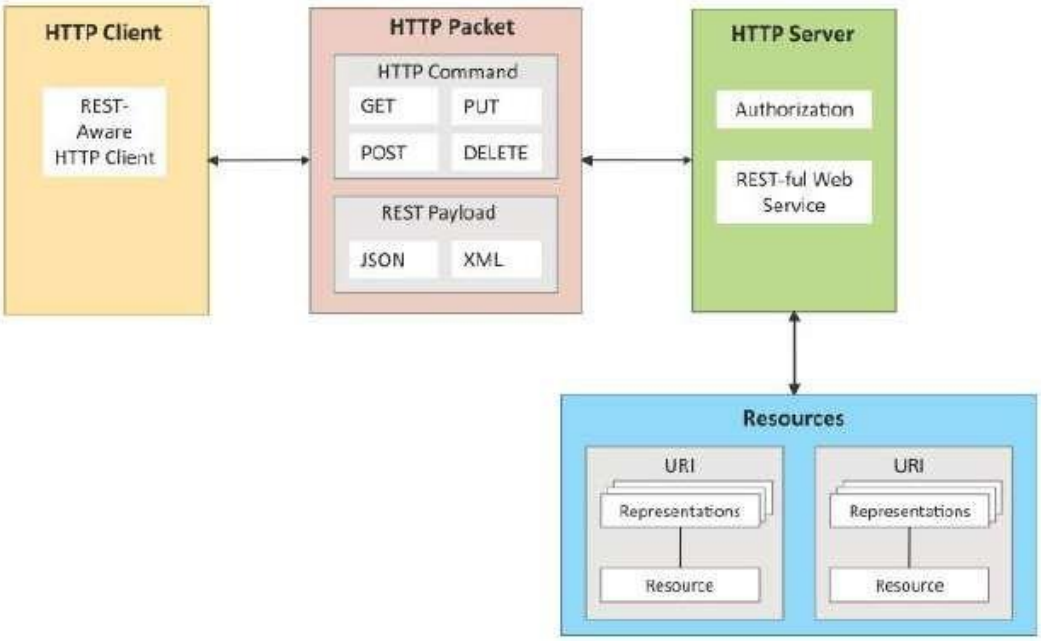
3) IoT Communication APIs: Two communication APIs are:

a) REST based communication APIs(Request-Response Based Model)

b) WebSocket based Communication APIs(Exclusive PairBased 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: The following Figure shows communication between client servers 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.

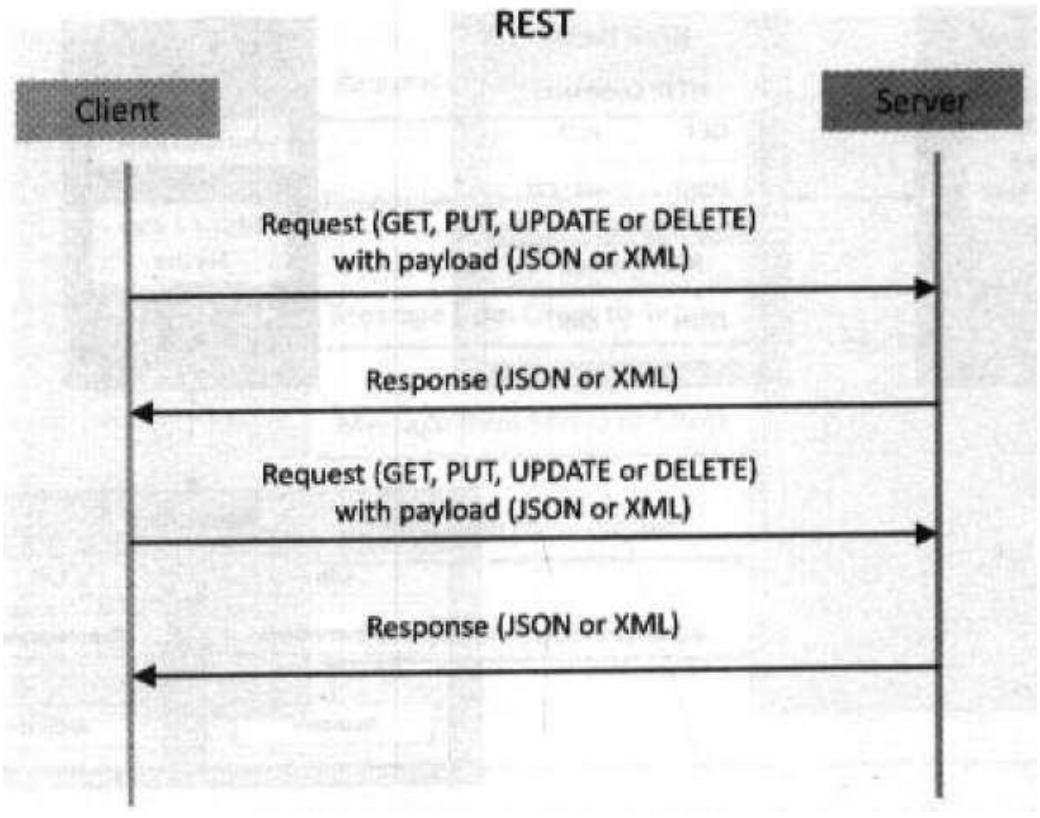
Cache-able: Cache constraint requires that the data within a response to a request be implicitly or explicitly labeled as cache-able or non-cacheable. If a response is cache-able, then a client cache is given the right to reuse that response data for later, equivalent requests.

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.

