UNIT III

4 Introduction & IoT Technologies Behind Smart and Intelligent Devices

Syllabus

IoT Concepts, Introduction to IOT Communications, Telemetry vs IOT, Applications of IOT Communications, People, Processes and Devices. Automation, asset management, telemetry, transportation, telematics. Telemetry and Telemetric; Report location, logistics, tracking and remote assistance; Next generation kiosks, self-service technology; Cellular IOT connectivity services.

Contents

4.1 IoT Concept

- The Internet of Things (IoT) refers to the capability of everyday devices to connect to other devices and people through the existing Internet infrastructure. Devices connect and communicate in many ways.
- Examples of this are smartphones that interact with other smartphones, 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 third parties.
- Things are objects of the physical world (physical things) or of the information world (virtual world) which are capable of being identified and integrated into communication networks. Things have associated information, which can be static and dynamic.
- Physical things exist in the physical world and are capable of being sensed, actuated and connected. Examples of physical things include the surrounding environment, industrial robots, goods and electrical equipment.
- Virtual things exist in the information world and are capable of being stored, processed and accessed. Examples of virtual things include multimedia content and application software.
- A device is a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing.
- The devices collect various kinds of information and provide it to the information and communication networks for further processing. Some devices also execute operations based on information received from the information and communication networks.
- Fig. 4.1.1 shows evolutionary phase of internet.

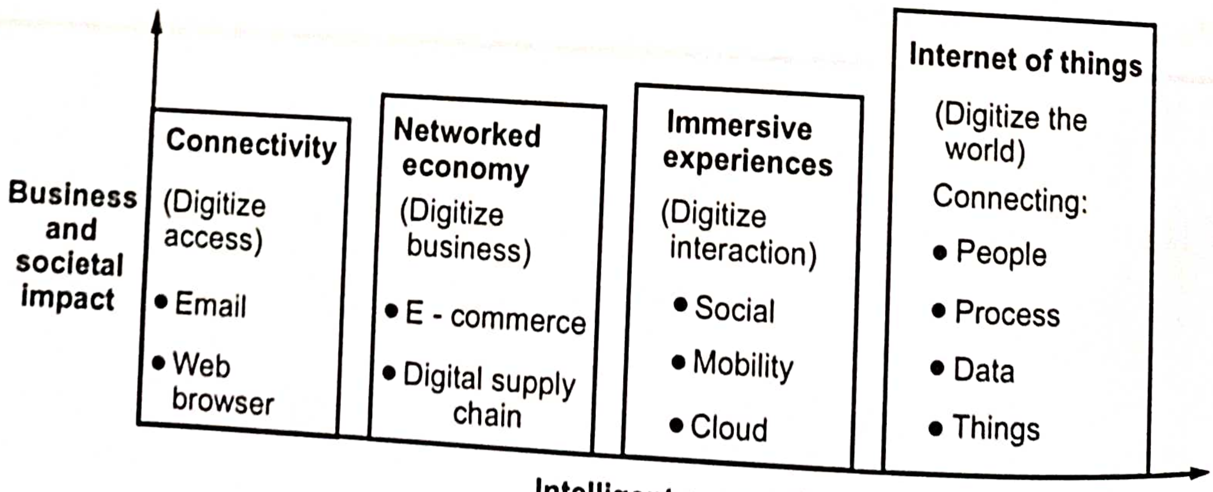


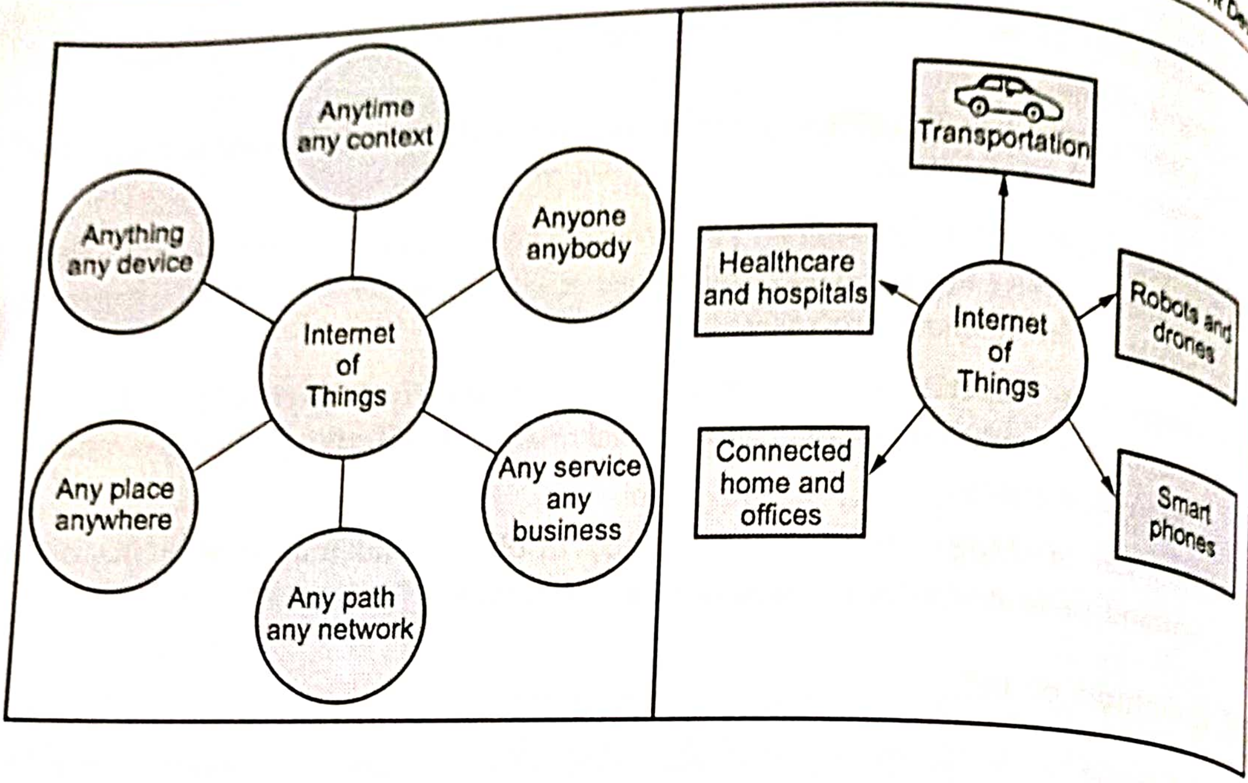
Fig. 4.1.1 : Evolutionary phase of internet

