SRI MUTHUKUMARAN INSTITUTE OF TECHNOLOGY

Chikkarayapuram, Near Mangadu, Chennai- 600 069.
Academic Year 2023 – 2024/ Odd Semester
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
(Regulation – 2021)
V SEM/ III YEAR
CEC 368 - IOT BASED SYSTEMS DESIGN

UNIT I - INTRODUCTION TO INTERNET OF THINGS

PART A

1.**Define Internet of Things.**

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 n/w, often communicate data associated with users and their environments.

2. **Mention the characteristics of IoT.**

- **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.
- **Self Configuring:** Itallowing a large number of devices to work together to provide certain functionality.
- **Inter Operable Communication Protocols:** support a number of interoperable communication protocols and can communicate with other devices and also with infrastructure.
- **Unique Identity:** Each IoT device has a unique identity and a unique identifier(IP address).
- **Integrated into Information Network:** that allow them to communicate and exchange data with other devices and systems.

3.**List out the key application functionalities of IoT systems**.

The key application functionalities of IoTsystems:

1.Information and analysis

a. Tracking behavior
b. Enhanced situational awareness
c. Sensor-drivendecisionanalytics

2. Automation and control
   Process optimization
   Optimized resource consumption
   Complex autonomous systems

4.**List out the requirements of cloud computing in Iot system?**

Minimizing latency: Milliseconds matter for many types of industrial systems, such as when you are trying to prevent manufacturing line shutdowns or restore electrical service. Analyzing data close to the device that collected the data can make a difference between averting disaster and a cascading system failure.

■ **Conserving network bandwidth:** Offshore oil rigs generate 500 GB of data weekly. Commercial jets generate 10 TB for every 30 minutes of flight. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge

devices to the cloud. Nor is it necessary because many critical analyses do not require cloud-scale processing and storage.

- **Increasing local efficiency:** Collecting and securing data across a wide geographic area with different environmental conditions may not be useful. The environmental conditions in one area will trigger a local response independent from the conditions of another site hundreds of miles away. Analyzing both areas in the same cloud system may not be necessary for immediate efficiency.

5.Mention the data-related problems of fog computing

Bandwidth in last-mile IoT networks is very limited. When dealing with thousands/ millions of devices, available bandwidth may be on order of tens of Kbps per device or even less.

- Latency can be very high. Instead of dealing with latency in the milliseconds range, large IoT networks often introduce latency of hundreds to thousands of milliseconds.
- Network backhaul from the gateway can be unreliable and often depends on 3G/LTE or even satellite links. Backhaul links can also be expensive if a per-byte data usage model is necessary.
- The volume of data transmitted over the backhaul can be high, and much of the data may not really be that interesting (such as simple polling messages).
- Big data is getting bigger. The concept of storing and analyzing all sensor data in the cloud is impractical. The sheer volume of data generated makes real-time analysis and response to the data almost impossible.

6.Define fog computing.

The best-known embodiment of edge services in IoT is fog computing. Any device with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and IoT gateways. Analyzing IoT data close to where it is collected minimizes latency, offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the local network.

7. List out the characteristics of fog computing.

The defining characteristic of fog computing are as follows:

- **Contextual location awareness and low latency:** The fog node sits as close to the IoT endpoint as possible to deliver distributed computing.
- **Geographic distribution:** In sharp contrast to the more centralized cloud, the services and applications targeted by the fog nodes demand widely distributed deployments.
- **Deployment near IoT endpoints:** Fog nodes are typically deployed in the presence of a large number of IoT endpoints. For example, typical metering deployments often see 3000 to 4000 nodes per gateway router, which also functions as the fog computing node.

8.What is edge computing?

Edge computing is also sometimes called “mist” computing. If clouds exist in the sky, and fog sits near the ground, then mist is what actually sits on the ground. Thus, the concept of mist is to extend fog to the furthest point possible, right into the IoT endpoint device itself.

9. Define sensor.

A sensor does exactly as its name indicates: It senses. More specifically, a sensor measures some physical quantity and converts that measurement reading into a digital representation. That digital representation is typically passed to another device for transformation into useful data that can be consumed by intelligent devices or humans.

10. **List out the different categorise of sensors.**

Active or passive: Sensors can be categorized based on whether they produce an energy output and typically require an external power supply (active) or whether they simply receive energy and typically require no external power supply (passive).

■ **Invasive or non-invasive:** Sensors can be categorized based on whether a sensor is part of the environment it is measuring (invasive) or external to it (non-invasive).
■ **Contact or no-contact:** Sensors can be categorized based on whether they require physical contact with what they are measuring (contact) or not (no-contact).
■ **Absolute or relative:** Sensors can be categorized based on whether they measure on an absolute scale (absolute) or based on a difference with a fixed or variable reference value (relative).

11.Mention the different types of sensors.

1.Acoustic sensor- Acoustic sensors measure sound levels andconvert that information into digital or analog
data signals.
e.g. Microphone, geophone,hydrophone
2.Humidity sensor-Humidity sensors detect humidity (amount ofwater vapor) in the air or a mass. Humidity
levels can be measured in various ways: absolutehumidity, relative humidity, mass ratio, and so on.
e.g Hygrometer,humistor, soilmoisture sensor
Light sensor-Light sensors detect the presence of light (visibleor invisible).
e.g Infrared sensor,photodetector,flame detector
Radiation sensor- Radiation sensors detect radiation in the environment. Radiation can be sensed by scintillating or ionization detection.
e.g Geiger-Müllercounter, scintillator, neutron detector

12. What is actuator?
Actuators are natural complements to sensors. Figure 3-4 demonstrates the symmetry and complementary nature of these two types of devices. As discussed in the previous section, sensors are designed to sense and measure practically any measurable variable in the physical world. They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human). Actuators, on the others hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.

13.How the actuators can be classified.
Type of motion: Actuators can be classified based on the type of motion they produce (for example, linear, rotary, one/two/three-axes).
■ **Power:** Actuators can be classified based on their power output (for example, high power, low power, micro power)
■ **Binary or continuous:** Actuators can be classified based on the number of stable-state outputs.
■ **Area of application:** Actuators can be classified based on the specific industry or vertical where they are used.
■ **Type of energy:** Actuators can be classified based on their energy type.

14. What is MEMS
Micro-electro-mechanical systems (MEMS), sometimes simply referred to as micro-machines, can integrate and combine electric and mechanical elements, such as sensors and actuators, on a very small (millimeter or less) scale. One of the keys to this technology is a microfabrication technique that is similar to what is used
for microelectronic integrated circuits. This approach allows mass production at very low costs. The combination of tiny size, low cost, and the ability to mass produce makes MEMS an attractive option for a huge number of IoT applications.

15.Define smart objects.
Smart objects are, quite simply, the building blocks of IoT. They are what transform everyday objects into a network of intelligent objects that are able to learn from and interact with their environment in a meaningful way. It can't be stressed enough that the real power of smart objects in IoT comes from being networked together rather

than being isolated as standalone objects. This ability to communicate over a network has a multiplicative effect and allows for very sophisticated correlation and interaction between disparate smart objects.

