Fundamental ofIoT

*Syllabus*

*EvolutionofInternetofThings-EnablingTechnologies-IoTArchitectures:oneM2M,IoTWorld Forum(IoTWF)andAlternativeIoTmodels–SimplifiedIoTArchitectureandCoreIoTFunctional Stack-Fog,EdgeandCloudinIoT-FunctionalblocksofanIoTecosystem-Sensors,Actuators, Smart Objects and Connecting SmartObjects*

***Contents***

* 1. *Evolution of Internet ofThings*
  2. *EnablingTechnologies*
  3. *loTArchitecture*
  4. *Fog, Edge and Cloud inloT*
  5. *M2M*
  6. *Functional Blocks of an IoTEcosystem*
  7. *Sensors*
  8. *Actuators*
  9. *SmadObjects*



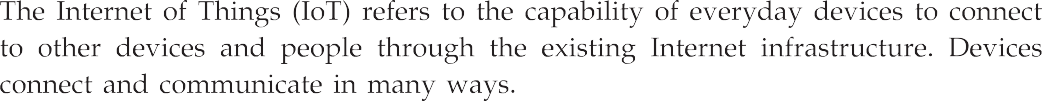
UNIT - I

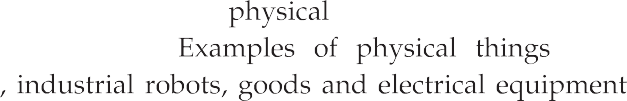
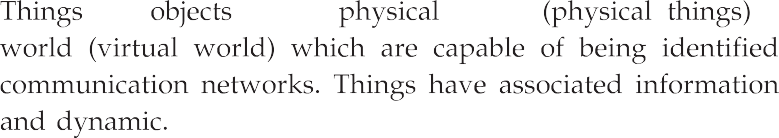












**Business and societal impact**

**Connectivity**

(Digitize access)

Email

Web browser

**Networked economy**

(Digitize business)

E - commerce

Digital supply chain

**Immersive experiences**

(Digitize interaction)

Social Mobility

Cloud

**Internet of things**

(Digitize the world)

Connecting: People Process Data Things

**Intelligent connection**

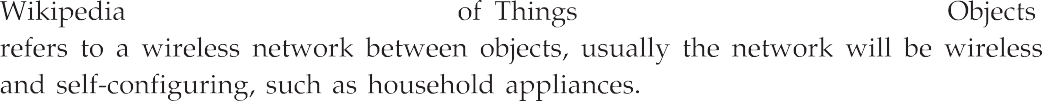
















|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Anytime any context |  |  | Transportation |  |
| Anything any device | Internet of Things | Anyone anybody | Healthcare and hospitals | Internet of Things | Robots and drones |
| Any place anywhere |  | Any service any business | Connected home and offices |  | Smart phones |
|  | Any path any network |  |  |  |  |

#### Devices connect and communicate in many ways. Examples of this are smart phones that interact with other smart phones, vehicle-to-vehicle communication, connected video cameras, and connected medical devices. They are able to communicate with consumers, collect and transmit data to companies, and compile large amounts of data for thirdparties.

* IoT data differs from traditional computing. The data can be small in size and frequent in transmission. The number of devices, or nodes, that are connecting to the network are also greater in IoT than in traditional PCcomputing.
* Machine-to-Machine communications and intelligence drawn from the devices and the network will allow businesses to automate certain basic tasks without dependingoncentralorcloudbasedapplicationsandservices.
* IoT impacts every business. Mobile and the Internet of Things will change the types of devices that connect into a company's systems. These newly connected devices will produce new types ofdata.
* The Internet of Things will help a business gain efficiency, harness intelligence from a wide range of equipment, improve operations and increase customer satisfaction.
* Ubiquitous computing, pervasive computing, Internet Protocol, sensing technologies, communication technologies, and embedded devices are merged together in order to form a system where the real and digital worlds meet and are continuously in symbioticinteraction.
* The smart object is the building block of theIoT vision. By putting intelligence into everyday objects, they are turned into smart objects able not only to collect information from the environment and interact /control the physical world, but also to be interconnected, to each other, through Internet to exchange data and information.
* The expected huge number of interconnected devices and the significant amount of available data open new opportunities to create services that will bring tangible benefits to the society, environment, economy and individualcitizens.
* However, the IoT is still maturing, in particular due to a number of factors, which limit the full exploitation of the IoT. Some of the factors are listed below:

1. Thereisnouniqueidentificationnumbersystemforobjectintheworld.
2. IoT uses Architecture Reference Model (ARM) but there is no further development inARM.

issing large-scale testing and learning environments

1. Difficulties in exchangingof sensor information in heterogeneous environments.
2. Difficulties in developing business which embraces the full support of the Internet ofThings.

IoT Characteristics

1. Interconnectivity : Everything can be connected to the global information and communicationinfrastructure.
2. Heterogeneity : Devices within IoT have different hardware and use different but they can still interact with other devices through differentnetworks.
3. services : Provides things-related services within the constraints of things, such as privacy and semantic consistency between physical and virtual thing.
4. Dynamic changes: The state of a device can change dynamically, thus the number of devices canvary.
5. Integrated into information network: IoT devices are integrated with information network for communication purpose. It will exchange data with otherdevices.
6. Self-adapting: Self-Adaptive is a system that can automatically modify itself in the face of a changing context, to best answer a set ofrequirements.
7. Self-configuration primarily consists of the actions of neighbour and service discovery, network organization, and resourceprovisioning.

## Component of IoT

* The hardware utilized in IoT systems includes devices for a remote dashboard, devices for control, servers, a routing or bridge device, and sensors. These devices manage key tasks and functions such as system activation, action specifications,

and detection to support-specific goals and actions.

* of IoT devices are as follows:

1. Control units : A small computer on a single integrated circuit containing processor core, memory and a programmable I/O peripheral. It is responsible for the mainoperation.
2. Sensor : Devices that can measure a physical quantity and convert it into a signal, which can be read and interpreted by the microcontroller unit. These devices consist of energy modules, power management modules, RF modules, and sensing modules. Most sensors fall into 2 categories : Digital or analog. An analog data is converted to digital value that can be transmitted to theInternet.

### Temperature sensors :accelerometers

#### Image sensors :gyroscopes

* 1. Light sensors : acousticsensors
  2. Micro flow sensors : humiditysensors
  3. Gas RFID sensors : pressure sensors

1. Communication modules : These are the part of devices and responsible for communication with rest of IoT platform. They provide connectivity according to wireless or wired communication protocol they are designed. The communication between IoT devices and the Internet is performed in twoways:
2. There is an Internet-enable intermediate node acting as agateway;
3. The IoT Device has direct communication with theInternet.

* The communication between the main control unit and the communication module uses serial protocol in mostcases.

1. Power Sources : In small devices the current is usually produced by sources like batteries, thermocouples and solar cells. Mobile devices are mostly powered by lightweight batteries that can be recharged for longer lifeduration.

* Communication Technology and Protocol :IoT primarily exploits standard protocols and networking technologies. However, the major enabling technologies and protocols of IoT are RFID, NFC, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A, and WiFi-Direct. These technologies support the specific networking functionality needed in an IoT system in contrast to a standard uniform network of commonsystems.

## Working of IoT

#### Fig 1.1.2 shows working ofIoT.

1. Collect and transmit data : The device can sense the environment and collect information related to it and transmit it to a different device or to theInternet.
2. based on triggers : It can be programmed to actuate other devices based on conditions set byuser.