- Evolutionary phase of internet is Connectivity, Networked Economy, Immersive Experiences and IoT.

1. **Connectivity** : In the phase, peoples are connected to email, web services and searches the information.
2. **Networked economy** : This phase support e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.
3. **Immersive experiences** : This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility.
4. **Internet of things** : It adds connectivity to objects and machines in the world around us to enable new services and experiences.

4.1.1 Definition of IoT

- 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 exchange data.
- Wikipedia definition : The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects, usually the network will be wireless and self-configuring, such as household appliances.
- WSIS 2005 Definition : By embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things.
- The Internet of Things refers to the capability of everyday devices to connect to other devices and people through the existing Internet infrastructure.
- 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 third parties.
- 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 PC computing.
- Machine-to-Machine communications and intelligence drawn from the devices and the network will allow businesses to automate certain basic tasks without depending on central or cloud based applications and services.



- 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 of data.
- 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 symbiotic interaction.
- The smart object is the building block of the IoT 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 individual citizens.

- 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. There is no unique identification number system for object in the world.
  2. IoT uses Architecture Reference Model (ARM) but there is no further development in ARM.
  3. Missing large-scale testing and learning environments.
  4. Difficulties in exchanging of sensor information in heterogeneous environments.
  5. Difficulties in developing business which embraces the full support of the Internet of Things.

4.1.2 IoT Characteristics

1. **Interconnectivity :** Everything can be connected to the global information and communication infrastructure.
2. **Heterogeneity :** Devices within IoT have different hardware and use different networks but they can still interact with other devices through different networks.
3. **Things-related 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 can vary.
5. **Integrated into information network :** IoT devices are integrated with information network for communication purpose. It will exchange data with other devices.
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 of requirements.
7. Self-configuration primarily consists of the actions of neighbour and service discovery, network organization and resource provisioning.

4.1.3 Components 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, security, communication, and detection to support-specific goals and actions.

- Major components 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 main operation.

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 the Internet.

   a. Temperature sensors : Accelerometers

   b. Image sensors : Gyroscopes

   c. Light sensors : Acoustic sensors

   d. Micro flow sensors : Humidity sensors

   e. Gas RFID sensors : Pressure sensors

3. **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 two ways :

   a) There is an Internet-enable intermediate node acting as a gateway;

   b) The IoT Device has direct communication with the Internet.

- The communication between the main control unit and the communication module uses serial protocol in most cases.

4. **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 life duration.

- **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 common systems.

4.1.4 Working of IoT

- Fig. 4.1.2 shows working of IoT.

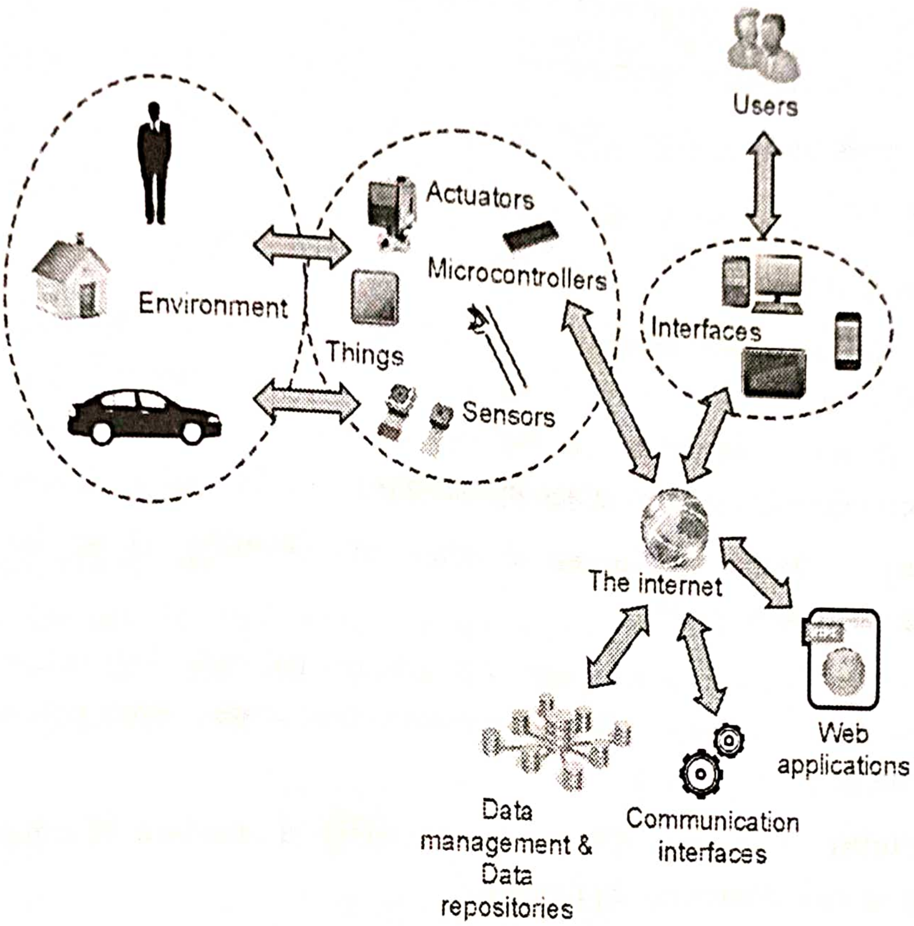


Fig. 4.1.2 : Working of IoT

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 the Internet.
2. **Actuate device based on triggers :** It can be programmed to actuate other devices based on conditions set by user.
3. **Receive information :** Device can also receive information from the network.
4. **Communication assistance :** It provides communication between two devices of same network or different network.