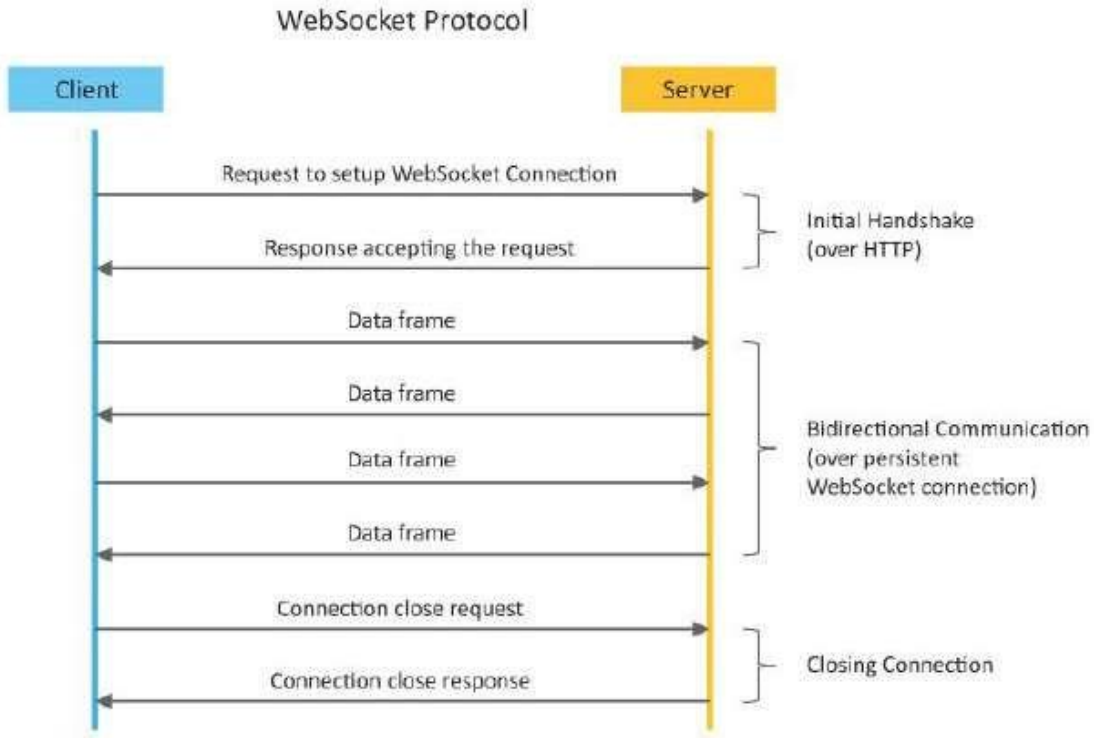
Code on Demand: Servers can provide executable code or scripts for clients to execute in their context. This constraint is the only one that is optional.

Request-Response model used by REST:



RESTful 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.

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.



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 other data, which is aggregated and analyzed.
- Indoor air quality monitoring systems: to collect data on the indoor air quality and concentration of various gases.
- Soil Moisture Monitoring Systems: to monitor soil moisture at variouslocations.
- Surveillance Systems: use WSNs for collecting surveillance data (motiondata detection).
- Smart Grids : use WSNs for monitoring grids at variouspoints.

- 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: 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: 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.

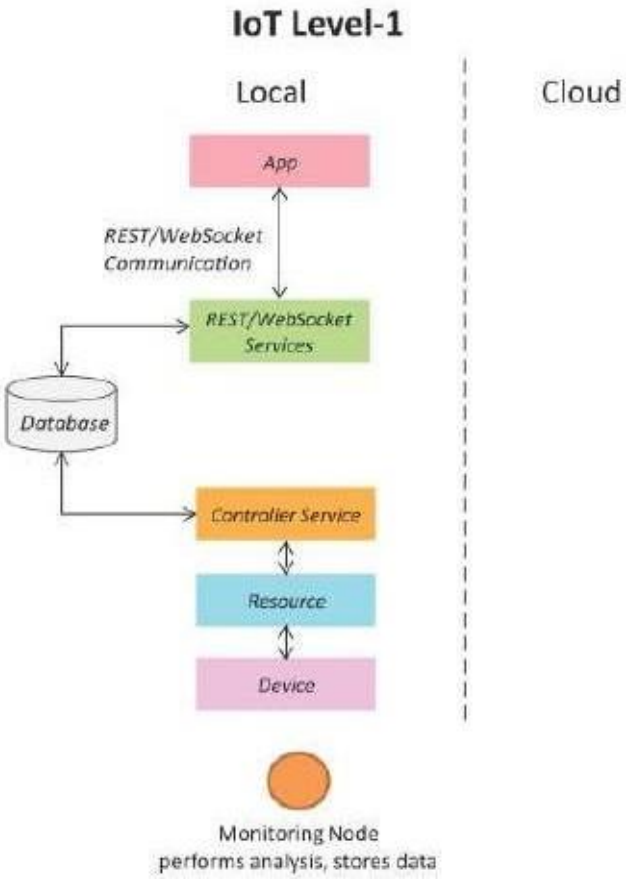
- Allow devices to exchange data over network.
- Define the exchange formats, data encoding addressing schemes for device and routing of packets from source to destination.
- It includes sequence control, flow control and retransmission of lost packets.

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.

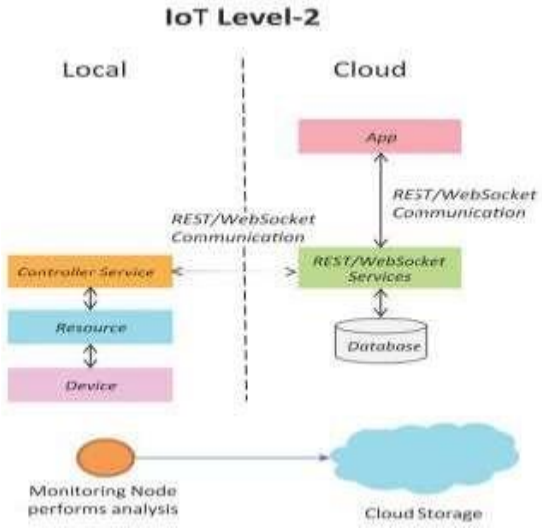
IoT Levels and Deployment Templates:

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

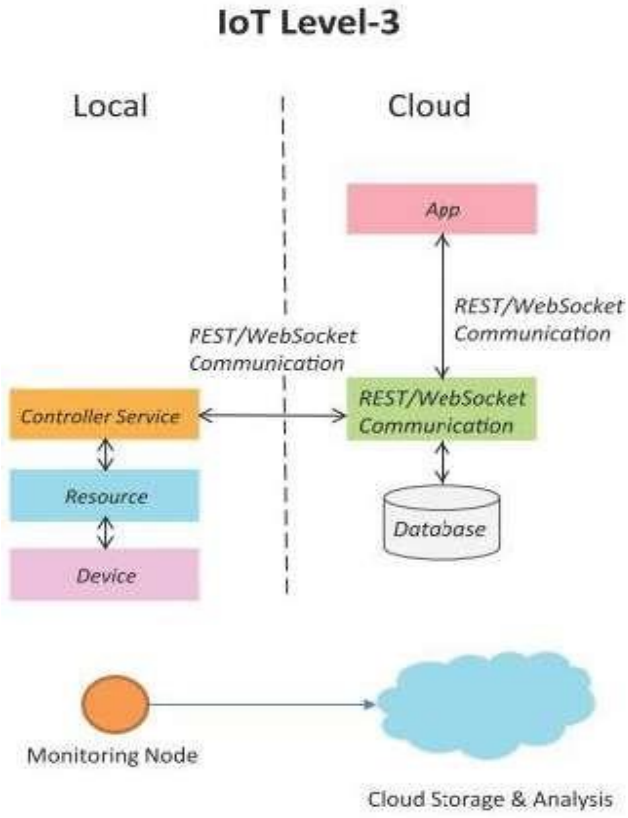
and low complexity solutions where the data involved is not big and analysis requirement are not computationally intensive. An example, of IoT Level1 is Home automation.



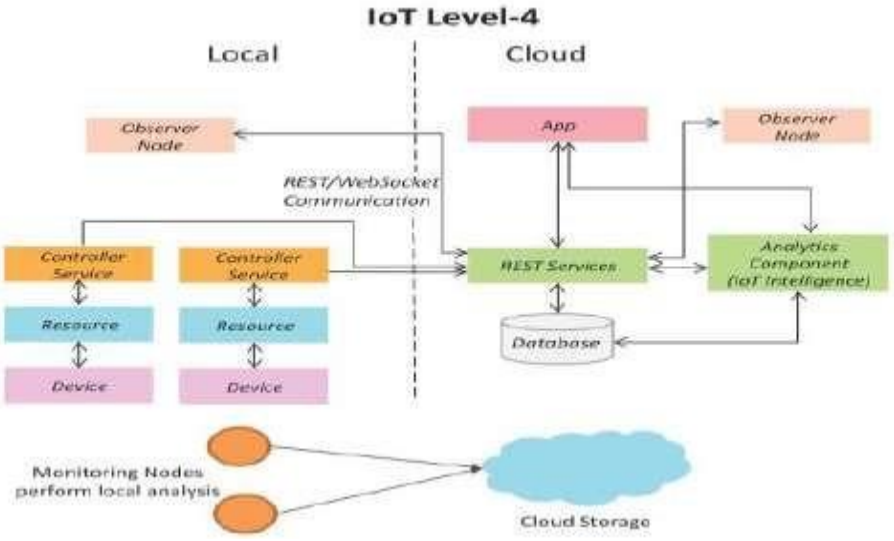
2) IoT Level2: It has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not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



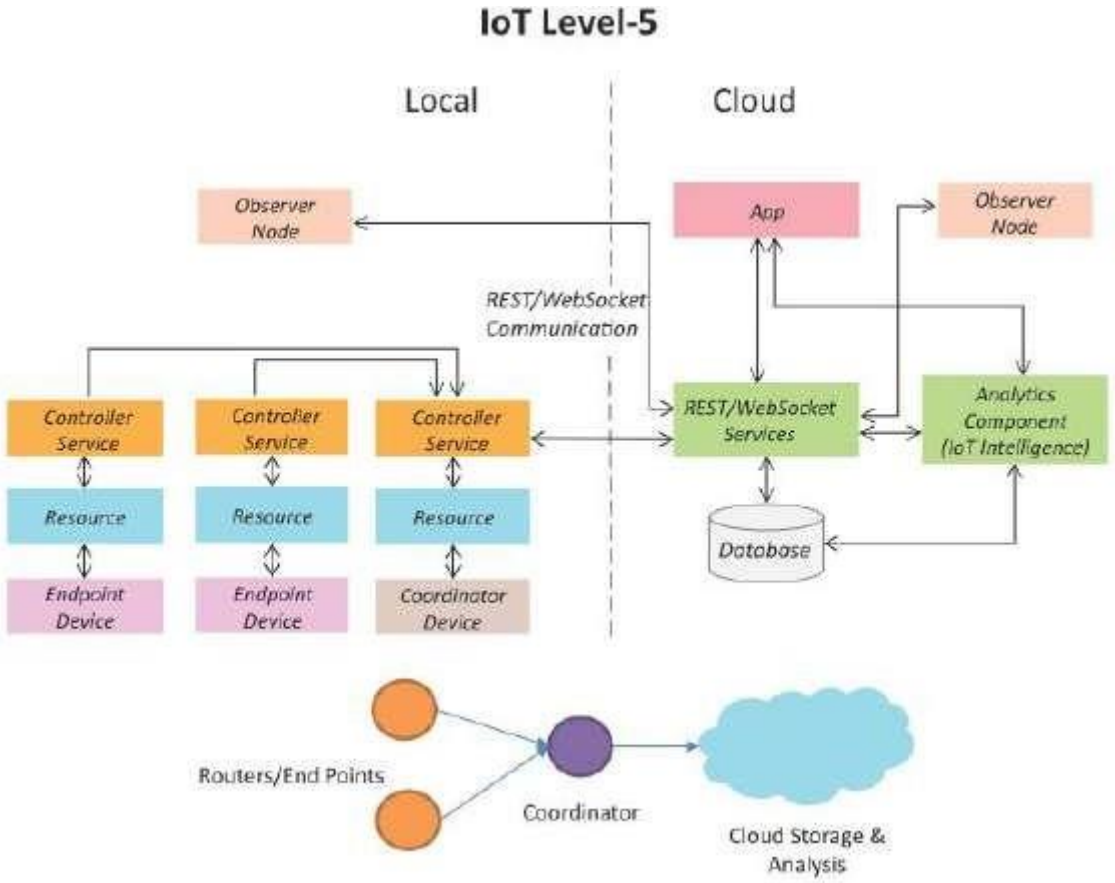
3) IoT Level3: system has a single node. Data is stored and analyzed in the cloud application is cloud based as shown in the following figure. Level3 IoT systems are suitable for solutions where the data involved is big and analysis requirements are computationally intensive. An example, of IoT level3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