16.Mention the characteristics of smart objects.

Processing unit
Sensors/actuators
Communication device
Power source

17. List out the trends in smart objects.

Size is decreasing: As discussed earlier, in reference to MEMS, there is a clear trend of ever-decreasing size. Some smart objects are so small they are not even visible to the naked eye. This reduced size makes smart objects easier to embed in everyday objects.

- **Power consumption is decreasing:** The different hardware components of a smart object continually consume less power. This is especially true for sensors, many of which are completely passive. Some battery-powered sensors last 10 or more years without battery replacement.
- **Processing power is increasing:** Processors are continually getting more powerful and smaller. This is a key advancement for smart objects, as they become increasingly complex and connected.
- **Communication capabilities are improving:** It's no big surprise that wireless speeds are continually increasing, but they are also increasing in range. IoT is driving the development of more and more specialized communication protocols covering a greater diversity of use cases and environments.
- **Communication is being increasingly standardized:** There is a strong push in the industry to develop open standards for IoT communication protocols. In addition, there are more and more open source efforts to advance IoT.

18. List out the technologies used for connecting smart objects.

The following subsections cover technologies for connecting smart objects:

- **IEEE 802.15.4:** This section highlights IEEE 802.15.4, an older but foundational wireless protocol for connecting smart objects.
- **IEEE 802.15.4g and IEEE 802.15.4e:** This section discusses improvements to 802.15.4 that are targeted to utilities and smart cities deployments.
- **IEEE 1901.2a:** This section discusses IEEE 1901.2a, which is a technology for connecting smart objects over power lines.
- **IEEE 802.11ah:** This section discusses IEEE 802.11ah, a technology built on the well-known 802.11 Wi-Fi standards that is specifically for smart objects.
- **LoRaWAN:** This section discusses LoRaWAN, a scalable technology designed for longer distances with low power requirements in the unlicensed spectrum.
- **NB-IoT and Other LTE Variations:** This section discusses NB-IoT and other LTE variations, which are often the choice of mobile service providers looking to connect smart objects over longer distances in the licensed spectrum.

19. What is constrained network.

Constrained-node networks are often referred to as low-power and lossy networks (LLNs). *Low-power* in the context of LLNs refers to the fact that nodes must cope with the requirements from powered and batterypoweredconstrained nodes. *Lossy networks* indicates that network performance maysuffer from interference and variability due to harsh radio environments. Layer 1 and Layer 2 protocols that can be used for constrained-node networks must be evaluated in the context of the following characteristics for use-case applicability: data rate and throughput, latency and determinism, and overhead and payload

20.List out the different forms of CloudComputing.

1.Infrastructure-as-a-service(IaaS):provides users the ability to provision computingand storage resources.These resources are provided to the usersasa virtualmachineinstancesand virtualstorage.

2.Platform-as-a-Service(PaaS):providesuserstheability todevelopanddeployapplication in cloud using the development tools, APIs, software libraries andservicesprovided bythecloud serviceprovider.

3.Software-as-a-Service(SaaS): provides the user a complete software application ortheuser interfaceto theapplicationitself.

21.What is Wireless Sensor Network. Give example.

WSN Comprises of distributed devices with sensors whichare used to monitor the environmental and physical conditions. Zig Bee is one of the mostpopularwireless technologies used by WSNs.

WSNsusedinIoTsystemsaredescribedasfollows:

- WeatherMonitoringSystem: in whichnodes collect temp, humidityandotherdata,which is aggregatedand analyzed.
- Indoor air quality monitoring systems: to collect data on the indoor air quality andconcentrationofvariousgases.
- SoilMoistureMonitoringSystems:tomonitorsoilmoistureatvariouslocations.
- SurveillanceSystems:useWSNsforcollectingsurveillancedata(motiondata detection).

SmartGrids: useWSNsformonitoring gridsat variouspoints

22.Diffrentiate level 1 and level 2.

IoT Level1: System has a single node that performs sensing and/or actuation, stores data,performsanalysis and host the application as shown in fig. Suitable for modeling lowcostandlowcomplexitysolutionswherethedatainvolvedisnotbigandanalysisrequirementarenot computationallyintensive.Ane.g.,ofIoTLevel1isHomeautomation.

IoT Level2:has a single node that performs sensing and/or actuating andlocal analysisas shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoTsystems are suitable for solutions where data are involved is big, however, the primaryanalysis requirement is not computationally intensive and can be done locally itself. Ane,g.**,**ofLevel2IoT systemforSmart Irrigation.

23. **What is Embedded Systems?**

It is a computer system that has computer hardware and softwareembedded to perform specific tasks. Embedded System range from low cost miniaturizeddevicessuchasdigitalwatchestodevicessuchasdigitalcameras,POSterminals,vending machines, appliances etc

24.Diffrentiate the class 0 and class 2 of constrained nodes.

Class 0

This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of Flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms. An example of a Class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging

new unlicensed LPWA wireless technology.

Class 2

Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and

250 KB of Flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.

25.List out the parameter mainly used in connecting objectsin iot.

Range: This section examines the importance of signal propagation and distance.
■ **Frequency Bands:** This section describes licensed and unlicensed spectrum, including sub-GHz frequencies.
■ **Power Consumption:** This section discusses the considerations required for devices connected to a stable power source compared to those that are battery powered.
■ **Topology:** This section highlights the various layouts that may be supported for connecting multiple smart objects.
■ **Constrained Devices:** This section details the limitations of certain smart objects from a connectivity perspective.
■ **Constrained-Node Networks:** This section highlights the challenges that are often encountered with networks connecting smart objects.

26.Mention the home application of iot device.

a) **Smart Lighting:** helps in saving energy by adapting the lighting to the ambient conditions and switching on/of for diming the light when needed.
b) **Smart Appliances:** make the management easier and also provide status information to theusers 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 totheuser.
d) **Smoke/GasDetectors:**Smokedetectorsareinstalledinhomesandbuildingstodetect smoke that is typically an early sign of fire. Alerts raised by smoke detectorscan be in the form of signals to a fire alarm system. Gas detectors can detect thepresenceof harmfulgases such as CO, LPGetc.,

PART B

1.Explain in detail about the IoT enabling technology.

IoT Enabling Technologies

IoTisenabledbyseveraltechnologiesincludingWirelessSensorNetworks,CloudComputing, Big Data Analytics, Embedded Systems, Security Protocols and architectures,CommunicationProtocols,WebServices,Mobileinternetandsemanticsearchengines.

2) **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 monitors oil moisture at various locations.
- Surveillance Systems: It use WSNs for collecting surveillance data(motion data detection).
- Smart Grids: use WSNs for monitoring grids at various points.

StructuralHealthMonitoringSystems:

It Use WSNs to monitor the health of structures(building, bridges) by collecting vibrations from sensor nodes deployed at various points in the structure.

3) **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.