#### Receive information : Device can also receive information from thenetwork.

1. Communication assistance : It provides communication between two devices of same network or differentnetwork.



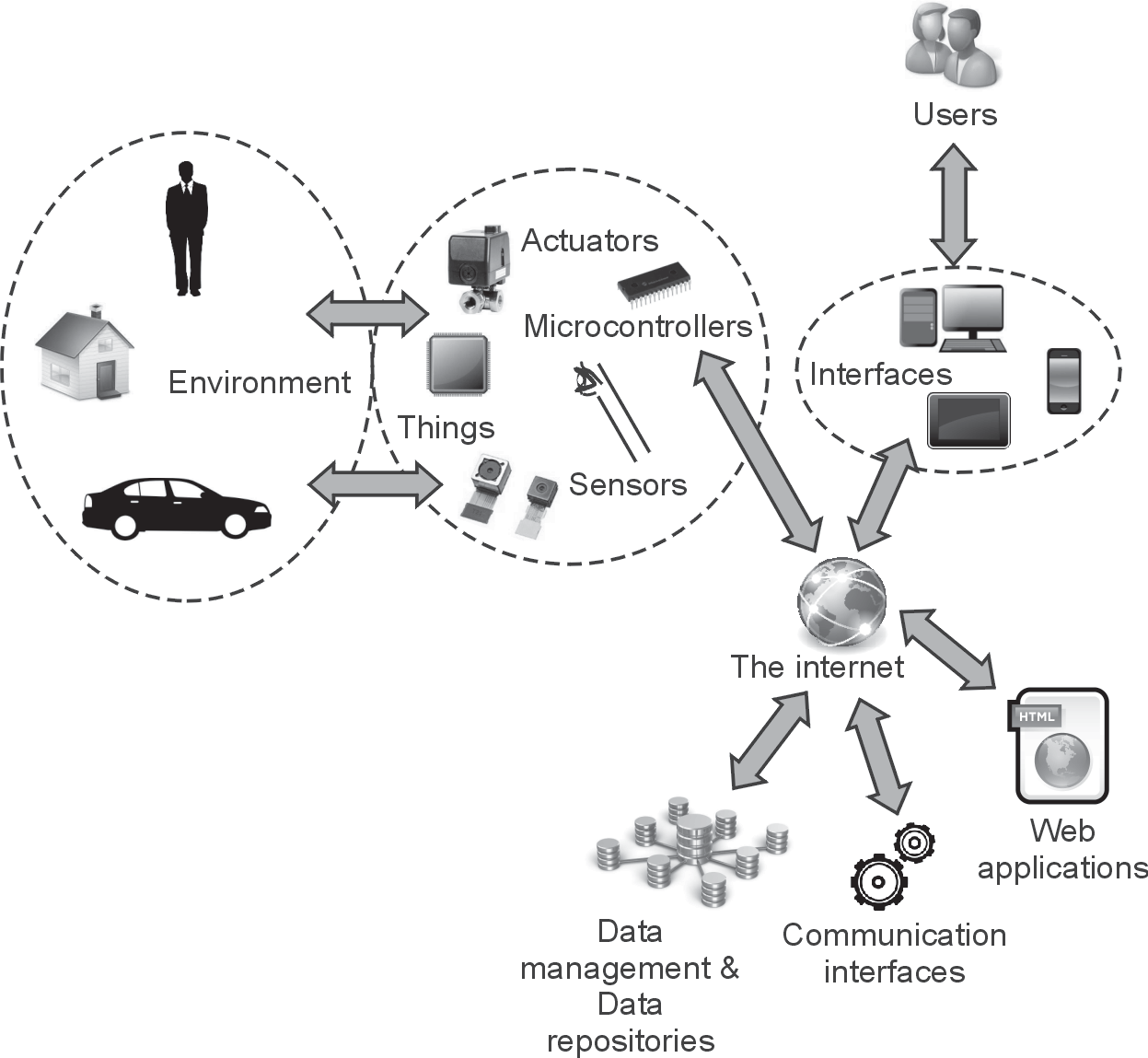


Fig. 1.1.2 : Working of IoT

#### Sensors for various applications are used in different IoT devices as per different applicationssuchastemperature,power,humidity,proximity,forceetc.

* Gateway takes care of various wireless standard interfaces and hence one gateway can handle multiple technologies and multiplesensors.
* The typical wireless technologies used widely are 6LoWPAN, Zigbee, Zwave, RFID, NFC etc. Gateway interfaces with cloud using backbone wireless or wired technologies such as WiFi, Mobile , DSL orFibre.

#### Advantages and Disadvantages

Advantages of loT

#### Improved customer engagement andcommunication.

1. Support for technologyoptimization
2. range of datacollection
3. Reducedwaste

Disadvantages of loT

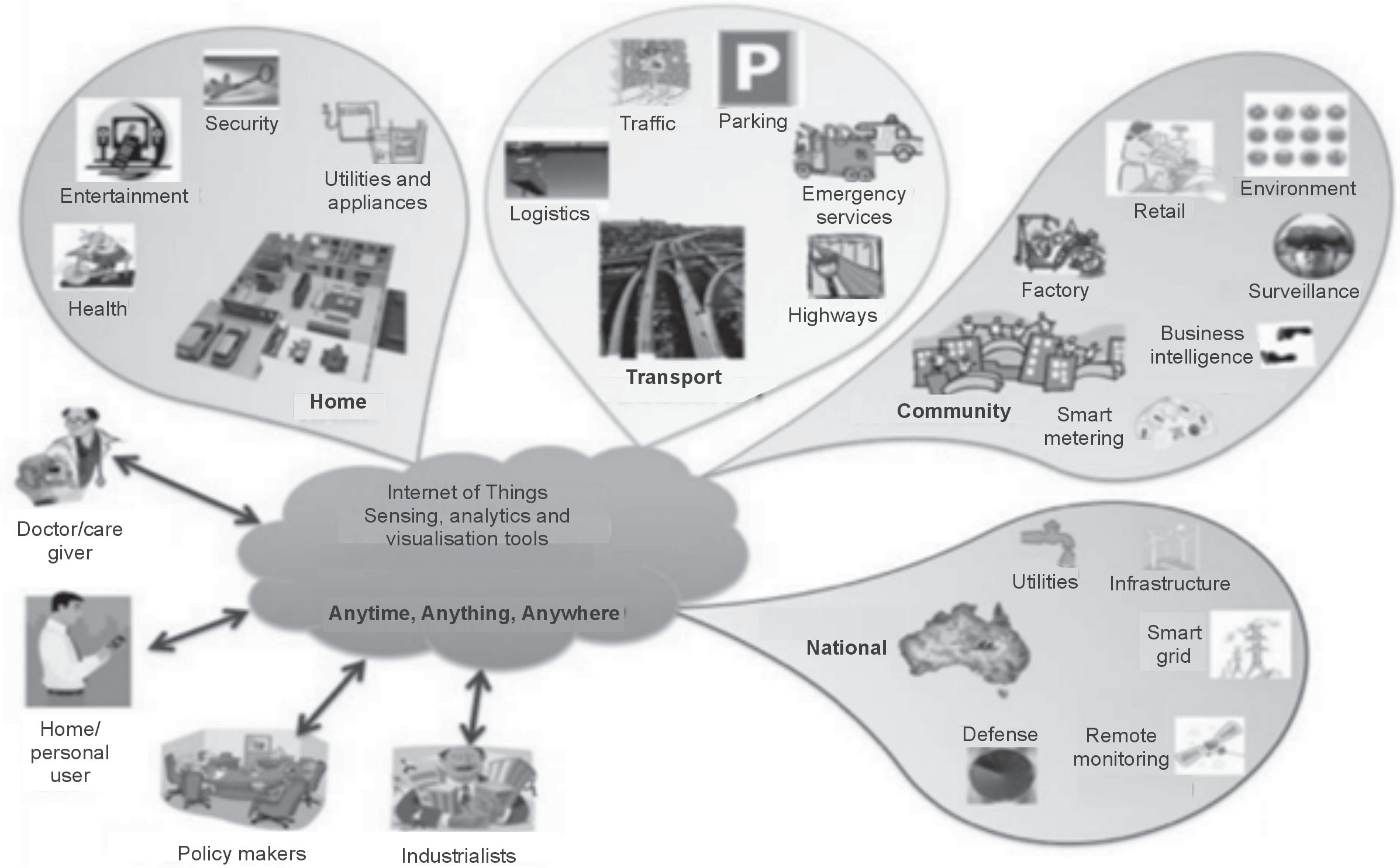
1. Loss of privacy and security : As all the household appliances, industrial machinery, public sector services like water supply and transport, and many other devices all are connected to the Internet, a lot of information is available on it. This information is prone to attack byhackers.