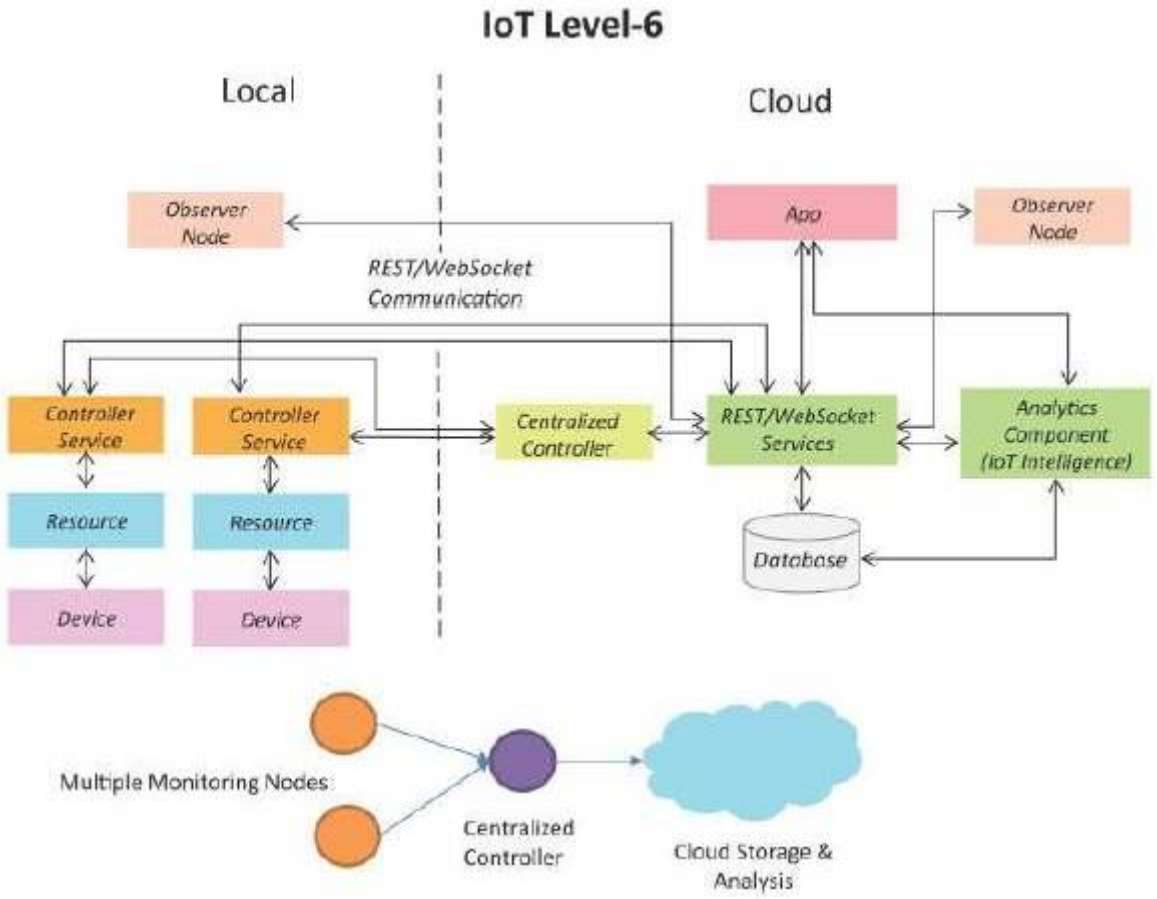
4) IoT Level4: System has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud based as shown in fig. Level4 contains local and cloud based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices. An example of 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 from the end nodes and sends to the cloud. Data is stored and analyzed in the cloud and 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 are computationally 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 the following figure. The analytics component analyses the data and stores the result in the cloud database. The results are visualized with cloud based application. The centralized controller is aware of the status of all the end nodes and sends control commands 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.

b) **Smart Appliances:** Make the management easier and also provide status information to the users remotely.

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.

d) **Smoke/Gas Detectors:** Smoke detectors are installed in homes and buildings to detect 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.

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 number of empty parking slots and send information over internet to smart application backends.

b) **Smart Lighting:** For roads, parks and buildings can help in saving energy.

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.

d) **Structural Health Monitoring:** Uses a network of sensors to monitor the vibration levels in the structures such as bridges and buildings.

e) **Surveillance:** The video feeds from surveillance cameras can be aggregated in cloud based scalable storage solution.

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.

3) Environment:

a) **Weather Monitoring:** Systems collect data from a number 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 number of sensor nodes that monitor the water level and flow rate sensors.

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 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:

a) **Inventory Management:** IoT systems enable remote monitoring of inventory using data collected by RFID readers.

b) **Smart Payments:** Solutions such as contact-less payments powered by technologies such as Near Field Communication(NFC) and Bluetooth.

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.

6) Logistics:

a) **Route generation & scheduling:** IoT based system backed by cloud can provide first response to the route generation queries and can be scaled upto serve a large transportation network.

b) **Fleet Tracking:** Use GPS to track locations of vehicles inreal-time.

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 spoilage.

d) **Remote Vehicle Diagnostics:** Systems use on-board IoT devices for collecting data on Vehicle operations (speed, RPMetc.,) and status of various vehicle subsystems.

7) Agriculture:

a) **Smart Irrigation:** to determine moisture amount in soil.

b) **Green House Control:** to improve productivity.