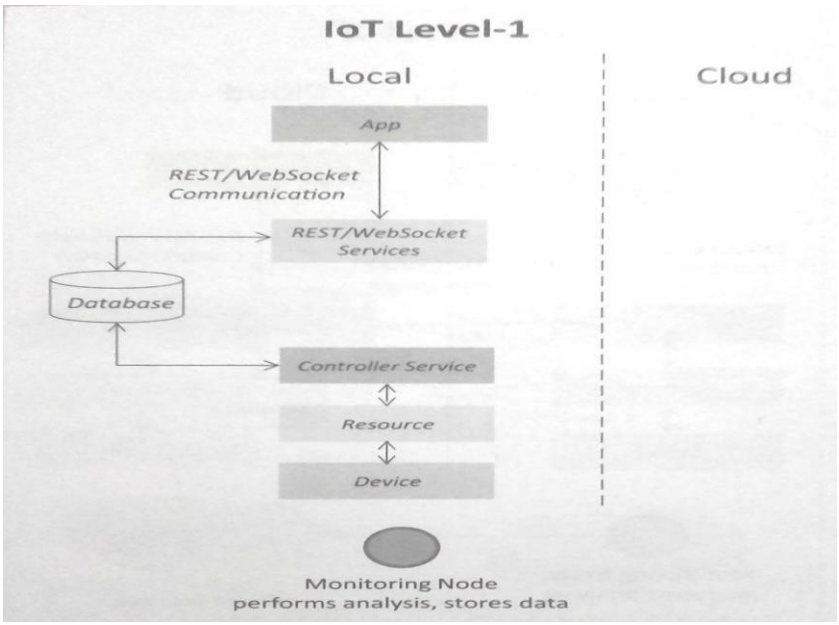
4) **Big Data Analytics:** Some examples of big data generated by IoT are
   - Sensor data generated by IoT systems.
   - Machine sensor data collected from sensors established in industrial and energy systems.
   - Health and fitness data generated IoT devices.
   - Data generated by IoT systems for location and tracking vehicles.
   - Data generated by retail inventory monitoring systems.

5) **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 include sequence control ,flow control and retransmission of lost packets.

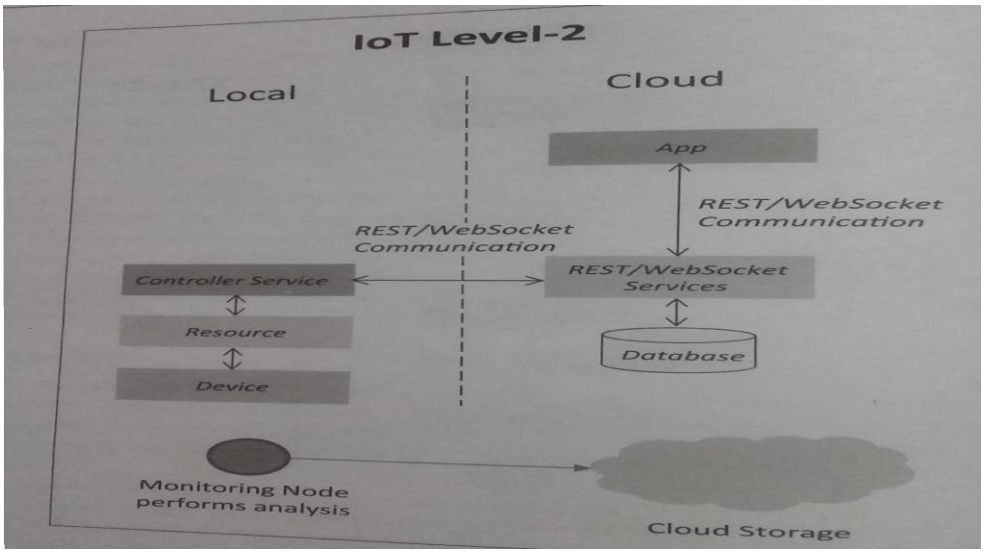
6) **Embedded Systems:** is a computer system that has computer hardware and software embedded to perform specific tasks. Embedded System range from low cost miniaturizeddevicessuchasdigitalwatchestodevicessuchasdigitalcameras,POSterminals ,vendingmachines, appliances etc.,

2.Explain in detail about the IoT Levels and Deployment Templates

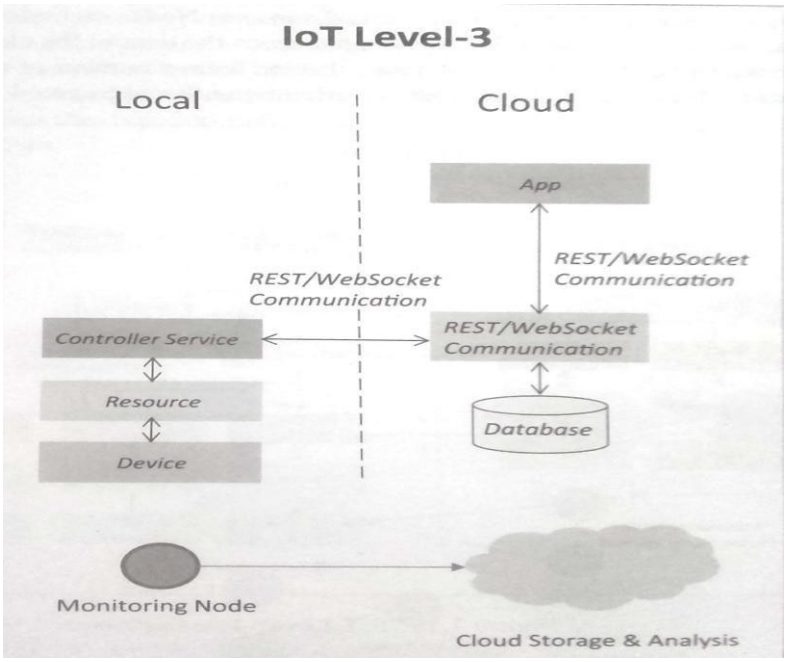
1) **IoT Level1:** System has a single node that performs sensing and/or actuation, stores data, performs analysis and host the application as shown in fig. Suitable for modeling lowcostandlowcomplexitysolutionswherethedatainvolvedisnotbigandanalysisrequirement arenotcomputationallyintensive.An e.g. of IoT Level1 is Home automation.