- Sensors for various applications are used in different IoT devices as per different applications such as temperature, power, humidity, proximity, force etc.
- Gateway takes care of various wireless standard interfaces and hence one gateway can handle multiple technologies and multiple sensors.
- 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 or Fibre.

4.1.5 Advantages and Disadvantages

Advantages of IoT

1. Improved customer engagement and communication.
2. Support for technology optimization.
3. Support wide range of data collection.
4. Reduced waste.

Disadvantages of IoT

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 by hackers.
2. **Flexibility :** Many are concerned about the flexibility of an IoT system to integrate easily with another.
3. **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 of inconvenience.
4. **Compatibility :** Currently, there is no international standard of compatibility for the tagging and monitoring equipment.
5. Save time and money.

4.1.6 IoT Framework and Architecture

- Fig 4.1.3 shows IoT functional blocks.

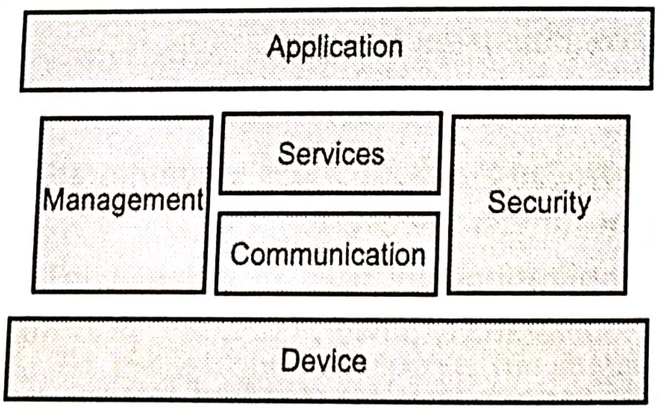


Fig. 4.1.3 : Functional block of IoT

- IoT functional block consists of device, communication, services, security and application.

- **Device** : An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.
- **Communication** : Handles the communication for the IoT system.
- **Services** : Services for device monitoring, device control service, data publishing services and services for device discovery.
- **Management** : This block provides various functions to govern the IoT system.
- **Security** : This block secures the IoT system and by providing functions such as authentication, authorization, message and content integrity, and data security.
- **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 processed data.

4.2 Introduction to IoT Communications

Request/Response model :

- In the Request/Response model, client requests information from the server and waits till the response is served from the server. Fig. 4.2.1 shows Request/Response model.

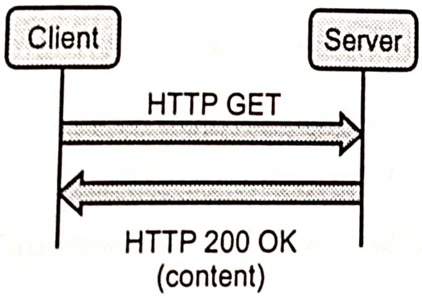


Fig. 4.2.1 Request / Response model

- HTTP protocol is used by Request/Response model. For example, a browser client may request a web page from the server through a "Request" and the corresponding web page will be served by the server as a "Response".
- The client and the server can communicate one to one, or one to many with more requests.
- This model is stateless communication model and each request-response pair is independent of others.

Publish/Subscribe Model :

- **Publishers** : Publishers generate event data and publishes them.
- **Subscribers** : Subscribers submit their subscriptions and process the events received

- **Publish/Subscribe service :** It's the mediator/broker that filters and routes events from publishers to interested subscribers.
- Fig. 4.2.2 shows Publish/Subscribe Model.

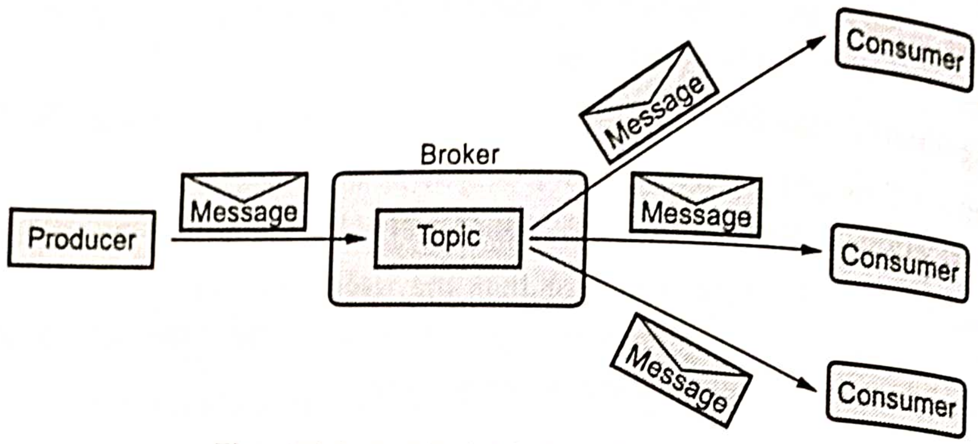


Fig. 4.2.2 Publish / Subscribe model

- The publishers and subscribers are autonomous, which means that they do not need to know the presence of each other.
- This model is highly suited for mobile applications, ubiquitous computing and distributed embedded systems.
- Failure of publishers or subscribers does not bring down the entire system.
- No strong guarantee on broker to deliver content to subscriber. After a publisher publishes the event, it assumes that all corresponding subscribers would receive it.
- Potential bottleneck in brokers when subscribers and publishers overload them.