8) Industry:

a) Machine diagnosis and prognosis

b) Indoor Air Quality Monitoring

9) Health and LifeStyle:

a) Health & Fitness Monitoring

b) Wearable Electronics

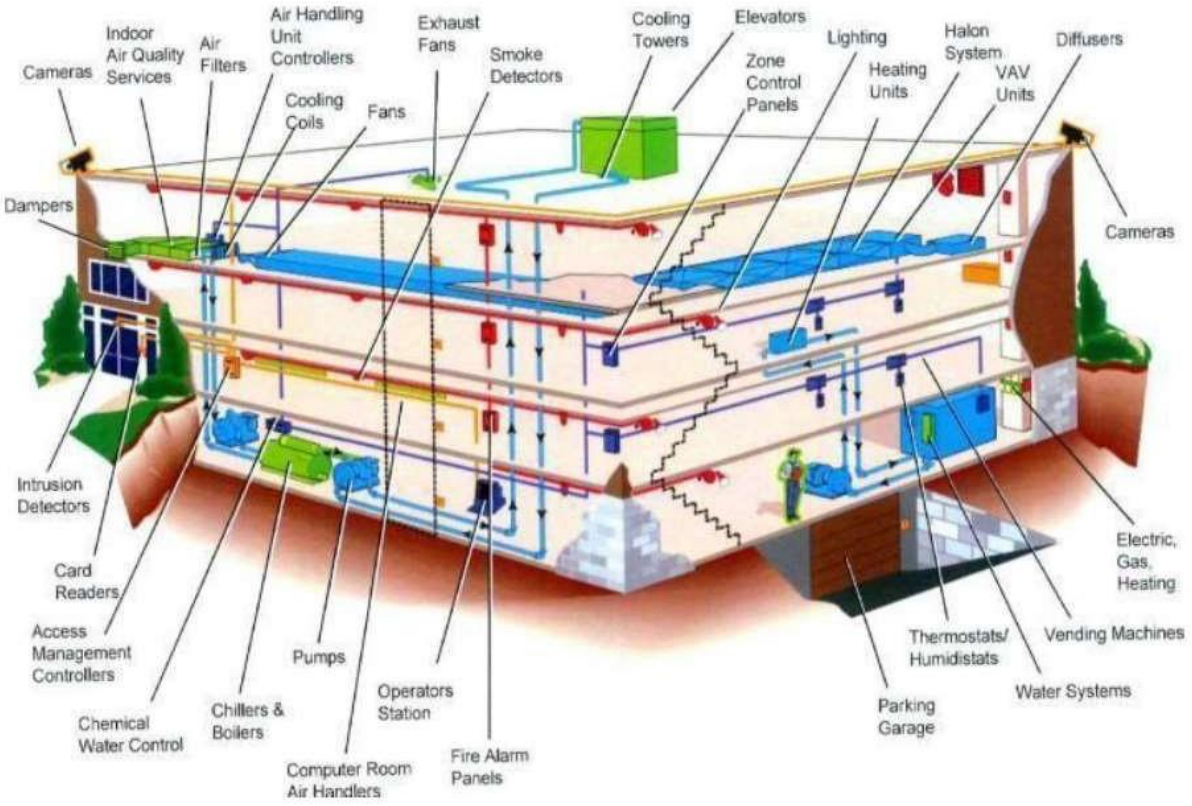
Case Study in IoT: Home Automation:

An IoT software-based approach on the field of Home Automation. Common use-cases include measuring home conditions, controlling home appliances and controlling home access through RFID cards as an example and windows through servo locks. However, the main focus of this paper is to maximize the security of homes through IoT. More specifically, monitoring and controlling servo door locks, door sensors, surveillance cameras, surveillance car and smoke detectors, which help ensuring and maximizing safety and security of homes.
A user has the following features through a mobile application in which he/she:

1. can turn on or off LED lights and monitor the state of the LED.
2. can lock and unlock doors through servo motors and monitor if the doors are locked or unlocked.
3. can monitor if the doors are closed or opened through IR sensors.
4. is notified through email if the door is left open for too long.
5. is notified of who entered through the door as the camera captures the face image and send it to him/her via email.
6. is notified through email if the fire detector detect smoke.
7. is able to control the surveillance car from anywhere to monitor his/her home.

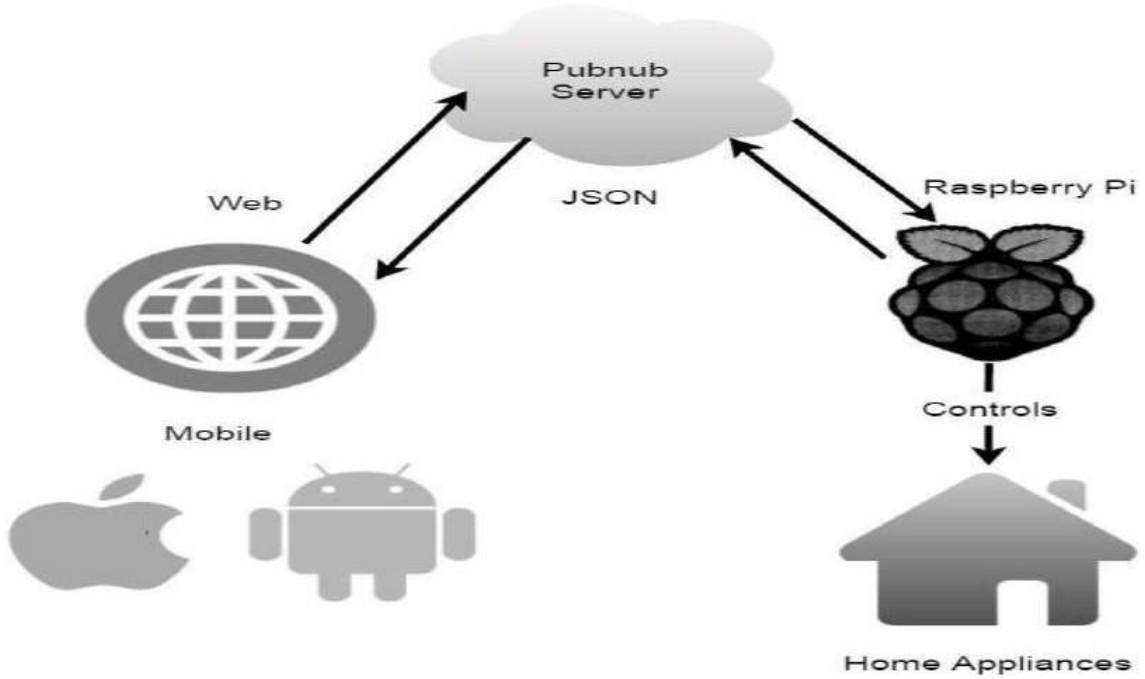
As the field of Home Automation through IoT is a wide application in a very wide and challenging field due to the reasons mentioned in the previous paragraphs, I chose to work on that field as part of this thesis, specifically in maintaining and ensuring security and safety inside home.