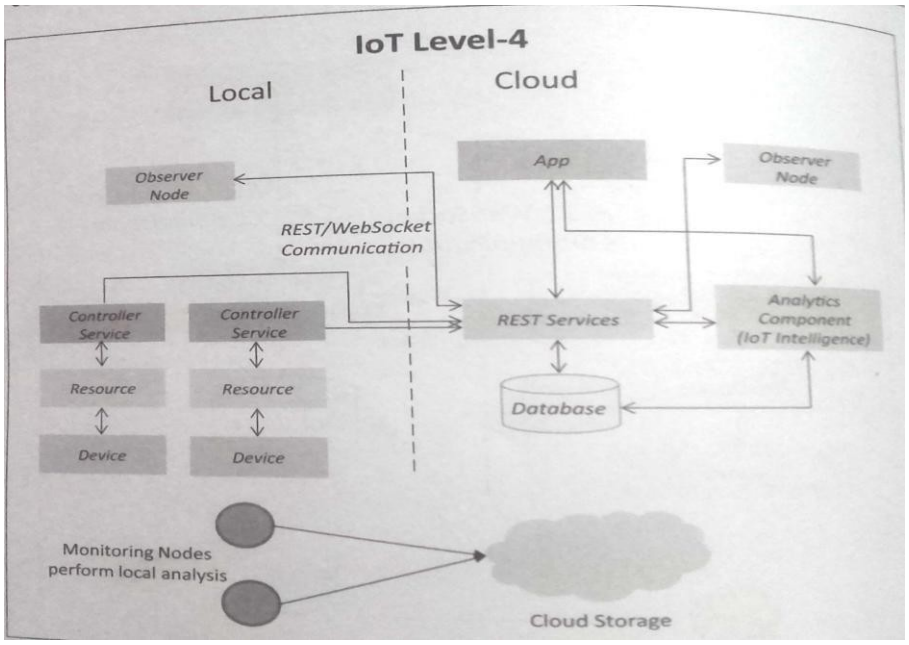
2) **IoT Level2:** It has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself. Ane,g.,ofLevel2IoT system for Smart Irrigation.



3) **IoTLevel3:** 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.

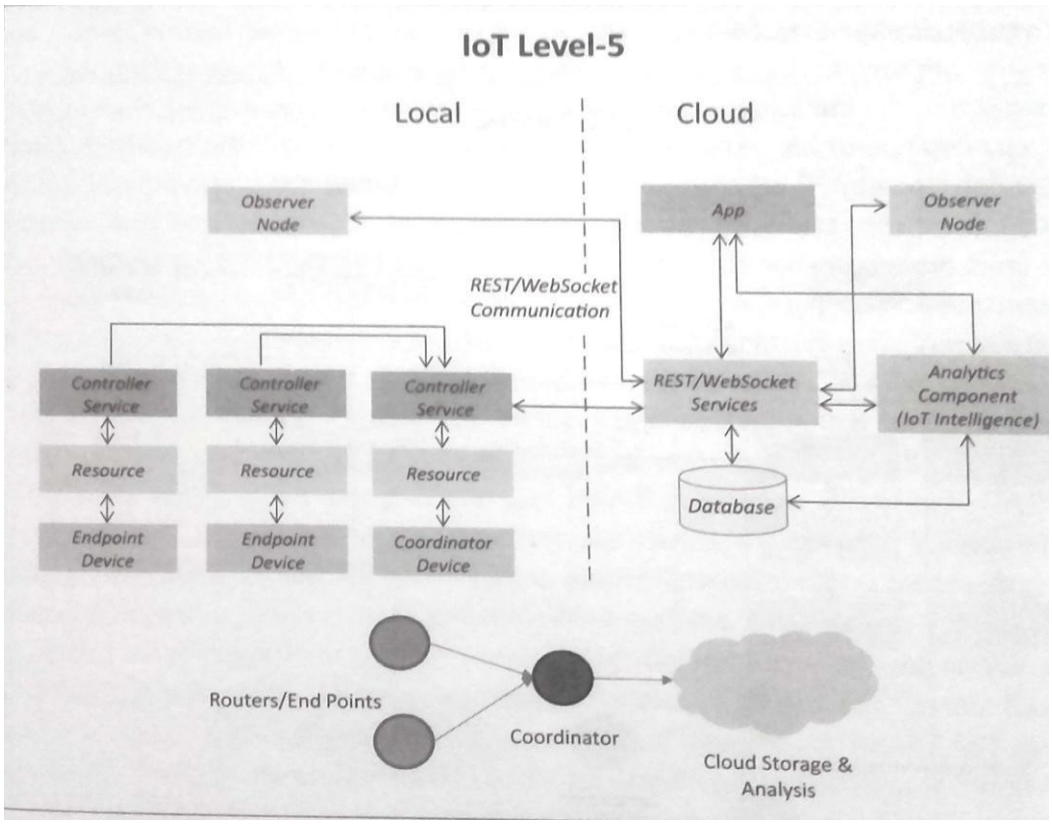


4) **IoT Level 4:** System has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud based as shown in fig. Level4 contains local and cloud based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices. An example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

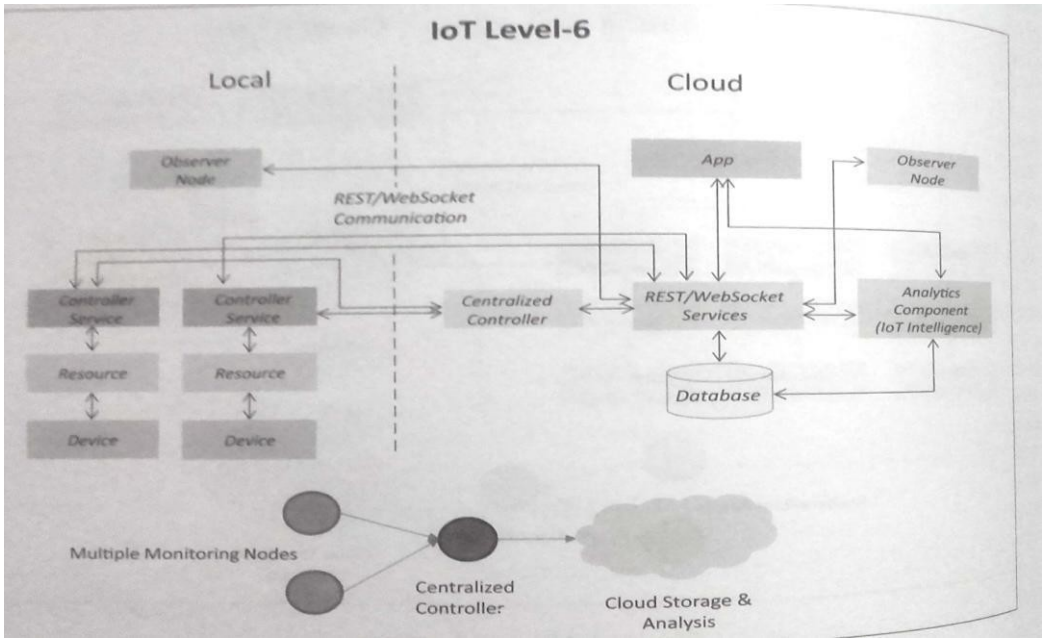


5) **IoT Level 5:** System has multiple end nodes and one coordinator node as shown in fig. The end nodes that perform sensing and/or actuation. Coordinator node collects data from the end nodes and sends to the cloud. Data is stored and analyzed in the cloud and