2 Flexibility : Many are concerned about the flexibility of an IoT system to integrate easily withanother

1. Complexity : The IoT is a diverse and complex network. Any failure or bugs in the software or hardware will have serious consequences. Even power failure can cause a lot ofinconvenience.
2. Compatibility : Currently, there is no international standard of compatibility for the tagging and monitoringequipment
3. Save time andmoney.

1.1.6Applications of IoT

1. Home : Buildings where people live. It controls home and securitysystems.
2. Offices : Energy management and security in office buildings; improved for mobileemployees.
3. Factories : Places with repetitive work routines, including hospitals and farms; operating efficiencies, optimizing equipment use andinventory.
4. Vehicles : Vehicles including cars, trucks, ships, aircraft, and trains; condition-based maintenance, usage-based design, pre-salesanalytics
5. Cities : Public spaces and infrastructure in urban settings; adaptive traffic control, smart meters, environmental monitoring, resourcemanagement.
6. Worksites : It is custom production environments like mining, oi1 and gas, construction; operating efficiencies, predictive maintenance, health andsafety.



#### Enabling Technologies

Fig. 1.1.3

#### 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

Search engines.

Computing

* Cloud computing has the almost unlimited capacity of storage and processing power which is a more mature technology at least to a certain extent to solve the problem of most of the Internet ofthings.
* is a pay-per-use model for enabling available, convenient, network access to a shared pool of configurable computingresources

(e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction.

#### Cloud storage services may be accessed through a web service API, a cloud storage gateway or through a web-based userinterface.

* Cloud computing services are offered to users in different forms : Infrastructure- as- a- Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service(SaaS).

#### oftware as a Service (SaaS) : Model in which an application is hosted as a service to customers who access it via the Internet. The provider does all the patching and upgrades as well as keeping the infrastructure running. The traditional model of software distribution, in which software is purchased for and installed on personal computers.

* Platform as a Service (PaaS) : Platform as a service is another application delivery model and also known as cloud-ware. Supplies all the resources required to build applications and services completely from the Internet, without having to download or install software. Services includes application design, development, testing, deployment, and hosting, team collaboration, web service integration, database integration, security, scalability, storage, state management, and versioning. PaaS is closely related to SaaS but delivers a platform from which to work rather than an application to workwith.
* Infrastructure as a Service (IaaS) :SaaS and PaaS are providing apples to customers, IaaS doesn't. It offers the hardware so that your organization can put whatever they want onto it. Rather than purchase servers, software, racks, and having to pay for the datacenter space for them, the service provider rents for resources like server space, network equipment, memoryetc.

Big Data Analytic

* A category of technologies and services where I e capabilities provided to collect, store, search, share, analyze and visualize data which have the characteristics of high-volume, high-velocity andhigh-variety.
* of big data generated by IoT systems:
  1. Weather MonitoringStations
  2. Machine sensor data from industrialsystems
  3. Health and fitnessdata
  4. Location and trackingsystems

Data collection

Data Data Dataprocessing analysis execution

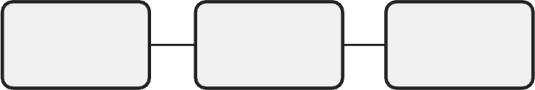
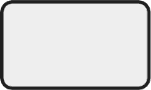


Fig. 1.2.1





#### A Wireless Sensor Network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure,etc.

* usually include sensor nodes, actuator nodes, gateways and large number of sensor nodes deployed randomly inside ofor near the

monitoring area, form networks through self-organization.

* Sensor nodes monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multi-hop routing, and finally reach the management node through the internet orsatellite.
* Standards for WSN technology have been well developed, such as Zigbee (IEEE 802.15.4). The IEEE 802.15.4 is simple packet data protocol for lightweight wireless networks.
* It works well for long battery life, selectable latency for controllers, sensors, remote monitoring and portableelectronics.

Communication Protocols

Communication protocols are used as a backbone of IoT systems. It enable network connectivity and coupling to applications. Communication protocols allow devices to exchange data over thenetwork.

* protocol also performs error correction and detection, flow control, data addressing mechanismetc.
* Sequence control, lost of packet, retransmission are the other functions of communicationprotocol.

Embedded System

* A system s a set of interacting or interdependent component parts forming a complex unit. It is a fixed plan to perform one or manytask.
* Embedded system is an electronic system which is designed to perform one or a of functions using software andhardware.
* General definition of embedded systems is : embedded systems are computing systems with tightly coupled hardware and software integration that are designed to perform a dedicated function. The word embedded reflects the fact that these systems are usually an integral part of a larger system, known as the embedding system. Multiple embedded systemscan coexist in an embedding system.





Automotive Home Energy application applicationapplication

Common service layer



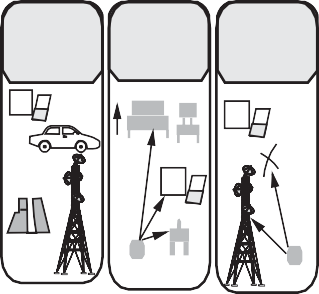












Automotive Home applicationapplication

Energy application

X

X

|  |  |  |
| --- | --- | --- |
| Communication technologies and protocols | | |
| Co | mmunicationnetworks |  |
|  | Communication devices and hardware |



$

















**Center**

IT Query based

OT Event based

**Edge**

Data at rest

Data in motion



|  |
| --- |
| 7 **Collaboration andprocesses**  (Involving people and business processes) |
| 6 **Application**  (Reporting, Analytics, Control) |
| 5 **Dataabstraction**  (Aggregation and access) |
| 4  **Data accumulation**  (Storage) |
| 3 **Edge (Fog)computing**  (Dataelementanalysisandtransformation) |
| 2 **Connectivity**  (Communication and processing units) |
| 1 **Physical devices and controllers**  (Sensors, Devices, Machines,  Intelligent edge nodes of all types) |

Non -real time

Real time











*InternetofThings 1-14 Fundamental ofloT*

oT reference model define a set of levels with control flowing from center to the edge which includes sensors, device, machines and other type of an intelligent nodes.

* Layer 1 : Comprises physical devices and controllers that might control multiple devices. This level enables devices to communicate with one another and to communicate, via the upper logical levels, with application platforms such as computers, remote-control devices, andsmart-phones.
* Layer 2 : The IWF model includes gateways in level 2. Because the gateway is a networking and connectivity device, its placement at level 2 seems to make more sense.
* Layer 3 : It performs data element analysis andtransformation.
* Layer 4 : The data accumulation level, is where data coming from the numerous devices, and filtered and processed by the edge computing level, is placed in storage that will be accessible by higher levels. This level marks a clear distinction in the design issues, requirements, and method of processing between lower-level (fog) computing and upper-level (typically cloud)computing.
* Layer 5, Data abstraction layer : Reconciles multiple data formats and ensures consistent semantics from various sources. Confirms that data set is complete and consolidates data into one place or multiple data storesusing virtualization.
* Layer 6, Application layer : Interprets data using software applications. Applications may monitor, control and provide reports based on the analysis of thedata.
* Layer 7, Collaboration and processes layer : Consumes and shares the application information.
* Using this reference model, following things are achieved:

1. Decompose the problem into smallerparts.
2. Identify different technologies at eachlayer.
3. Define a system in which different parts can be provided by differentvendors.
4. Have a process are defining interface that leads tointeroperability.
5. Define a tiered security model that is enforced at one transition points between levels.