IoT aims in creating a network between objects embedded with sensors, that can store, analyze, communicate and exchange data together over the internet. This leads to efficient industry, manufacturing, efficient energy management, resource management, accurate health care, smarter business decisions based on analyzed data, safer driving through smart cars that are able to communicate together, smart home automation and countless more applications.



The system designed for the home automation project presented in this paper needs a control unit, a computer, to be able to control the different electrical devices connected to it. Raspberry Pi, is a credit-card tiny computer, that can be plugged to a monitor, uses standard keyboard and mouse, that enables people of different ages learn how to program.

Illustrates the publish/subscribe model provided by PubNub



Illustrates the system architecture used in this home automation project.

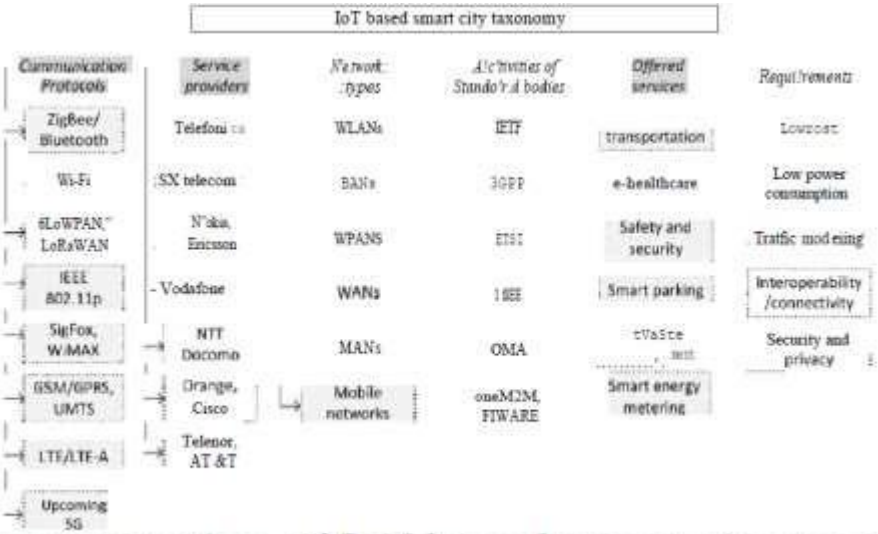
To simplify the publish/subscribe model along with the system architecture used in this Home Automation project, here is the explanation of the steps of constructing it: Different sensors, cameras and servo motors were connected to the Raspberry Pi. It was programmed to collect and publish the data, in the form of JSON string, acquired from these devices to PubNub. Data is published from the Raspberry Pi by providing it with the "publish key" and the "channel name". The data is sent to the channel provided by PubNub servers, and forwarded by PubNub to the subscribers of this channel.

The subscriber in this scenario, of a user acquiring data and readings by the sensors and monitoring devices, is the web/mobile application. The "subscription key" and "channel name" is embedded in the web/mobile application's code. Allowing it to receive messages forwarded by PubNub. On the other hand, in a scenario where the user wants to send a command to home appliances, controlling the LED lights for example, the web/mobile application is the publisher provided by the "publish key" and the "channel name". The command is sent in the form of JSON string to PubNub servers, while the "subscription key" and "channel name" is embedded in the Raspberry Pi code. This allows the Raspberry Pi to receive any published strings on the channel it is subscribed to. Upon receiving the JSON string, the Raspberry Pi take the action specified by that string. This allows full control and monitoring of all devices connected to the Raspberry Pi by the user.

Case Study in IoT: Smart Cities:

The Internet-of-Things (IoT) is the novel cutting-edge technology which proffers to connect plethora of digital devices endowed with several sensing, actuation and computing capabilities with the Internet, thus offers manifold new services in the context of a smart city. The appealing IoT services and big data analytics are enabling smart city initiatives all over the world. These services are transforming cities by improving infrastructure, transportation systems, reduced traffic congestion, waste management and the quality of human life. In this paper, we devise a taxonomy to best bring forth a generic overview of IoT paradigm for smart cities, integrated information and communication technologies (ICT), network types, possible opportunities and major requirements. Moreover, an overview of the up-to-date efforts from standard bodies is presented. Later, we give an overview of existing open source IoT platforms for realizing smart city applications followed by several exemplary case studies. In addition, we summarize the latest synergies and initiatives worldwide taken to promote IoT in the context of smart cities. Finally, we highlight several challenges in order to give future research directions.

An illustration based smart city



A representation of IoT-based smart city taxonomy

IOT BASED SMART CITY TAXONOMY:

This section presents a taxonomy of IoT based smart cities which categorizes the literature on the basis of existing communication protocols, major service providers, network types, standardization efforts, offered services, and crucial requirements.