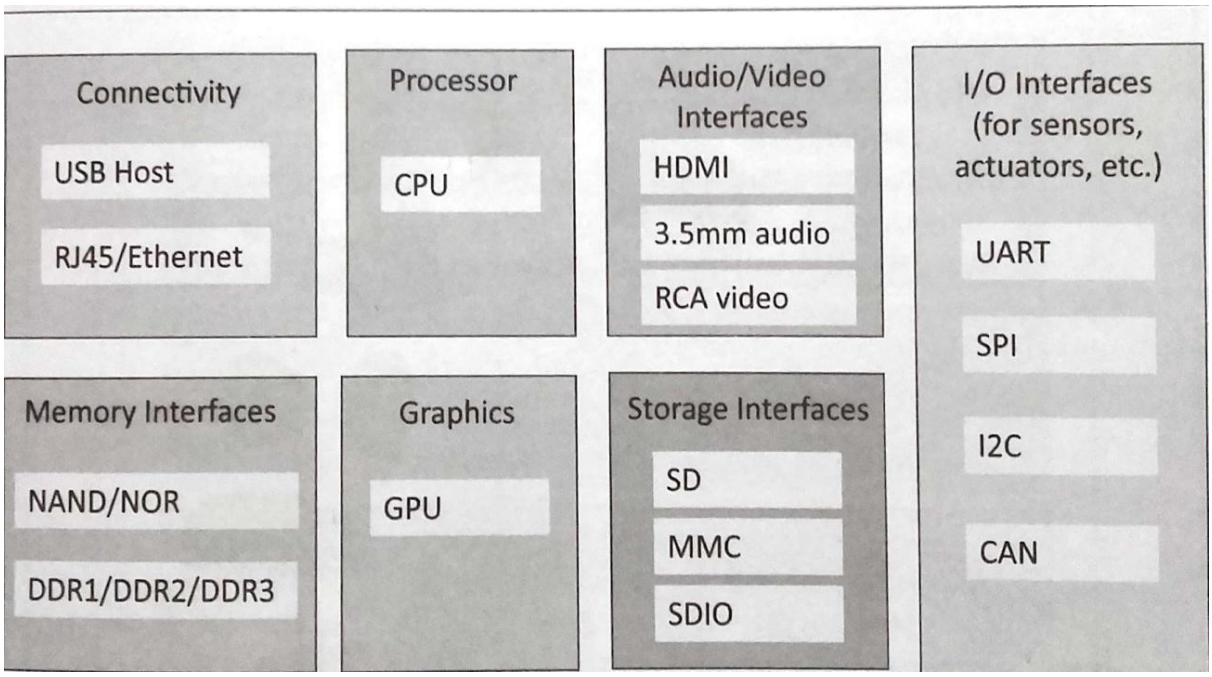
application is cloud based. Level5 IoT systems are suitable for solution based on wireless sensor network, In which data involved is big and analysis requirements are computationally intensive. An example of Level 5 system for Forest Fire Detection.



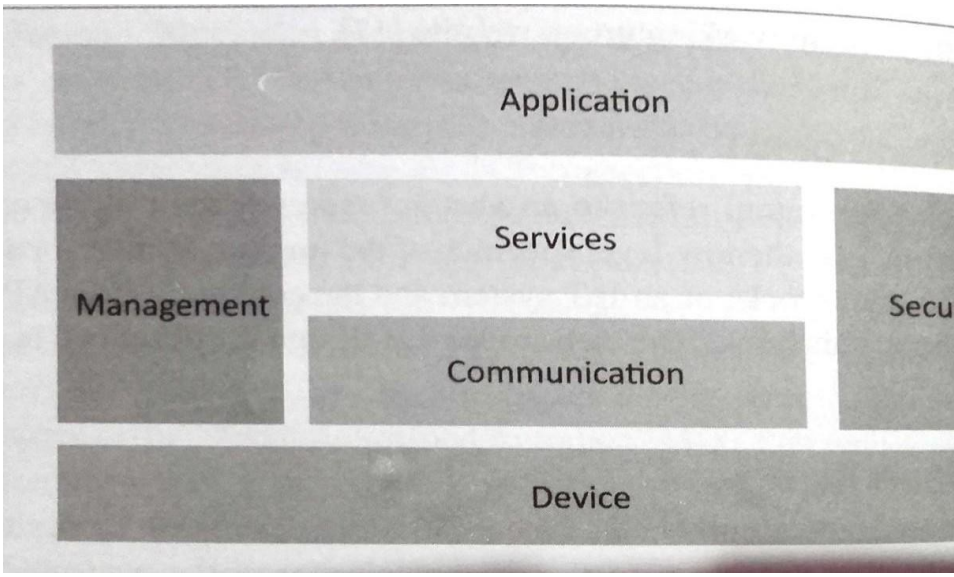
6) **IoT Level 6:** System has multiple independent end nodes that perform sensing and/or actuation and sensed data to the cloud. Data is stored in the cloud and application is cloud based as shown in fig. The analytics component analyses the data and stores the result in the cloud database. The results are visualized with cloud based application.Thecentralizedcontrollerisawareofthestatusofalltheendnodesandsendscontrolcommandstonodes.AnexampleofaLevel6IoTsystemforWeatherMonitoringSystem.



3.Explain in detail about the iot functional block diagram.



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, 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 a authentication ,authorization ,messageand context integrity and data security.
- **Application:** IoT application provide an interface that the users can use to control and monitor various aspects of IoT system.

4.Explain in detail about web 3.0 view with neat diagram.

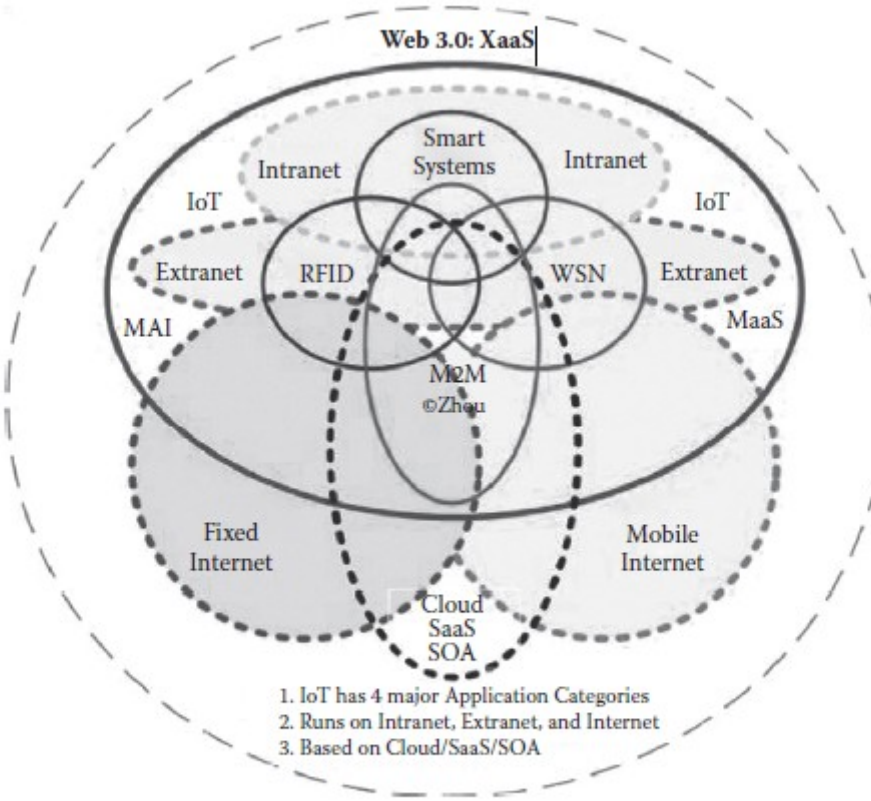


Figure 1.9 Web 3.0: The Internet of Things.