Characteristics of loTWF model

° Simplifies : It helps break down complex systems so that each part is more understandable.

° Clarifies : It provides additional information to precisely identify levels of the IoT and to establish commonterminology.











Core IoT functional stack

IoT data management and compute



Security

Edge

Fog

Cloud

Sensors and actuators

Communication

Applications















oreloT functional stack group

* The IoT gateway acts as the aggregation point for a group of sensors and actuators to coordinate the connectivity of these devices to each other and to an externalnetwork.
* An IoT gateway can be a physical piece of hardware or functionality that is incorporated into a larger "Thing" that is connected to thenetwork.
* For example, an industrial machine might act like a gateway, and so might a connected automobile or a home automationappliance.
* An IoT gateway will often offer processing of the data "at the edge" and storage capabilities to deal with network latency andreliability.
* For device to device connectivity, an IoT gateway deals with the interoperability issues between incompatibledevices.
* A typical IoT architecture would have many IoT gateways supporting masses of devices.

## Fog, Edge and Cloud in IoT

* Edge computing : it is also known as just "edge". It brings processing close to the data source, and it does not need to be sent to a remote cloud or other centralized systems for processing. Also called as "mist"computing.
* By the distance and time it takes to send data to centralized sources, we improve the speed and performance of data transport, as well as devices and applications on theedge.
* Fog computing is a standard that defines how edge computing should work, and it facilitates the operation of compute, storage and networking services between end devices and cloud computing datacentres.
* Examples : industrial controllers, switches, routers, embedded servers, and IoT gateways.

Fog nodes :

1. ReceivefeedsfromIoTdevicesusinganyprotocol,inrealtime.
2. Run IoT-enabled applications for real-time control and analytics, with millisecond responsetime.
3. Provide transient storage, often 1-2hours.
4. Send periodic data summaries to thecloud.

* Additionally, many use fog as a jumping-off point for edgecomputing.
* With edge, compute and storage systems reside at the edge as well, as close as possible to the component, device, application or human that produces the data beingprocessed.

e purpose is to remove processing latency, because the data needn't be sent from the edge of the network to a central processing system, then back to the edge.

* The applications for edge make sense: Internet of Things-connected devices are a clear use for edge computingarchitecture.
* With remote sensors installed on a machine, component or device, they generate massive amounts ofdata.
* If that data is sent back across a long network link to be analyzed, logged and tracked, that takes much more time than if the data is processed at the edge, close to the source of thedata.
* In essence, fog is the standard, and edge is the concept. Fog enables repeatable structure in the edge computing concept, so enterprises can push compute out of centralized systems or clouds for better and more scalableperformance.

Characteristics of Fog computing

1. Contextual location awareness andlow latency.
2. Graphicdistribution
3. Deployment near IoTendpoints.

Benefits of Fog Computing :

* Greater business agility : With the right tools, developers can quickly develop fog applications and deploy them whereneeded.
* Better security : Protect your fog nodes using the same policy, controls, and procedures you use in other parts of your IT environment. Use the same physical security and cyber securitysolutions.
* Deeper insights, with privacy control :Analyse sensitive data locally instead of sending it to the cloud foranalysis.
* Lower operating expense : Conserve network bandwidth by processing selected data locally instead of sending it to the cloud foranalysis.

# M2M

* Machine to Machine (M2M) communication is the communication among the physical things which do not need humanintervention.
* M2M communication is a form of data communication that involves one or more that do not necessarily require human interaction or intervention in the of communication. M2M is also named as Machine TypeCommunication

3GPP.

* M2M communication could be carried over mobile networks (e.g. GSM-GPRS, CDMA EVDO networks). In the M2M communication, the role of mobile network is largely confined to serve as a transportnetwork.

is only a subset of IoT. IoT is a more encompassing phenomenon because it also includes Human-to-Machine communication (H2M).

* RadioFrequency Identification (RFID), Location-Based Services (LBS), Lab-on-a-Chip (LOC), sensors, Augmented Reality (AR), robotics and vehicle telematics, which are some of the technology innovations that employ both M2M and H2Mcommunications.
* Reasons for shifting from M2M to IoT:
  1. It supports multiple application with multipledevice.
  2. It is information and servicecentric.
  3. It supports open marketplace.
  4. IoT uses Horizontal enablerapproach.
  5. It requires generic commoditydevices.
  6. Used in B2B andB2C.

Key features of M2M :

1. Low Mobility : M2M Devices do not move and if moves only within a certain area.
2. TimeControlled data can be sent or receive only at certain pre -defined time periods.
3. Time Tolerant : Sometimes data transfer can bedelayed.
4. Packet Switched : Network operator to provide packet switchedservice
5. Online small Data Transmissions : Devices frequently send or receive small amounts ofdata.
6. Low Power Consumption : To improve the ability of the system to efficiently serviceM2Mapplications.
7. LocationSpecificTrigger Intending to trigger M2Mdevice in a particulararea

e.g. wake up the device.

Six Pillars of M2M :

* The six pillars of M2M are as follows:

1. Remote monitoring is a generic term most often representing supervisory control, data acquisition and automation of industrialassets.
2. RFIDisadata-collectiontechnologythatuseselectronictagsforstoringdata.
3. A sensor network monitors physical or environmental conditions, with sensor nodes acting cooperatively to form/maintain thenetwork.
4. The term smart service refers to the process of networking equipment and monitoring it at a customer's site so that it can be maintained and serviced more effectively.
5. Telematics to the integration of telecommunications and infomatics, but most often it refers to tracking, navigation and entertainment applications invehicles.
6. Telemetry is usually associated with industrial, medical and wildlife-tracking applications that transmit small amounts of vehiclesdata.

#### Architecture and Components of M2M

* Fig. 1.5.1 shows M2Marchitecture.