Push/Pull Model :

- Data procedure push the data to queues and consumers pull the data from the queues. Fig. 4.2.3 shows push-pull model.

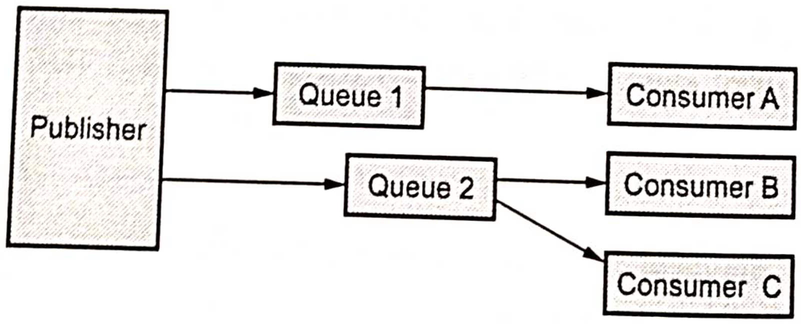


Fig. 4.2.3 Push-Pull model

- Sometimes queue act as buffer in between producer and consumer. Producer does not need to be aware of the consumers.

Exclusive Pair Model :

- This communication model is full duplex, bi-directional communication model. It uses persistent connection between client and server. Fig. 4.2.4 shows exclusive pair model.

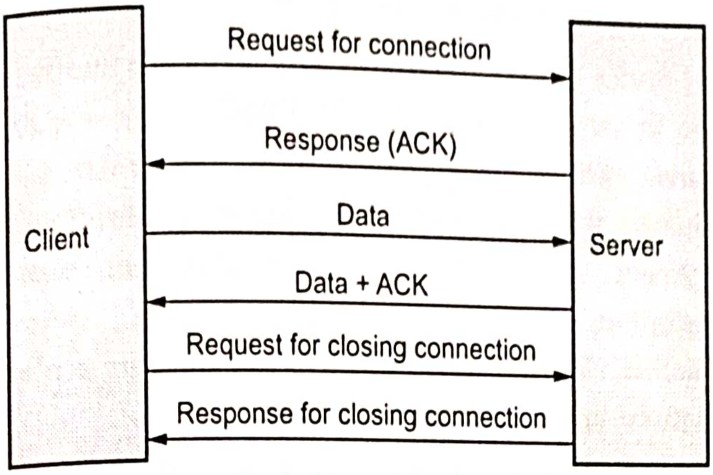


Fig. 4.2.4 Exclusive pair model

- Client send request to server for opening the connection. This connection is open till the client send request for closing the connection.

4.2.1 IoT Enabling Technologies

- IoT is enabled by several technologies including wireless sensor networks, cloud computing, Big data analytics, Embedded Systems, Security Protocols and architectures, communication protocols, web services, Mobile Internet, and Semantic Search engines.

4.2.1.1 Cloud 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 of things.
- Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (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 user interface.
- **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).

- **Software 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 work with.
- **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, memory etc.

4.2.1.2 Big Data Analytic

- A category of technologies and services where the capabilities provided to collect, store, search, share, analyze and visualize data which have the characteristics of high-volume, high-velocity and high-variety.
- Examples of big data generated by IoT systems :
  a) Weather monitoring stations
  b) Machine sensor data from industrial systems
  c) Health and fitness data
  d) Location and tracking systems

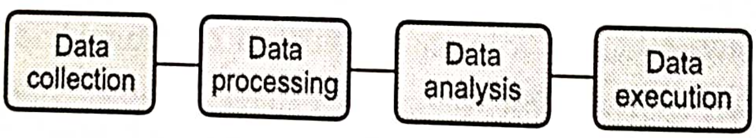


Fig. 4.2.5

4.2.1.3 Wireless Sensor Networks

- 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.

- WSNs nowadays usually include sensor nodes, actuator nodes, gateways and clients. A large number of sensor nodes deployed randomly inside of or 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 or satellite.
- 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 portable electronics.

4.2.1.4 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 the network.
- Communication protocol also performs error correction and detection, flow control, data encoding, addressing mechanism etc.
- Sequence control, lost of packet, retransmission are the other functions of communication protocol.

4.2.1.5 Embedded System

- A system is a set of interacting or interdependent component parts forming a complex unit. It is a fixed plan to perform one or many task.
- Embedded system is an electronic system which is designed to perform one or a limited set of functions using software and hardware.
- 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 systems can coexist in an embedding system.
- An embedded system has three main components: Hardware, Software and time operating system.
- Hardware parts includes power supply, processor, memory, times & communication ports, system application specific circuit etc.

- Software parts includes the application software is required to perform the series of tasks. An embedded system has software designed to keep in view of three constraints :
  a. Availability of system memory
  b. Availability of processor speed
  c. The need to limit power dissipation when running the system continuously in cycles of wait for events, run , stop and wake up.
- Demand for low cost and higher density platform requires the integration of devices. As integration levels increases, more and more logic is added to the processor die, creating families of applications specific service processors.
- System-on-Chip (SoC) designs increasingly become the driving force of a number of modern electronics systems. A number of key technologies integrate together in forming the highly complex embedded platform.