The Internet (network) and the web (application) are two sides of a coin. The Internet was invented by Vinton Cerf in 1973, and the invention of the web in 1989 was credited to Tim Berners-Lee and later caught worldwide attention by Marc Andreessen's Mosaic web browser in 1992. The Internet (hardware) is the infrastructure and the web (software) is the application everybody uses. Just like the Internet revolution, in the Internet of Things, web-based applications and software (the supporting data representation and middleware) are the keys.

McKinsey [36] summarized the key application functional- ities of IoT systems:

3. Information and analysis
   a. Tracking behavior

b. Enhanced situational awareness
c. Sensor-driven decision analytics

4. Automation and control
   a. Process optimization
   b. Optimized resource consumption
   c. Complex autonomous systems

According to Harbor Research, the web-based applications, systems, and networked services of smart systems or IoT are expanding more rapidly than the hardware and infrastructure [37]. This means the software (middleware and web-based integrated applications) market will play a pivotal role in the IoT business.

As is well known, Web 1.0 is about publishing and pushing content to the users. It's mostly a unidirectional flow of information. The shift from Web 1.0 to Web 2.0 can be seen as a result of technological refinements as well as the behavior change of those who use the World Wide Web, from publishing to participation, from web content as the outcome of large

up-front investment to an ongoing and interactive process. Web 2.0 is about two-way flow of information and is associ- ated with web applications that facilitate participatory infor- mation sharing, interoperability, user-centered design, and collaboration. Example applications of Web 2.0 include blogs, social networking services (SNSs), wikis, mashups, folkson- omies, video-sharing sites, massive multiplayer online role- playing games, virtual reality, and so on.

Enterprise 2.0 is the use of Web 2.0 technologies within an organization to enable or streamline business processes while enhancing collaboration (Figure 1.8). It is the extension of Web 2.0 into enterprise applications. IoT technologies and applications can be integrated into Enterprise 2.0 for enterprises that need to monitor and control equipment and facilities and integrate with their ERP and CRM back office systems.

Definitions of Web 3.0 vary greatly. Many believe that its most important features are Semantic Web and personaliza- tion; some argued that Web 3.0 is where the *computer* is gen- erating new information rather than the human.

The term Semantic Web was coined by Tim Berners-Lee, the inventor of the World Wide Web. He defines the Semantic Web as "a web of data that can be processed directly and indi- rectly by machines." Humans are capable of using the web to carry out tasks such as reserving a library book or searching

5.Explain in detail about the fog computing,edge computing,cloud computing.

However, this model also has limitations. As data volume, the variety of objects connecting to the network, and the need for more efficiency increase, new requirements appear, and those requirements tend to bring the need for data analysis closer to the IoT system. These new requirements include the following:

- **Minimizing latency:** Milliseconds matter for many types of industrial systems, such as when you are trying to prevent manufacturing line shutdowns or restore electrical service. Analyzing data close to the device that collected the data can make a difference between averting disaster and a cascading system failure.
- **Conserving network bandwidth:** Offshore oil rigs generate 500 GB of data weekly. Commercial jets generate 10 TB for every 30 minutes of flight. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud. Nor is it necessary because many critical analyses do not require cloud-scale processing and storage.
- **Increasing local efficiency:** Collecting and securing data across a wide geographic area with different environmental conditions may not be useful. The environmental conditions in one area will trigger a local response independent from the conditions of another site hundreds of miles away. Analyzing both areas in the same cloud system may not be necessary for immediate efficiency.

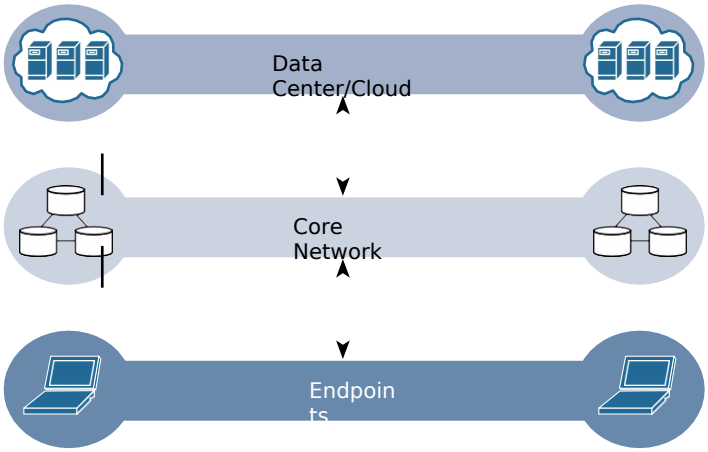
An important design consideration, therefore, is how to design an IoT network to manage this volume of data in an efficient way such that the data can be quickly analyzed and lead to business benefits. The volume of data generated by IoT devices can be so great that it can easily overrun the capabilities of the headend system in the data center or the cloud. For example, it has been observed that a moderately sized smart meter network of 1 million meters will generate close to 1 billion data points each day (including meter reads and other instrumentation data), resulting in 1 TB of data. For an IT organization that is not prepared to contend with this volume of data storage and real-time analysis, this creates a whole new challenge.

The volume of data also introduces questions about bandwidth management. As the massive amount of IoT data begins to funnel into the data center, does the network have the capacity to sustain this volume of traffic? Does the application server have the ability to ingest, store, and analyze the vast quantity of data that is coming in? This is sometimes referred to as the "impedance mismatch" of the data generated by the IoT system and the

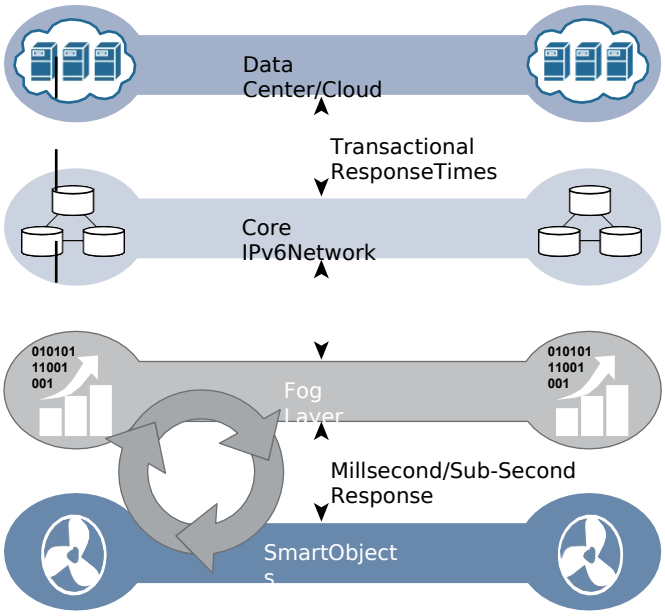
management application's ability to deal with that data.
As illustrated in Figure 2-14, data management in traditional IT systems is very simple. The endpoints (laptops, printers, IP phones, and so on) communicate over an IP core network to servers in the data center or cloud. Data is generally stored in the data center, and the physical links from access to core are typically high bandwidth, meaning access to IT data is quick.
millions of devices, available bandwidth may be on order of tens of Kbps per device or even less.
■ Latency can be very high. Instead of dealing with latency in the milliseconds range, large IoT networks often introduce latency of hundreds to thousands of milliseconds.
■ Network backhaul from the gateway can be unreliable and often depends on 3G/LTE or even satellite links. Backhaul links can also be expensive if a per-byte data usage model is necessary.
■ The volume of data transmitted over the backhaul can be high, and much of the data may not really be that interesting (such as simple polling messages).
■ Big data is getting bigger. The concept of storing and analyzing all sensor data in the cloud is impractical. The sheer volume of data generated makes real-time analysis and response to the data almost impossible.