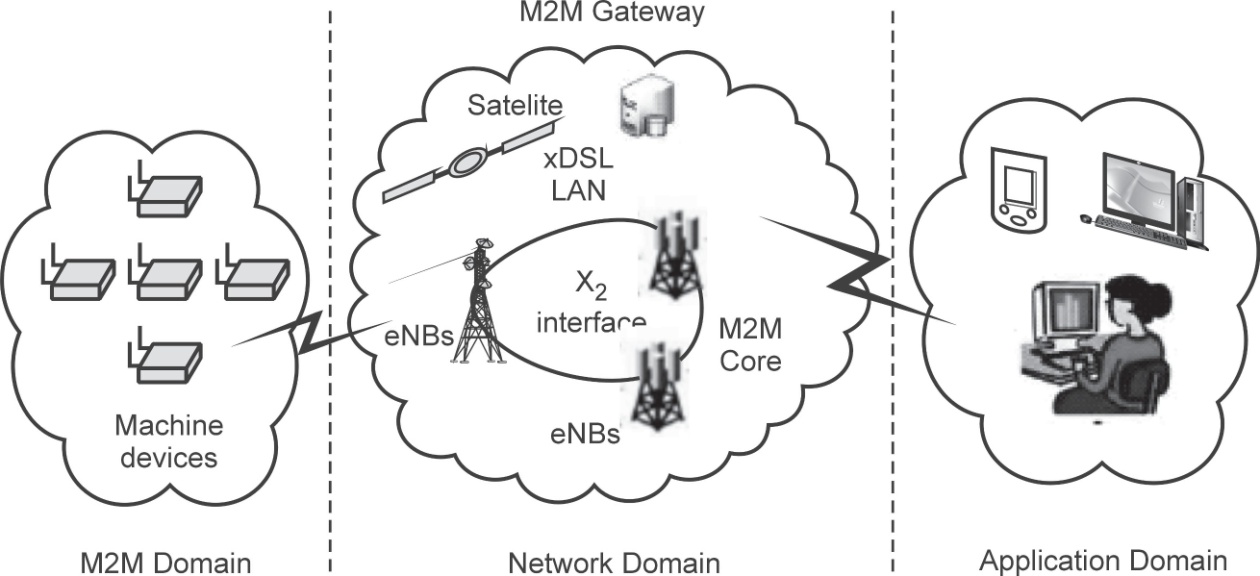
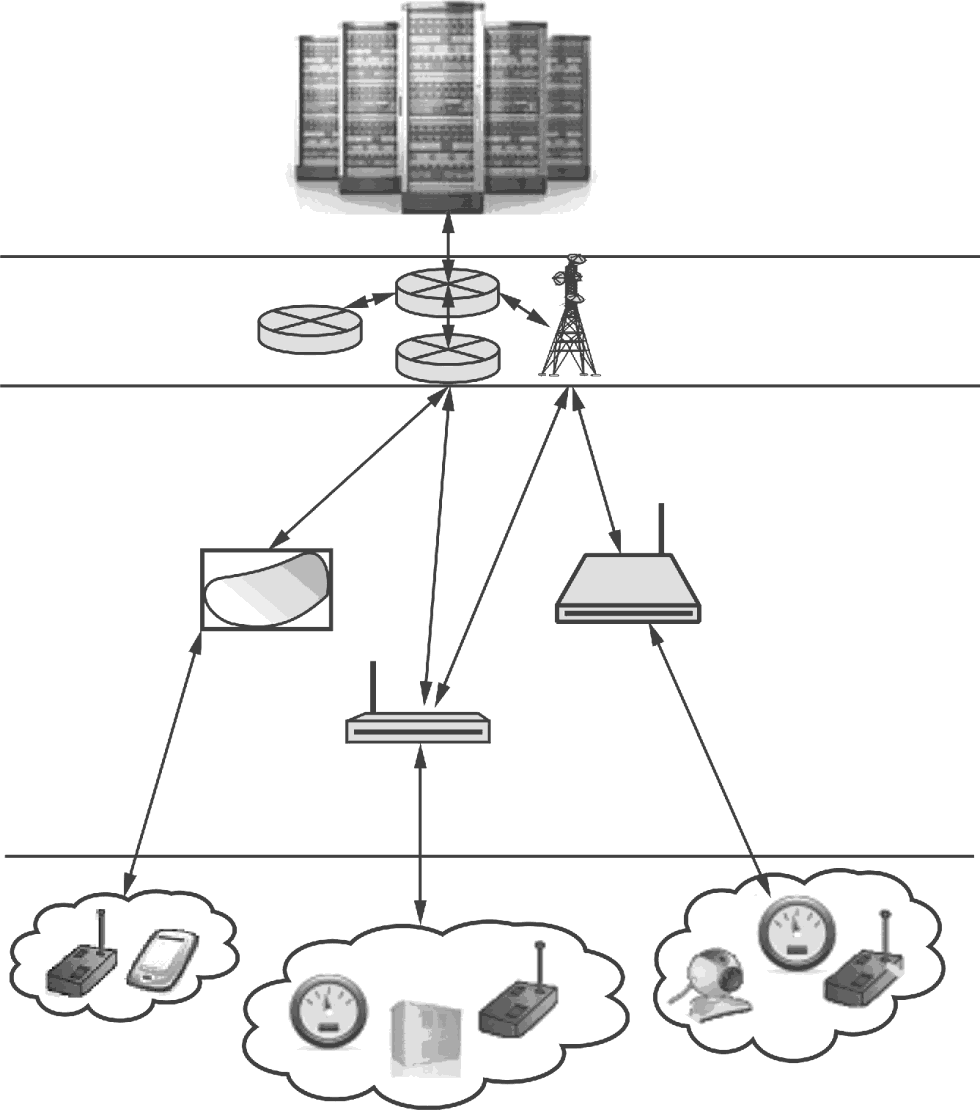


Fig. 1.5.1 : M2M arch tecture

#### The system components of an M2M solution are as follows:

1. M2M Device : A device that runs application(s) using M2M capabilities and network domain functions. An M2M device is either connected straight to an access network or interfaced to M2M gateways via an M2M areanetwork.
2. M2M area network : A M2M area network provides connectivity between M2M devices and M2M gateways. Examples of M2M areabetworks include : Personal area network technologies such as IEEE 802.15, SRD, UWB, Zigbee, Bluetooth, etc or local networks such as PLC, M-BUS, WirelessM-BUS.
3. M2M gateways :Equipments using M2M capabilities to ensure M2M devices interworking and interconnection to the network and application domain. The M2M gateway may also run M2Mapplications.
4. M2M applications server : Applications that run the service logic and use service capabilities accessible via openinterfaces.
5. M2M application : The application component of the solution is a realization of the highly specific monitor and control process. The application is further integrated into the overall business process system of theenterprise.

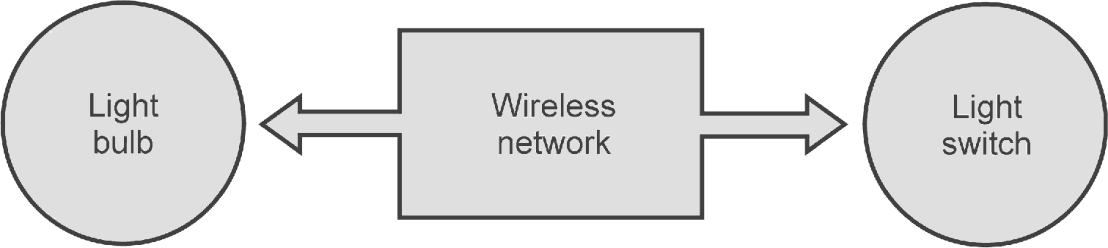
* Fig. 1.5.2 shows generic M2Msolution.

Backend (Datacentre, cloud)

Network core

M2M gateways

M2M devices



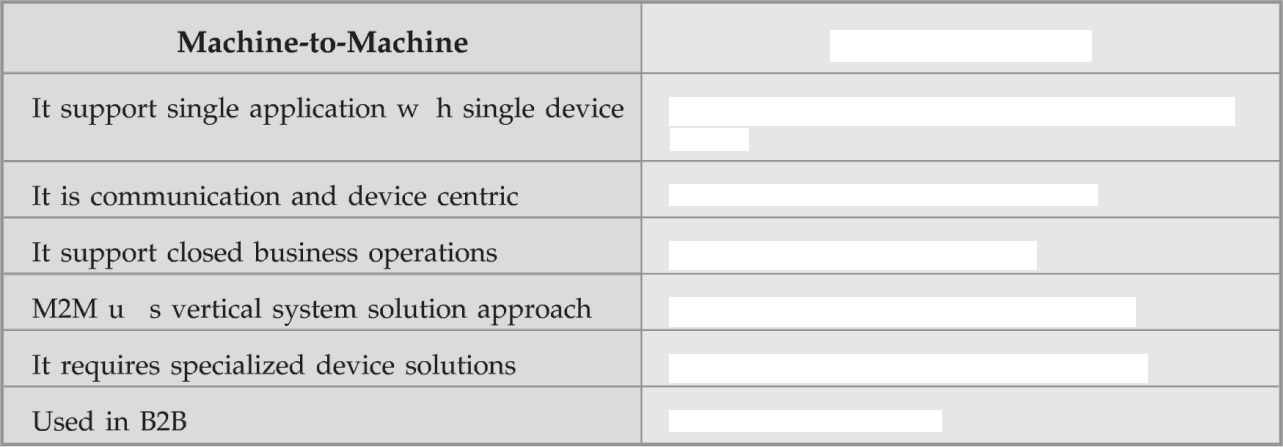
ManufacturerA Bluetooth, Z-wave,Zigbee

Fig. 1.5.2 Generic M2M solution

Manufacturer B

#### A number of sub-sets of users of M2M services can be identified : Consumers in the home, business users and facility managers, city goverrunents, logistics businesses, energy providers andmore.