4.2.1.6 Unmanned Aerial Vehicle

- Unmanned Aerial Vehicle (UAV), popularly known as Drone, is an airborne system or an aircraft operated remotely by a human operator or autonomously by an onboard computer.
- An Unmanned Aerial System has three components :
  1. An autonomous or human-operated control system which is usually on the ground or a ship but may be on another airborne platform;
  2. An Unmanned Aerial Vehicle (UAV);
  3. A command and control (C2) system - sometimes referred to as a communication, command and control (C3) system - to link the two.
- UAVs. Fig. 4.2.6 shows UAV.

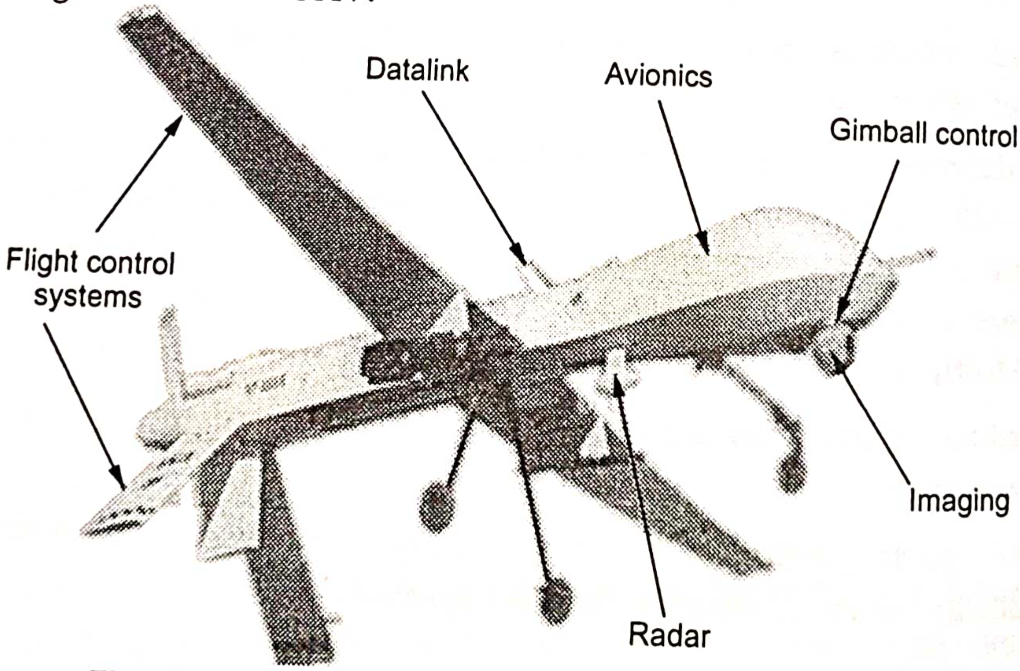


Fig. 4.2.6 Unmanned aerial vehicle block diagram

- UAV based Remote Sensing (UAV-RS) is the new addition to the North Eastern Space Applications Centre (NE-SAC) for large-scale mapping and real time assessment and monitoring activities of various applications.
- Nishant is a multi-mission Unmanned Aerial Vehicle with day/night capability used for battlefield surveillance and reconnaissance, target tracking & localization, and artillery fire correction. A sophisticated image processing system is used for analyzing the images transmitted from the UAV. It is launched using a Mobile Hydro pneumatic Launcher.
- UAVs are now capable of carrying out remote sensing, remote monitoring, courier delivery and a lot more. UAV networks are many times used for unmanned missions. There have been many attacks on civilian, military, and industrial targets that were carried out using remotely controlled or automated.
- UAVs can be categorized into fixed wing, multi-rotor, flapping and vertical flier kinds. Recently, many challenging tasks have been carried out using UAVs such as patrolling, border surveillance and wildfire monitoring.
- In the civilian sector, UAVs are currently used as toys, hobby aircraft, and research flight platforms. They have been employed in such tasks as airport wildlife control and population monitoring and are expected to contribute to autonomous crop surveying, atmospheric weather monitoring and search and rescue missions.

4.3 Telemetry vs IoT

- Telemetry is the automated communication processes from multiple data sources. Telemetry data is used to improve customer experiences, monitor security, application health, quality and performance.
- Telemetry is used for technologies that measure and collect data from remote locations and transmit this data to receiving systems for monitoring and analysis. Traditional examples of telemetry are :

  a) Monitoring data from space crafts

  b) Animal tracking devices

  c) Automobile sensors for fuel level, engine heat, vehicle speed and more

  d) Heart monitors (EKG)

  e) Convicted felon ankle bracelets

  f) Wearables such as Fitbit health monitoring devices
- Today, telemetry applications include measuring and transmitting data from sensors located in automobiles, smart meters, power sources, robots and even wildlife in what is commonly called the Internet of Things (IoT).

- Telemetry sensor devices are composed of transmission system, image and registration or control
- IoT are just the beginning of a very wide set of technologies. Intelligent objects have to be connected to a network to transmit the information they collect through the sensors from the environment. The data they transmit to this network is called telemetry.
- In a simple data exchange, telemetry may not be large, but consider that user have to send data from tens, hundreds or even thousands of sensors. At this point, user will need very well optimized, classified telemetry data.
- Depending of the usage area, telemetry data can be stored as a stateful variable either in the iCloud network or on a device. Storing on the device will increase the hardware requirements of the smart object. Storing in iCloud will require a stable network connection. In both scenarios, systematically coded telemetry data will need to be created.
- IoT devices used for telemetry such as remote sensors have the following requirements :
  a) Low power - Many IoT devices are powered from an embedded battery. New battery technologies have life expectancies of 10 to 20 years.
  b) Low-code footprint - IoT devices are required to be as small as possible. This requires lightweight protocols that do not need heavy computing or wireless transmission power requirements.
  c) Low bandwidth - Higher bandwidth transmissions require higher power and additional hardware footprints.
  d) Local intelligent IoT gateways - The closer this system is to the IoT device, the lower the power required to transmit to this receiving system.