Communication Protocols:

IoT based smart city realization significantly relies on numerous short and wide range communication protocols to transport data between devices and backend servers. Most prominent short range wireless technologies include Zig-Bee, Bluetooth, Wi-Fi, Wireless Metropolitan Area Network (WiMAX) and IEEE 802.11p which are primarily used in smart metering, e-healthcare and vehicular communication. Wide range technologies such as Global System for Mobile communication (GSM) and GPRS, Long-Term Evolution (LTE), LTE- Advanced are commonly utilized in ITS such as vehicle-to infrastructure (V2I), mobile e- healthcare, smart grid and infotainment services. Additionally, LTE-M is considered as an evolution for cellular IoT (C-IoT). In Release 13, 3GPP plans to further improve coverage, battery lifetime as well as device complexity [7]. Besides well-known existing protocols, LoRa alliance standardizes the LoRaWAN protocol to support smart city applications to primarily ensure interoperability between several operators. Moreover, SIGFOX is an ultra-narrowband radio technology with full star-based infrastructure offers a high scalable global network for realizing smart city applications with extremely low power consumption. A comparative summary2 of the major communication protocols.

Service Providers:

Pike Research on smart cities estimated this market will grow to hundreds of billion dollars by 2020, with an annual growth of nearly 16 billion. IoT is recognized as a potential source to increase revenue of service providers. Thus, well-known worldwide service providers have already started exploring this novel cutting edge communication paradigm. Major service providers include Telefonica, SK telecom, Nokia, Ericsson, Vodafone, NTT Docomo, Orange, Telenor group and AT&T which offer variety of services and platforms for smart city applications such as ITS and logistics, smart metering, home automation and e-healthcare.

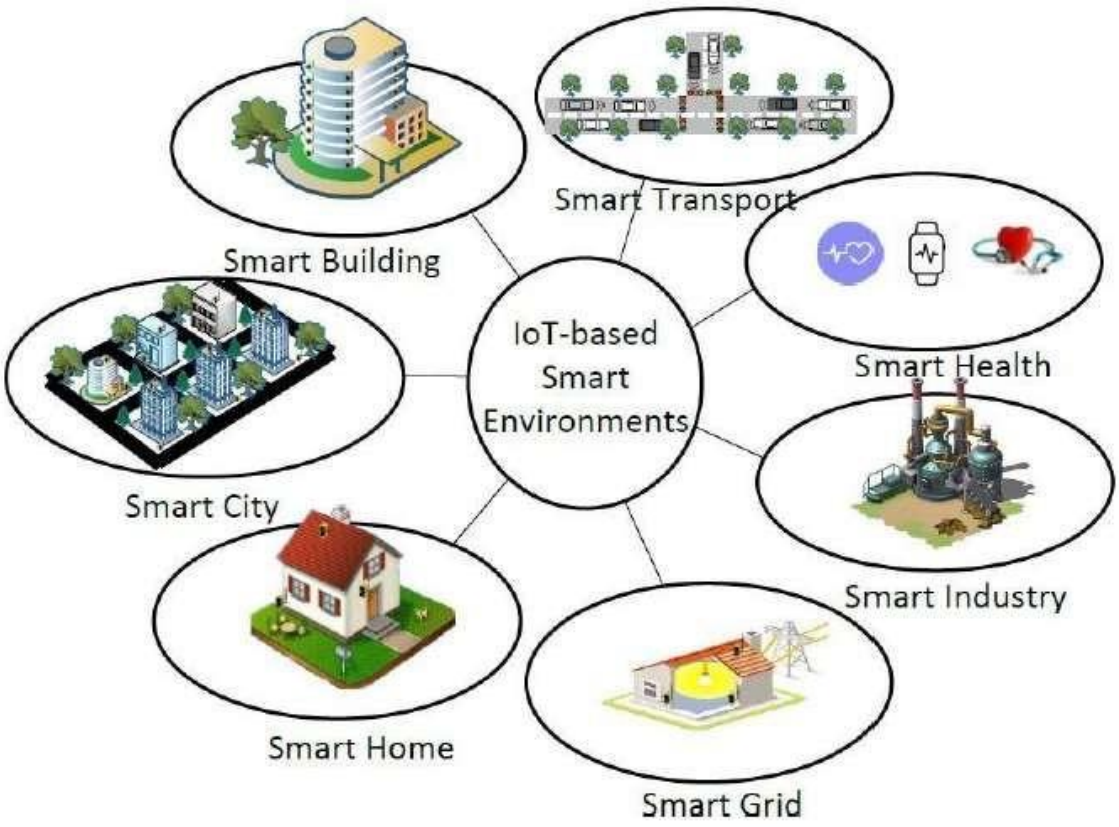
Network Types:

IoT based smart city applications rely on numerous network topologies to accomplish a fully autonomous environment. The capillary IoT networks offer services over a short range. Examples include wireless local area networks (WLANs), BANs and wireless personal area networks (WPANs). The application areas include indoor e-healthcare services, home automation, street lighting. On the other hand, applications such as ITS, mobile e-healthcare and waste management use wide area networks (WANs), metropolitan area networks (MANs),and mobile communication networks. The above networks pose distinct features in terms of data, size, coverage, latency requirements, and capacity.

Case Study in IoT: Smart Environment:

The rapid advancements in communication technologies and the explosive growth of Internet of Things (IoT) have enabled the physical world to invisibly interweave with actuators, sensors, and other computational elements while maintaining continuous network connectivity. The continuously connected physical world with computational elements forms a smart environment. A smart environment aims to support and enhance the abilities of its dwellers in executing their tasks, such as navigating through unfamiliar space and moving heavy objects for the elderly, to name a few. Researchers have conducted a number of efforts to use IoT to facilitate our lives and to investigate the effect of IoTbased smart environments on human life. This paper surveys the state-of-the-art research efforts to enable the IoT-based smart environments. We categorize and classify the literature by devising a taxonomy based on communication enablers, network types, technologies, local area wireless standards, objectives, and characteristics. Moreover, the paper highlights the unprecedented opportunities brought about by IoT-based smart environments and their effect on human life.

Some reported case studies from different enterprises are also presented. Finally, we discuss open research challenges for enabling IoT-based smart environments.