Difference between M2M andIoT



Internet of Thigs

It support multiple applation with multiple device

It is information and service centrIt support open market place

IoT uses horizontal enablerapoach It requires generic commodity dices

Used in B2B and B2C

Functional Blocks of an IoTEcostern

* Fig 1.6.1 showsIoTfunc ocks.
* IoT functional block consists of device, communication, services, security and application.

Application

Services

Management Security

Communication

Device

F g. 1.6.1 : functional block of IoT

#### Device : An IoT system comprises of devices that provide sensing, actuation, monitoring and controlfunctions.

* Communication : Handles the communication for the IoTsystem.
* Services : services for device monitoring, device control service, data publishing services and services for devicediscovery.

#### Management : this block provides various functions to govern the IoTsystem.

* Security : this block secures the IoT system and by providing functions such as authentication, authorization, message and content integrity, and datasecurity.

#### Application : This is an interface that the users can use to control and monitor various aspects of the IoT system. Application also allow users to view the system status and view or analyse the processeddata.

Sensors

* Sensor converts a physical quantity into a corresponding voltage. Sensor is a device that when exposed to a physical phenomenon (temperature, displacement, force,etc.)producesaproportionaloutputsignal(electrical,mechanical,magnetic,
* transducer is often used synonymously with sensors. Sensor is a device that responds to a change in the physical phenomenon. On the other hand, a transducer is a device that converts one form of energy into another form of energy. Sensors are transducers when they sense one form of energy input and output in a different form ofenergy.
* Sensors can also be classified as passive or active. In passive sensors, the power required to produce the output is provided by the sensed physical phenomenon itself whereas the active sensors require external powersource.
* In embedded system, sensor and actuators are used for controlling the system. Sensors are connected to input port. Actuators are connected to outputport.
* Sensor captures the changes in the environmental variable. Middle system process the information. Actuators are changed according to the input variable. It displays theoutput.
* Example of control is air conditioner system. It controls the room temperature to a specifiedlimit.
* Deflection : The signal produces some physical (deflection) effect closely related to the measured quantity and transuded to beobservable.
* Null : The signal produced by the sensor is counteracted to minimize the deflection. That opposing effect necessary to maintain a zero deflection should be proportional to the signal of themeasurand.
* Here, the output is usually an 'electrical quantity' and measurand is a ’physical quantity, property or condition which is to bemeasured'.
* A sensor is a device that responds to a physical stimulus, measures the physical stimulus quantity and converts it into a signal usually electrical, which can be read by an observer or by aninstrument.
* A sensor can be very small and itself can be a trackable devices. The sensor itself, if not corinected is not part of the IoT or WSN valuechain.

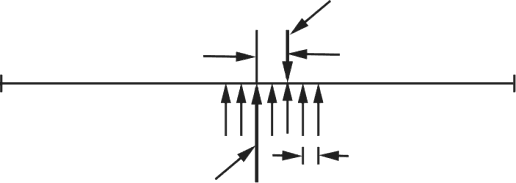
pecifications of Sensor :

1. Accuracy : Error between the result of a measurement and the true value being measured.
2. Resolution : The smallest increment of measure that a device canmake.
3. Sensitivity : The ratio between the change in the output signal to a small change in input physical signal. Slope of the input-output fitline.
4. Repeatability/Precision : The ability of the sensor to output the same value for the same input over a number oftrials.
5. Bandwidth : the frequency range between the lower and upper cut-off frequencies, within which the sensor transfer function is constantgain or linear.

Measurement

Accuracy

Resolution



True value

Fig. 1.7.1 : Accuracy v.R n

Types of Sensors

* Mechanical sensor : Any suitable mechanical / electrical switch may be adopted but because a certain amount of force is required to operate a mechanical switch it is common to usemicro-switches.
* sensor : These proximity sensors operate by breaking or disturbing an air pneumatic proximity sensor is an example or a contact type sensor. These cannot be used where light components may be blownaway.
* Optical sensor : In there simplest form, optimcal proximity sensors operate by breaking a light beam which falls onto a light sensitive device such as a photocell. These are examples of non contact sensors. Care must be exercised with the lighting environment of these sensors for example optical sensors can be blinded by flashes from are welding processes, airborne dust and smoke clouds may impede light transmissionetc.
* Electrical sensor : Electrical proximity sensors may be contact or non-contact. Simple contact sensors operate by making the sensor and the component complete an electrical circuit. Non-contact electrical proximity sensors rely on the electrical principles of either induction for detecting metals or capacitance for detecting non metals aswell.

ange sensing : Range sensing concerns detecting how near or far a component is from the sensing position, although they can also be used as proximity sensors. Distance or range sensors use non-contact analog techniques. Short range sensing, between a few millimetres and a few hundred millimetres is carried out using transmitted energy waves of various types e.g. radio waves, sound waves and lasers.

Sensor data Communication Protocols

1. Direct transmission protocols:
   * In direct communication protocol, each sensor sends its data directly to the base station.Ifthebasestationisfarawayfromthenodes,directcommunication

a large amount of transmit power from each node.

* + quickly drain the battery of the nodes and reduce the system lifetime. However, the only receptions in this protocol occur at the base station, so if either the base station is close to the nodes, or the energy required receiving data is large, this may be an acceptable method ofcommunication.

1. Minimum transfer energy protocols:
   * In these protocols, nodes act as routers for other nodes’ data in addition to sensing the environment. These protocols differ in the way the routes are chosen.
   * Some of these protocols only consider the energy of the transmitter and neglect the energy dissipation of the receivers indetermining the routes.
   * Depending on the real time costs of the transmit amplifier and the radio electronics, the total energy expended in the system might actually be greater using MTE routing than direct transmission to the basestation.
   * It is clear that in MTE routing, the nodes closest to the base station will be used to route a large number of data messages to the basestation.
   * Thus, these nodes will die out quickly, causing the energy required to get the remaining data to the base station to increase and more nodes todie.

Wireless Sensor Network

* WSN is more for sensing and information-colleting purposes. Other networks include body sensor network (BSN), visual or video sensor network (VSN), vehicular sensor networks, underwater (acoustic) sensor networks, interplanetary sensor networks, fieldbus networks andothers.
* The scope of WSN is the USN or ubiquitous sensor network, a network of intelligent sensors that could one day becomeubiquitous.

#### A wireless sensor network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with some sensors to detect physical phenomena. In IoT, the sensor nodes and devices are interconnected to transmit useful measurement information via distributed sensor networks.

* Other networks are body sensor network (BSN), video sensor network (VSN), vehicular sensor network (V2V), interplanetary sensor networketc.
* VSN devices come with image sensors, adequate processing power and memory. They use wireless communication interfaces to collaborate and jointly solve tasks such as tracking persons within the network. In all applications, VSNs monitor a potentially large group of people and record sensitive image data which might contain identities of persons, their behaviour, interaction patterns or personal preferences.
* A central idea of VSNs is to keep data processing local to reduce the amount of transmitted data. Fig. 1.7.2 showsVSN.