4.4 Application of IoT Communication, People, Processes and Devices

1. **Home :** Buildings where people live. It controls home and security systems.
2. **Offices :** Energy management and security in office buildings; improved productivity, including for mobile employees.
3. **Factories :** Places with repetitive work routines, including hospitals and farms; operating efficiencies, optimizing equipment use and inventory.
4. **Vehicles :** Vehicles including cars, trucks, ships, aircraft and trains; condition-based maintenance, usage-based design, pre-sales analytics.

5. **Cities :** Public spaces and infrastructure in urban settings; adaptive traffic control, smart meters, environmental monitoring, resource management.

6. **Worksites :** It is custom production environments like mining, oil and gas, construction; operating efficiencies, predictive maintenance, health and safety.

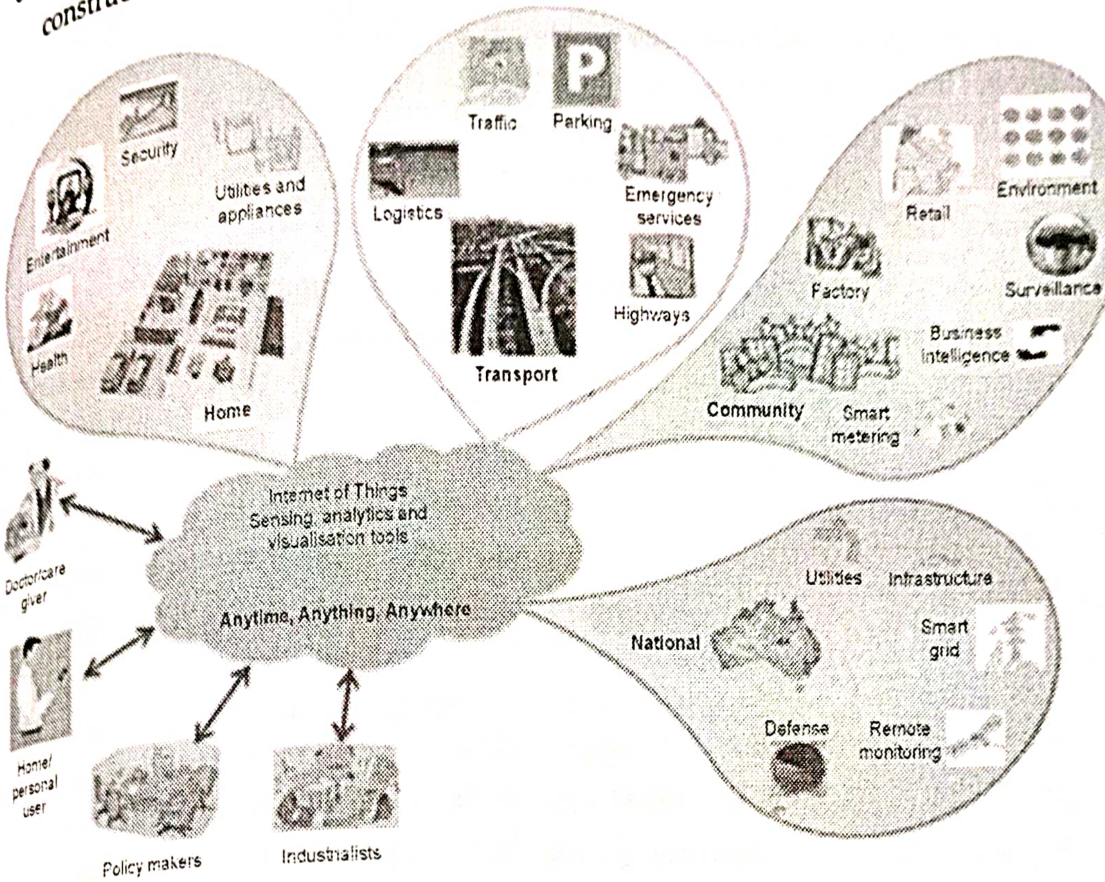


Fig. 4.4.1

4.4.1 Asset Management

- Asset management and monitoring refers to a systematic process of tracking and maintaining valuable things for any business entity or organization.
- Asset management involves the tracking of every physical device, either big or small, in an organization. It gives every detail about the status, location, condition and performance of the device in real-time. It helps in balancing and improving productivity with low cost-effectiveness.
- In the simplest form, asset management and monitoring can be described as a systematic process where assets are detected, categorized, supervised, maintained, operated, upgraded and replaced cost-effectively.
- An IoT-enabled asset management solution typically involves :
  a) Remote asset tracking
  b) Asset health/condition monitoring

c) Asset lifecycle management

d) Asset workflow automation

e) Predictive asset maintenance

4.4.2 Telematics

- Telematics is the technology used to monitor a wide range of information relating to an individual vehicle or an entire fleet. Telematics systems gather data including vehicle location, driver behaviour, engine diagnostics and vehicle activity, and visualize this data on software platforms that help fleet operators manage their resources.
- In recent years, telematics has changed the face of a number of industries, with it driving major transformation in transport, construction and site excavation. Firms managing fleets of vehicles across a huge range of sectors have come to adopt telematics, which has helped to improve reliability, boost customer service standards, increase efficiency and enhance the bottom line.
- Fleet telematics gathers a range of data using Global Positioning System (GPS) technology, sensors and vehicle engine data to provide fleet operators with the information they need to manage their fleet.
- It is automated vehicle routing and scheduling. It supports driver compliance, safety and performance reporting. Vehicle fleet tracking system uses GPS technology to track the location of the vehicle in the real time.
- Fig. 4.4.2 shows application using fleet.