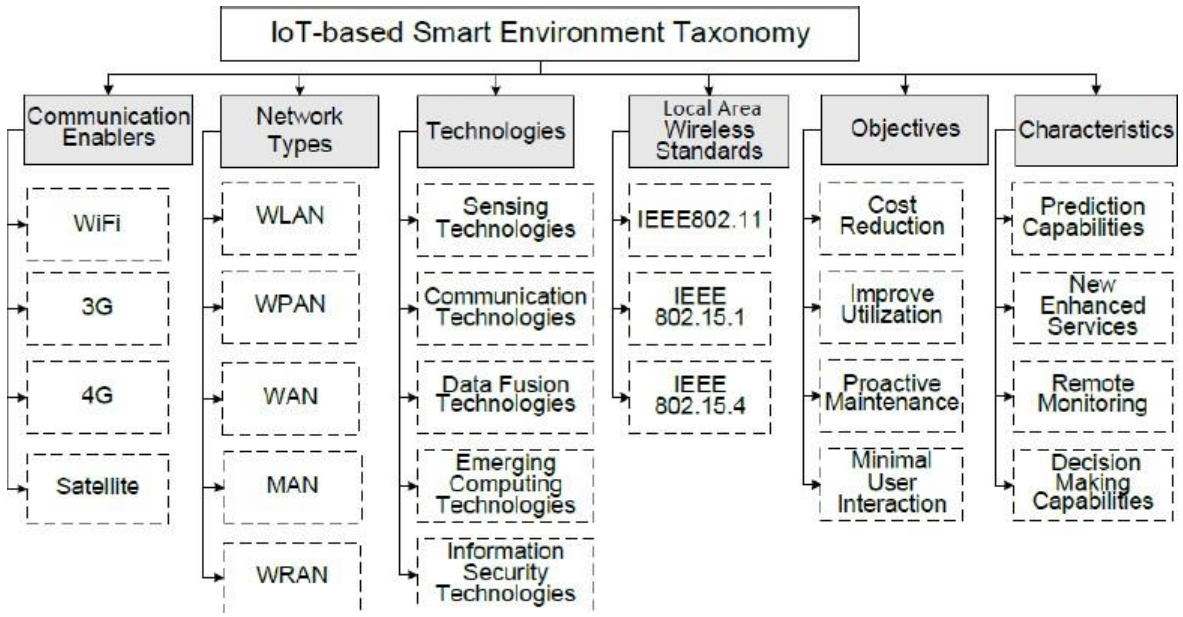
IoT-based Smart Environments

Immense developments and increasing miniaturization of computer technology have enabled tiny sensors and processors to be integrated into everyday objects. This advancement is further supported by tremendous developments in areas such as portable appliances and devices, pervasive computing, wireless sensor networking, wireless mobile communications, machine learning-based decision making, IPv6 support, human computer interfaces, and agent technologies to make the dream of smart environment a reality. A smart environment is a connected small world where sensor-enabled connected devices work collaboratively to make the lives of dwellers comfortable. The term smart refers to the ability to autonomously obtain and applies knowledge; and the term environment refers to the surroundings. Therefore, a smart environment is one that is capable of obtaining knowledge and applying it to adapt according to its inhabitants needs to ameliorate their experience of that environment.

The functional capabilities of smart objects are further enhanced by interconnecting them with other objects using different wireless technologies. In this context, IPv6 plays a vital role because of several features, including better security mechanisms, scalability in case of billion of connected devices, and the elimination of NAT barriers1. This concept of

connecting smart objects with the Internet was first coined by Kevin Ashton as ―Internet of Things (IoT).

Nowadays, IoT is receiving attention in a number of fields such as healthcare, transport, and industry, among others. Several research efforts have been conducted to integrate IoT with smart environments. The integration of IoT with a smart environment extends the capabilities of smart objects by enabling the user to monitor the environment from remote sites. IoT can be integrated with different smart environments based on the application requirements. The work on IoT-based smart environments can generally be classified into the following areas: a) smart cities, b) smart homes, c) smart grid, d) smart buildings, e) smart transportation, f) smart health, and g) smart industry. Illustrates the IoT-based smart environments.



The taxonomy of the IoT based smart environment. The devised taxonomy is based on the following parameters: communication enablers, network types, technologies, wireless standards, objectives, and characteristics.

Communication Enablers:

Communication enablers refer to wireless technologies used to communicate across the Internet. The key wireless Internet technologies are WiFi, 3G, 4G, and satellite. WiFi is mainly used in smart homes, smart cities, smart transportation, smart industries, and smart building environments; whereas, 3G and 4G are mainly used in smart cities and smart grid environments. Satellites are used in smart transportation, smart cities, and smart grid environments. Table presents the comparative summary of the communication technologies used in IoT based smart environments.

Network Types:

IoT-based smart environments rely on different types of networks to perform the collaborative tasks for making the lives of inhabitants more comfortable. The main networks are wireless local area networks (WLANs), wireless personal area networks (WPANs), wide area networks (WANs), metropolitan area networks (MANs), and wireless regional area networks (WRANs). These networks have different characteristics in terms of size, data transfer, and supported reach ability.

Technologies

IoT-based smart environments leverage various technologies to form a comfortable and suitable ecosystem. These technologies are including sensing, communication, data fusion, emerging computing, and information security. Sensing technologies are commonly used to acquire data from various locations and transmit it using communication technologies to a central location. The emerging computing technologies, such as cloud computing and fog computing, deployed in the central location, leverage the data fusion technologies for integrating the data coming from heterogeneous resources. In addition, smart environments also use information security technologies to ensure data integrity and user privacy.

Local Area Wireless Standards

The commonly used local area wireless standards in IoT-based smart environments are IEEE 802.11, IEEE 802.15.1, and IEEE 802.15.4. These standard technologies are used inside the smart environment to transfer the collected data among different devices. IEEE 802.11 is used in smart homes, smart buildings, and smart cities. IEEE 802.15.1 and IEEE 802.15.4 have relatively shorter coverage than IEEE 802.11 and are used mainly in sensors and other objects deployed in the smart environments.

****