Fog Computing

The solution to the challenges mentioned in the previous section is to distribute data management throughout the IoT system, as close to the edge of the IP network as possible. The best-known embodiment of edge services in IoT is fog computing. Any device



with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and IoT gateways. Analyzing IoT data close to where it is collected minimizes latency, offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the local network.



6. A Panoramic View of IoT Applications

In 1874, French engineers built a system of weather and snow-depth sensors on Mont Blanc that transmitted real-time information to Paris. Telecommand and telematics (telecommunication+informatics) were more related to telemetry in earlier times. However, telematics nowadays often refers to vehicle tracking, especially passenger car tracking and global positioning system (GPS) services.

Most recently, the IoT is increasingly finding its way into mainstream news. Executives of large companies and even government officials, such as President Obama and the Chinese premier, are speaking about the possibilities and opportunities of having ubiquitous sensors connected to the Internet.

"The next big revolution that will happen is the Internet of Things," said Cisco chief technology officer Padma Warrior. Although the widespread adoption of IoT will take time, the timeline is advancing thanks to improvements in underlying technologies. Advances in networking technologies and the standardization [31] of communication protocols, XML-based data representations, and middleware architectures make it possible to collect data from sensors and devices almost anywhere at anytime. Ever-smaller silicon chips are gaining new capabilities, while costs are falling. Massive increases in storage and computing power, available via cloud comput-ing, make number crunching possible at a very large scale and at declining cost. It's easy to speculate on possibilities:

- Radio-frequency identification (RFID) tags that know where your luggage is
- Mesh networks of sensors that can more reliably monitor the changing concentrations of volcanic ash
- Heating, ventilating, and air-conditioning (HVAC) units that can coordinate to act in concert, rather than independently
- Smart sticking plasters that detect microscopic changes in skin condition or blood flow
- An in-vehicle terminal or called an edge device that can detect if you are too sleepy to drive safely
- Surveillance systems that can analyze what they are film-ing, being alert for security abnormalities
- Smart glasses for the visually impaired that can interpret what you're looking at
- A toothbrush that can let you know if you're not putting enough effort into cleaning the inner sides of your lower right molars
- And all of these devices connected together…

The arrival of the IoT concept and its worldwide attention is closely relevant to environmental, societal, and economic challenges such as climate change, environment protection, energy saving, and globalization. For these reasons the IoT is increasingly used in a large number of sectors. Key sectors in this context are transportation, healthcare, energy and environment, safety and security, logistics, and manufacturing. M2M and embedded mobile devices are sending mobile data to servers that are increasingly useful and valuable to ERPs [34].

Harbor Research segments the IoT/M2M market into 10 key sectors [32], 30+ subsectors, and countless systems and devices:

- Buildings: Institutional/Commercial/Industrial/Home. HVAC, fire and safety, security, elevators, access control systems, lighting
- Energy and Power: Supply/Alternatives/Demand. Turbines, generators, meters, substations, switches
- Industrial: Process Industries/Forming/Converting/Discrete Assembly/Distribution/Supply Chain. Pumps, valves, vessels, tanks, automation and control equipment, capital equipment, pipelines
- Healthcare: Care/Personal/Research. Medical devices, imaging, diagnostics, monitor, surgical equipment

- Retail:Stores/Hospitality/Services.Point-ofsaleterminals,vendingmachines,RFIDtags,scannersandregisters,lightingandrefrigerationsystems
- Security and Infrastructure: Homeland Security/EmergencyServices/NationalandRegionalDefense.GPSsystems,radarsystems,environmentalsensors,vehicles,weaponry,fencing
- Transportation: On-Road Vehicles/Off-Road Vehicles/Nonvehicular/TransportInfrastructure.Commercialvehicles,airplanes,trains,ships,signage, tolls,RFtags,parkingmeters,surveillancecameras,trackingsystems
- InformationTechnologyandNetworkInfrastructure:Enterprise/ DataCenters.Switches,servers,storage
- Resources: Agriculture/Mining/Oil/Gas/Water. Mining equipment,drillingequipment,pipelines,agriculturalequipment
- Consumer/Professional: Appliances/White Goods/OfficeEquipment/HomeElectronics.M2Mdevices,gadgets,smartphones,tabletPCs,homegateways

MachinaResearchclassifiedtheIoT/M2Mmarketinto3cat-egoriesand11segments[35]:

- IntelligentEnvironment:Intelligentbuildings/smartcitiesandtransportation
- IntelligentLiving:Automotive/consumerelectronics
- IntelligentEnterprise:Health/utilities/manufacturing/ retailandleisure/construction/agricultureandextraction/emergencyservicesandnationalsecurity

PertheIoTdefinitionofthepreviouschapter,thegoalofIoTistoachievepervasiveM2Mconnectivityandgrandintegrationandtoprovidesecure,fast,andpersonalizedfunctionalitiesandservicessuchasmonitoring,sensing,tracking,locating, alerting, scheduling, controlling, protecting, logging,auditing,planning,maintenance,upgrading,datamining,trending,reporting,decisionsupport,dashboard,back officeapplications,andothers.ThosefunctionalitiesarecommonfeaturesofIoTsystemssupportedbyacommonthree-tierIoTsystemarchitecturethatwillbedescribedinthelatterpartofthebook

Beecham Research tracks nine key industries and theirassociateddevicesusingallprincipletechnologiesforconnect-ingthem[33].Suchdevicesrangefromair-conditioning,accesscontrol,andliftsandescalatorsinthebuildingssectortowindturbines,utilitymeters,andpipelinesintheenergy/powersec-tor and to closed-circuit television and lone worker solutionsin the security/environment sector; from magnetic resonanceimaging(MRI)scanners,x-raymachines,andbloodanalyzersin the healthcare/life sciences sector to telematics systems forcars, trucks, containers, and off-road vehicles and road tollschemesinthetransportationsector.

panoramicviewoftheIoTapplicationsisshowninFigure2.1basedon

describedindustrycategoriesandsegments.Thefirstringisthesectors,thesecondringisapplicationgroups,thethird ringistargetobjectsorsites,andthefourthringisdevicesused.