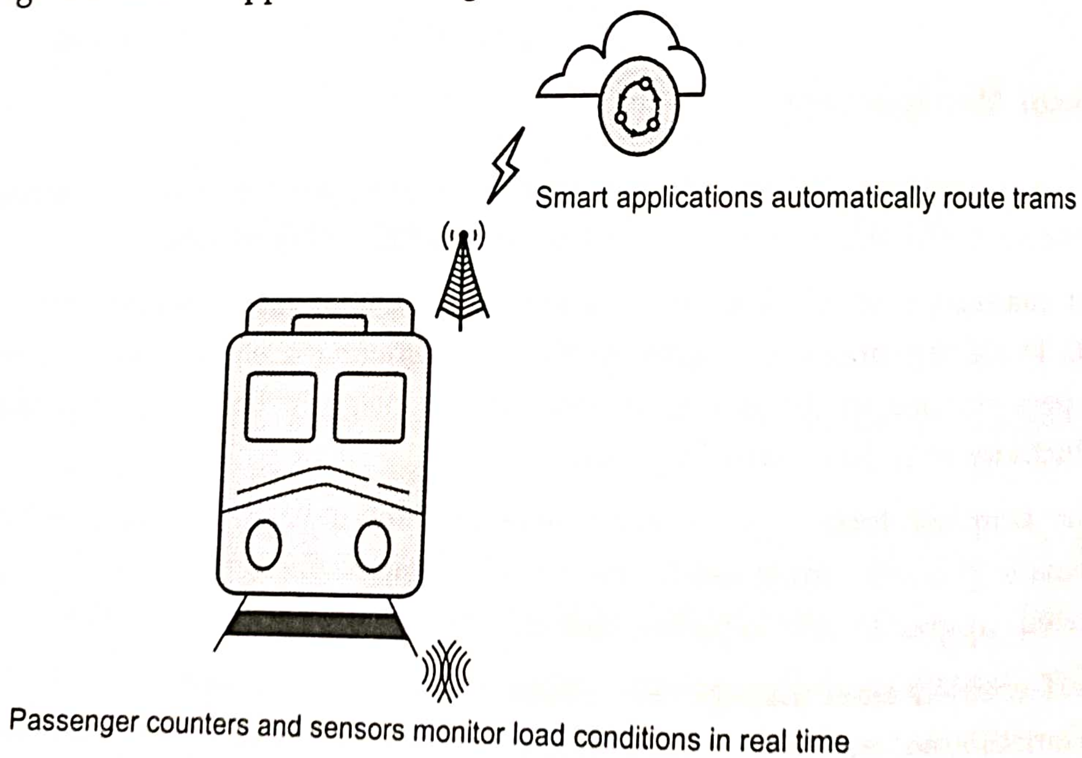


Fig. 4.4.2 (a)

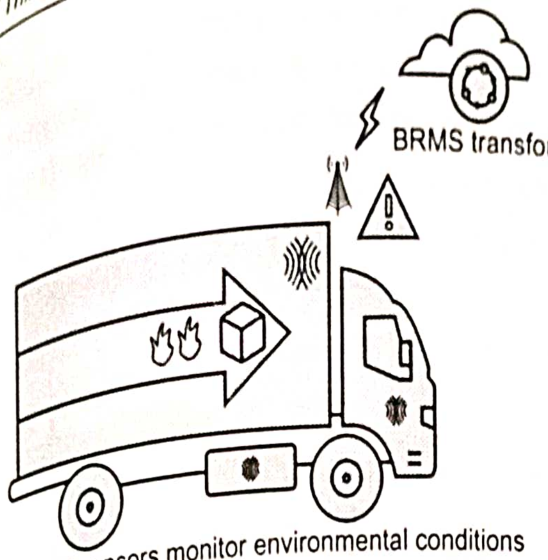


Fig. 4.4.2 (b) Fleet tracking

- Fleet maintenance and fuel conservation capabilities. Track, schedule and route vehicles in real time. Proactively manage fleet maintenance and fuel economy. It is also possible to monitor driver behavior and performance (distance traveled, speed, location).
- Telematics data is collected by a small device installed in the vehicle itself. This collects stores and transmits different types of information relating to the vehicle's performance, condition and usage. There are different types of telematics devices available that offer different functionality and benefits. The most accurate and secure telematics devices are hardwired, these devices offer tamper proof functionality and a wider range of connectivity to peripheral devices

Benefits :

a) Accelerate delivery and dispatch rates

b) Improve customer satisfaction

c) Reduce fuel consumption and vehicle maintenance costs

d) Ensure compliance with government and industry regulations

e) Improve fleet productivity, uptime, and safety

4.4.3 Telemetry

- The gathering of data from remote places for analysis and other purposes. It is at the heart of Industrial IoT (IIoT). In industry, telemetry was all wired, but the spread of low-power wireless devices that could form themselves into mesh networks made it ubiquitous.
- Telemetry is read-only data about the environment, usually collected through sensors. Each source of telemetry results in a channel. Telemetry data might be

preserved as a stateful variable on the device or in the cloud. Although each device might send only a single data point every minute, when user multiply that data by a large number of devices, user quickly need to apply big data strategies and patterns.

- Fig. 4.4.3 shows telemetry.