ationer

Visual sensor 3

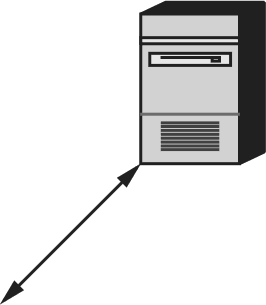
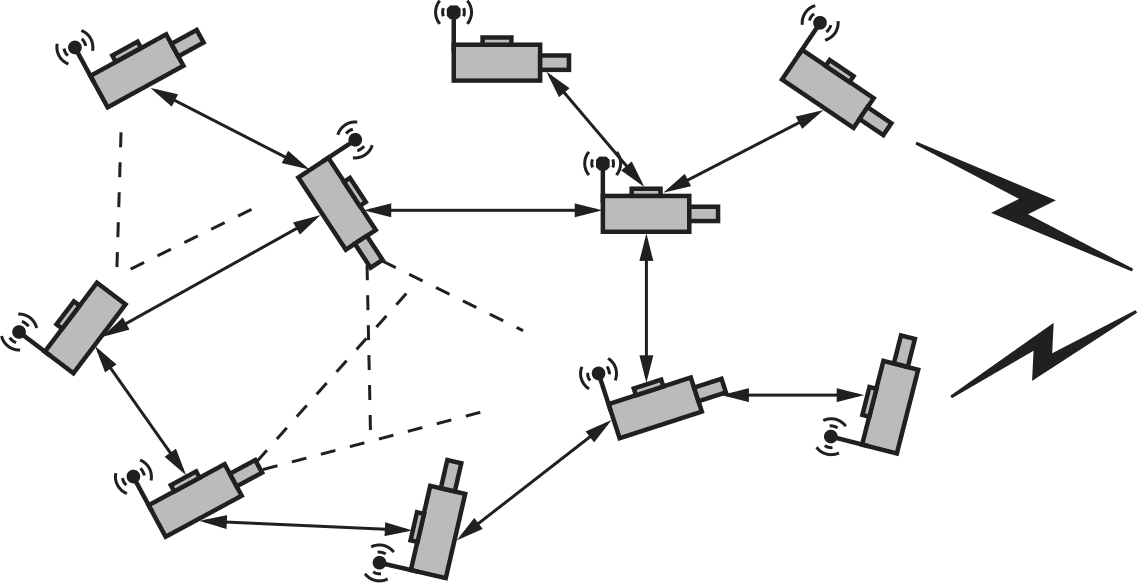
Objective

ensor 2

Visual sensor 1

Applic

serv



Visual s

Sink





#### A single VSN device has only a limited field of view but VSNs are typically designed to cover large areas. Therefore, multiple spatially distributed nodes are required. To avoid centralized control and data processing, VSNs use peer to peer communication for coordination, configuration, data exchange, handover of tracked objects or datafusion.

* To simplify deployment of spatially distributed VSNs, they rely no longer only on dedicated communication networks but make use of existing infrastructure which is not under full control of the VSNoperators.

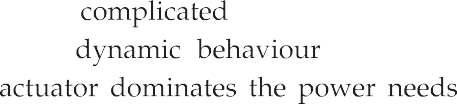
Actuators

* A device or mechanism capable of performing a physical action. Actuators interact with the world. Sensors capture information from theworld.
* The interface between the microcontroller and the sensors or the actuators is either digital.









Sensor Controlcenter Actuator



Temperature sensor detects heat.



F

Sends this detect signal to the control center.

Control center sends command to sprinkler.

Sprinkler turns on and puts out flame.

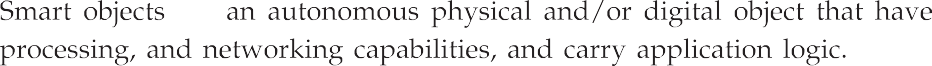
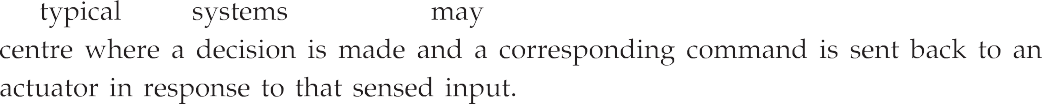
















i1 recently, smart objects were realized with limited communication capabilities, such as RFID tags, but the new generation of devices has bidirectional wireless communication and sensors that provide real-time data such as temperature, pressure, vibrations, and energymeasurement.

* Smart objects can be battery-operated, but not always, and typically have three components: a CPU (8-, 16- or 32-bit micro-controller), memory and a low-power wireless communicationdevice.
* The size is small and the price islow.
* Advantages in designing IoT systems based on smart objects are asfollows:

1. Energy saving is one of them. Smart objects are usually powered bybattery.
2. The second advantage is automation. IoT smart objects are autonomous and self-governed.
3. They operate independently and can collaborate with other objectsglobally.

* Challenges of Using Smart Objects:

1. Smart objects are often constrained devices and are usually poweredby battery.
2. Frequently they are working in real-time mode. These are the main causes of thechallenges.
3. Other challenge is connectivity. Currently a large number of networking technologies are being employed in connecting physical devices together and to theInternet.
4. Security and privacy is of big concern for smart object based IoTsystems.
5. Diversity of communication technologies: Depending on the application and the environment in which the system is deployed, smart objects can use a wide range of communicationtechnologies

Communication Patterns used for Smart Objects

* Smart object communication patterns can be divided into three categories: one-to-one, one-to-many andmany-to-one.
* Smart objects have specific communication patterns based on theirapplication
* often communicate over unreliable communication channels. The radio transmission of a smart object with a radio transceiver may be disturbed by other radio senders in thevicinity.

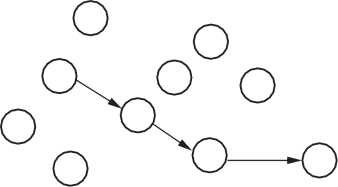
One-to-one communication pattern occurs when one smart object communicates with another smart object. The communication may involve other smart objects, however, as the communication may be routed through a network of smart objects. Fig 1.9.1 shows one-to-one communication in a smart objectnetwork.

Fig. .9.1 : one-to-one communication in a smart object network

1. One-to-many communication pattern is used for sending messages from one node to several other nodes and possibly all other nodes in the network. This can beused,forexample,forsendingacommandtoasetofnodesinthenetwork.

Fig 1.9.2 shows one-to-many communication in a smart objectnetwork.

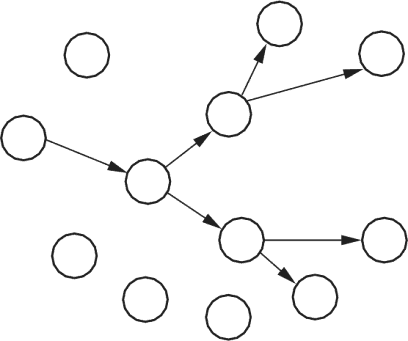
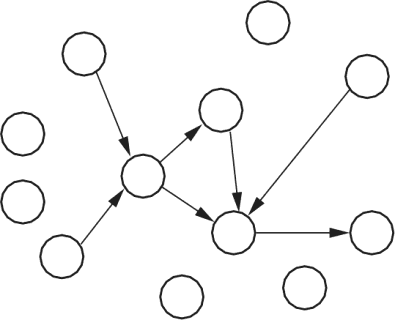


Fig.1..2 on o- munication in a smart objectnetwork

1. Many-to-one communication occurs frequently in smart object networks that collect data from the nodes. In many-to-one communication, several nodes send data toward a single node. This node is often called a sink node. Fig 1.9.3 shows Many-to-one communication in a smart objectnetwork.



ig.1. -t mmunication in a smart objectnetwork

#### any-to-one communication can be used to collect sensor data, such as temperature data, from the nodes in the network, but it can also be used for network health status information.

* + Nodes send periodic status reports to a sink node. The sink node then reports the overall performance of the network to an outsideobserver.

Connecting Smart Objects

* Range is one the communication criteia for smart objects. Range may be short, medium andlong.

1. Short range : classical example is serial cable. It supportingupto l0meters as distance between two devices. Example of wireless technologies are and visible lightcommunication.
2. Medium range : its range is 10 to 100 meters. It is main categories of IoT access technologies. Maximum distance between two devices is less than 1 mile. Example is 802.11 Wi-Fi, IEEE 802.15.4 and 802.15.4g WPAN. For wired technology, 802.3 Ethernet is anexample.
3. Long range : here the distance is greater than 1 miles between two devices. Example of wireless technology are 2G, 3G, 4Getc.