AsweseefromthepreviousparagraphsthetermInternetofThingsissometimesusedinterchangeablywithM2M bysomemarketresearchfirms.M2Mcanberegardedasone ofthefoursectorsundertheIoTumbrella;theotheronesinclude RFID, wireless sensor networks (WSN), and SCADA(or called smart systems, industry automation, etc.). Currently,eventhoughalmosteveryonebelievesthattheIoTmarket isahugemarket,fewresearchreportsaboutthesizeoftheentireIoTmarketasdefinedinthelastchapterhavebeenproducedbymarketresearchfirms.

Someresearchfirmshavereportsontwoorthreeofthefour IoTsectors,butnotallofthefoursectors.Forexample, HarborResearchforecaststhatthesmartsystems[186]andM2Mmarketvaluewillbe€280billionin2013.

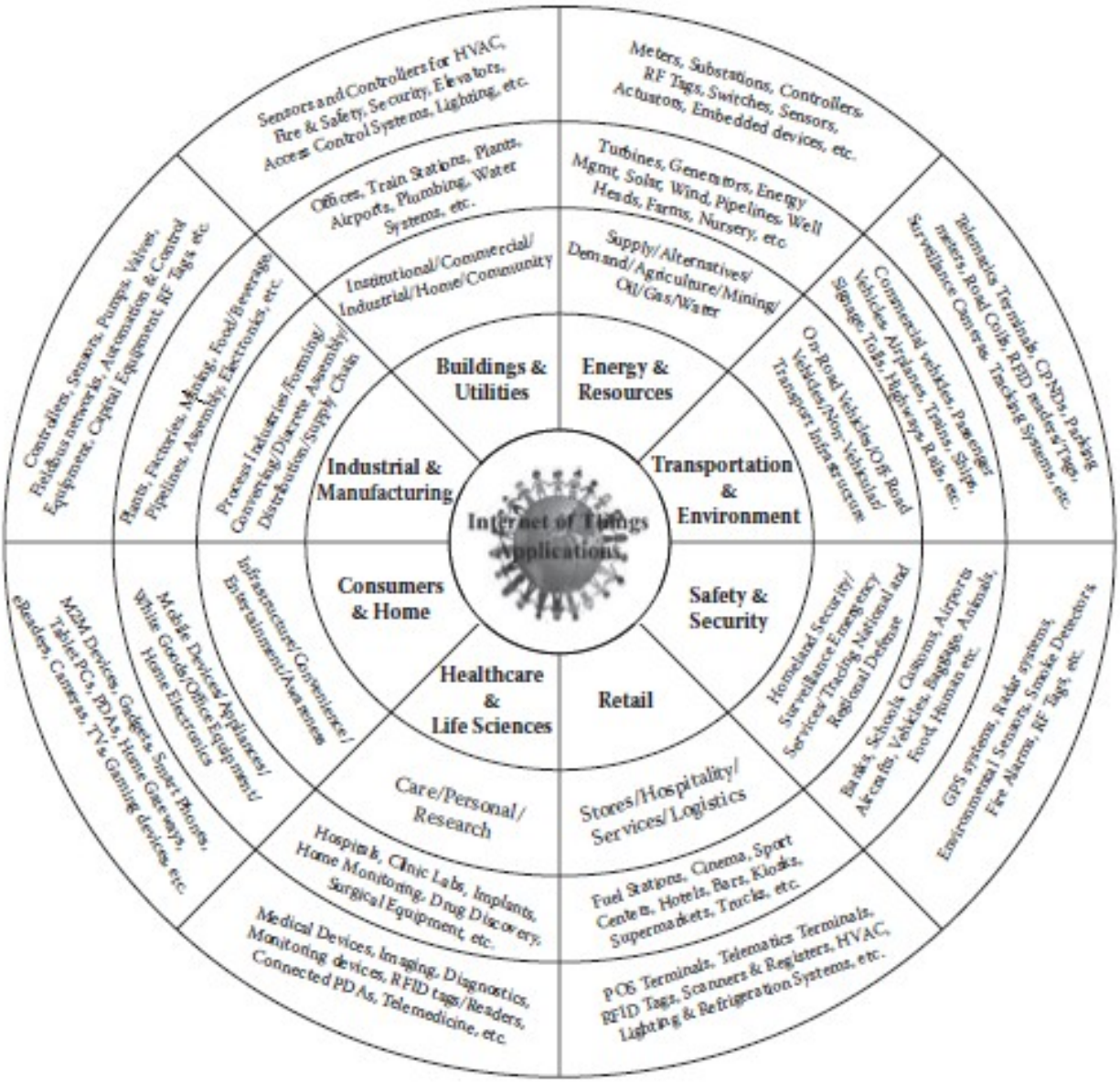


Figure 2.1 A panoramic view of IoT applications.

6.Explain in detail about the connecting devices.

IoT devices and sensors must be connected to the network for their data to be utilized. In addition to the wide range of sensors, actuators, and smart objects that make up IoT, there are also a number of different protocols used to connect them. This chapter takes a look at the characteristics and communications criteria that are important for the **technologies** that smart objects employ for their connectivity, along with a deeper dive into some of the major technologies being deployed today.

Two main sections divide this chapter. The first main section, "Communications Criteria," describes the characteristics and attributes you should consider when selecting and dealing with connecting smart objects. The various technologies used for connecting sensors can differ greatly depending on the criteria used to analyze them. The following subsections look closely at these criteria:

- **Range:** This section examines the importance of signal propagation and distance.
- **Frequency Bands:** This section describes licensed and unlicensed spectrum, including sub-GHz frequencies.
- **Power Consumption:** This section discusses the considerations required for devices connected to a stable power source compared to those that are battery powered.
- **Topology:** This section highlights the various layouts that may be supported for connecting multiple smart objects.

■ **Constrained Devices:** This section details the limitations of certain smart objects from a connectivity perspective.
■ **Constrained-Node Networks:** This section highlights the challenges that are often encountered with networks connecting smart objects.
The second main section of this chapter, "IoT Access Technologies," provides an in-depth look at some of the technologies that are considered when connecting smart objects.
IEEE 802.15.4: This section highlights IEEE 802.15.4, an older but foundational wireless protocol for connecting smart objects.
■ **IEEE 802.15.4g and IEEE 802.15.4e:** This section discusses improvements to 802.15.4 that are targeted to utilities and smart cities deployments.
■ **IEEE 1901.2a:** This section discusses IEEE 1901.2a, which is a technology for connecting smart objects over power lines.
■ **IEEE 802.11ah:** This section discusses IEEE 802.11ah, a technology built on the well-known 802.11 Wi-Fi standards that is specifically for smart objects.
■ **LoRaWAN:** This section discusses LoRaWAN, a scalable technology designed for longer distances with low power requirements in the unlicensed spectrum.
■ **NB-IoT and Other LTE Variations:** This section discusses NB-IoT and other LTE variations, which are often the choice of mobile service providers looking to connect smart objects over longer distances in the licensed spectrum.