Frequency Bands :

* Frequency band is a specific range of frequencies in the radio frequency (RF) spectrum, which is divided among ranges from very low frequencies (vlf) to extremely high frequencies (ehf). Each band has a defined upper and lower frequencylimit.
* Very low frequencies (vlf) range from 3 to 30 kilohertz (kHz). Time signals and standard frequencies are among the users of thisband.
* Low frequencies (lf) range from 30 to 300 kHz. Fixed, maritime mobile and navigational systems and radio broadcasting are among the users of thisband.
* Medium frequencies (ml) range from 300 to 3000 kHz. Land, maritime mobile and radio broadcasting are among the users of thisband.
* High frequencies (hf) - also called shortwaves - range from 3 to 30 megahertz (MHz). Fixed, mobile, aeronautical and marine mobile, amateur radio, and radio broadcasting are among the users of thisband.
* Cellular networks operate on different frequency bands including the 450 MHz band, 700 MHz band, 800 MHz band, 900 MHz band, 1800 MHz band, 2100 MHz band, and 2600 MHzband.

e industrial, scientific, and medical radio band (ISM band) refers to a group of radio bands or parts of the radio spectrum that are internationally reserved for the use of radio frequency (RF) energy intended for scientific, medical and industrial requirements rather than forcommunications.

* In the U.S., the 902-928 MHz, 2.4 GHz and 5.7-5.8 GHz bands were initially used for machines that emitted radio frequencies, such as RF welders, industrial heaters and microwave ovens, but not for radiocommunications.

Power Consumption :

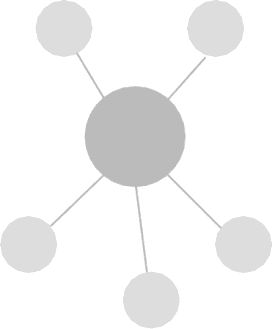
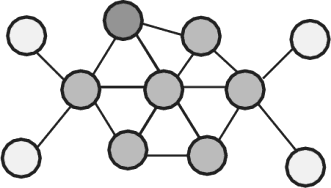
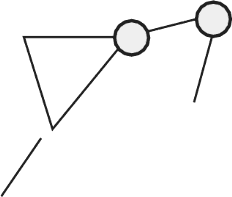
* IoT uses two types of devices: powered node and battery powerednode.
* Powered node has a direct connection to a power source and communications are usually not limited by power consumptionscriteria.
* Battery powered nodes bring much more flexibility. Batteries can be changed or device can bereplaced.
* Wireless sensor nodes are battery-powered devices, since it is generally difficult or impossible to run a mains supply to their deployment site. Power to the wireless sensor nodes is usually provided through primarybatteries
* Primary batteries are typical power sources for sensor nodes. By supplying their energy at the required voltage levels, they eliminate the need for intermediate power conditioningelectronics.
* When a primary battery is the single power source of a sensor node, the amount of initially stored energy determines the node's lifetime. The main metric of primary batteries is theirenergy density.

Topology :

* For connecting IoT devices, three main topologies are used. They are star, mesh and pee-to-peertopology.
* In the star network topology, a central node has a direct connection to all other nodes.
* In the mesh topology every node can be both an end device or a router, meaning that each node has several links to the coordinator. This means that if one of the routers goes offline, most of the network is still intact by rerouting through the remainingrouters.
* Peer-to-peer topology rely on multiple full functiondevices.
* A network is said to be fully meshed if all nodes are directly connected to all other nodes, and partially meshed if only some nodes have multiple connections to others. Meshing to create multiple paths increases resiliency under failure, but increasescost.



y node



Peer to Peer topology

Mesh topology

Sensor nodes

Gatewa

Star topology

* Peer-to-peer topology rely on multiple full functiondevices.
* A network is said to be fully meshed if all nodes are directly connected to all other nodes, and partially meshed if only some nodes have multiple connections to others. Meshing to create multiple paths increases resiliency under failure, but increasescost.

Constrained Devices

* Following are the classes of constrained nodes as defined by RFC7228

ass 0 devices : They are so severely constrained in memory and processing capabilities that most likely they will not have the resources required to communicate directly with the Internet in a secure manner. Class 0 devices will participate in Internet communications with the help of larger devices acting as proxies, gateways, or servers. Class 0 devices generally cannot be secured or managed comprehensively in the traditional sense. They will most likely be preconfigured with a very small data set. For management purposes, they could answer keepalive signals and send on/ off or basic health indications.

1. Class 1 devices are quite constrained in code space and processing capabilities, such that they cannot easily talk to other Internet nodes employing a full protocol stack such as using HTTP, Transport Layer Security (TLS), and related security protocols and XML-based data representations. However, they are capable enough to use a protocol stack specifically designed for constrained nodes and participate in meaningful conversations without the help of a gateway node. In particular, they can provide support for the security functions required on a largenetwork.
2. Class 2 devices are less constrained and fundamentally capable of supporting most of the same protocol stacks as used on notebooks or servers. However, even these devices can benefit from lightweight and energy-efficient protocols and from consuming less bandwidth. Furthermore, using fewer resources for networking leaves more resources available to applications. Thus, using the protocol stacks defined for more constrained devices on Class 2 devices might reduce development costs and increase theinteroperability.

Two Marks Questions with Answers

* 1. DefineIoT.

Ans. :By embedding short-range mobile transceivers into a wide array of addition 1 gadgets and everyday items, enabling new forms of communication between people and things, and betweenthings.

* + - The Internet of Things (IoT) is the network of physical objects i.e. devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchangedata.
  1. How IoT differ from traditional computing?

Ans. :IoT data differs from traditional computing. The data can be small in size and frequent in transmission. The number of devices, or nodes, that are connecting to the network are also greater in IoT than in traditional PCcomputing.

* 1. List the characteristics of the Internet ofThings.

Ans. : Characteristics of the Internet of Things are Interconnectivity, Heterogeneity, Things-related services and dynamic changes.

* 1. List the advantages of IoT. Ans. : Advantages:

1. Improved customer engagement andcommunication
2. Support for technologyoptimization
3. Support wide range of datacollection
4. Reducedwaste
   1. What do you mean autonomy in IoT†

Ans. : Autonomy in IoT can be realized by implementing self-managing systems. Self-management is the property of a system to achieve management and maintenance of its resources intrinsically and internally. Management and maintenance is realized through many levels of decision making.

* 1. What is M2M communication†

Ans. : M2M communication is a form of data communication that involves one or more entities that do not necessarily require human interaction or intervention in the process ofcommunication.

* 1. What are the key features of M2M communication?

Ans. :

* Some of the key features of M2M communication sy tern are given below:

1. Low mobility M2M devices do not move and if movesonly within a certainarea.
2. Time controlled : Data can be send or receive only at certain pre-defined timeperiods.
3. Time tolerant : Sometimes data transfer can bedelayed.
4. Packet switched : Network operator to provide packet switchedservice.
   1. What is M2M device?

Ans. : A device that runs application(s) using M2M capabilities and network domain functions. An M2M device is either connected straight to an access network or interfaced to M2M gateways via an M2M areanetwork.

* 1. **Definesensor.**

Ans. : Sensor converts a physical quantity into a corresponding voltage. Sensor is a device that when exposed to a physical phenomenon (temperature, displacement, force, etc.) produces a proportional output signal (electrical, mechanical, magnetic, etc.).

* 1. Definetransducer.

Ans. : The term transducer is often used synonymously with sensors. Sensor is a device that responds to a change in the physical phenomenon. On the other hand, a transducer is a device that converts one form of energy into another form of energy. Sensors are transducers when they sense one form of energy input and output in a different form ofenergy.

* 1. What is actuator†

Ans. : A device or mechanism capable of performing a physical action. Actuators interact with the world. Sensors capture information from the world. The interface between the microcontroller and the sensors or the actuators is either analog ordigital.

* 1. What is Participatory sensing†

Ans. : Participatory sensing is the process whereby individuals and communities use ever more capable mobile phones and cloud services to collect and analyze systematic data for use in discovery. Participatory Sensing is data collection andinterpretation.

* 1. Discuss active and passive sensor. Ans.:
     1. Active sensors : Require an external source of power (excitation voltage)tha

provides the majority of the output power of the signal.

* + 1. Passive sensors : The output power is almost entirely provided by the measured signal without an excitationvoltage.