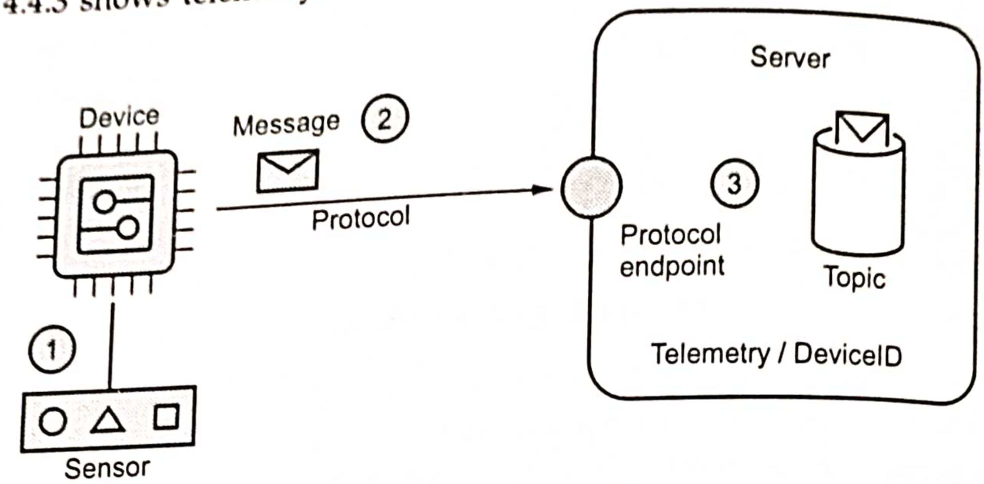


Fig. 4.4.3 Telemetry

1. The device obtains a measurement from a sensor operating in an environment remote from the IoT solution.
2. The device publishes a message to the message topic telemetry/deviceID containing the measurement. This message is sent via a transport protocol to a protocol endpoint made available by the Server.
3. The Server may then apply one or more rules to messages in order to perform fine-grained routing upon some or all of the message's measurement data. The routing can send a message to another component of the solution.

4.4.3.1 SCADA

- SCADA stands for supervisory control and data acquisition. Real-time industrial process control systems used to centrally monitor and control remote or local industrial equipment such as motors, valves, pumps, relays, sensors, etc. SCADA is combination of telemetry and Data Acquisition.
- SCADA is used to control chemical plant processes, oil and gas pipelines, electrical generation and transmission equipment, manufacturing facilities, water purification and distribution infrastructure, etc.
- SCADA generation :
  1. First generation : Early SCADA system computing was done by large minicomputers. Common network services did not exist at the time SCADA was developed. Thus SCADA systems were independent systems with no connectivity to other systems

2. Second generation : Distributed Systems. The system was distributed across multiple stations which were connected through a LAN.
3. Third generation : Networked Systems
4. Fourth generation : Internet of Things (IoT)

- Industrial Control Systems, like PLC (Programmable Logic Controller), DCS (Distributed Control System) and SCADA (Supervisory Control And Data Acquisition) share many of the same features. Industrial Control Systems are computer controlled systems that monitorand control industrial processes that existin the physicalworld.
- **Programmable Logic Controller** : A Digital Computer used for Automation and Control Applications. PLCs are suitable for Local Area Control (plants, production lines, etc.).
- Programmable Automation Controller : A Programmable Automation Controller (PAC) is a compactcontroller that combines the features and capabilities of a PC-based control system with that of a typical PLC.
- The SCADA system typically contains different modules, such as :
  1. OPC server
  2. A database that stores all the necessary data
  3. Control system
  4. Datalogging system
  5. Alarm system
- These modules are typically separate modules because they should be able to run on different computers in a network (distributed). Fig. 4.4.4 shows block diagram of SCADA.

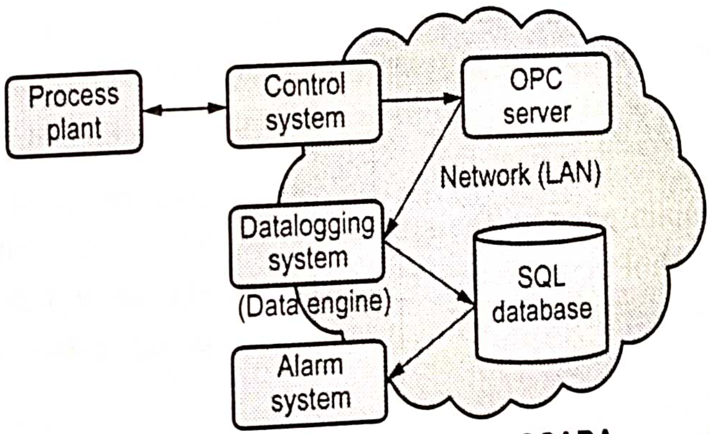


Fig. 4.4.4 : Block diagram of SCADA

- SCADA system usually includes signal hardware (input and output), controllers, networks, user interface (HMI), communications equipment and software. All together, the term SCADA refers to the entire central system. The central system usually monitors data from various sensors that are either in close proximity or off site.

- For the most part, the brains of a SCADA system are performed by the Remote Terminal Units (RTU).
- RTU is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA system. A RTU is a device installed at a remote location that collects data, codes the data into a format that is transmittable and transmits the data back to a central station, or master, e.g. a SCADA system.
- A RTU typically have analog and digital Inputs/Outputs. SCADA system will monitor and make slight changes to function optimally; SCADA systems are considered closed loop systems and run with relatively little human intervention.
- The data is transmitted through wireless medium over the internet to a database server where it can be analyzed and hosted in the web-site for general information. The system uses various sensors for detecting rainfall intensity and sensing the water level of the river. These data is first stored in a data logger, which supports CDMA transmission. The data is stored and transmitted at an interval of every minute so that the data can be logged.
- The three components of a SCADA system are : RTU, Master Station and HMI computer, communication infrastructure.
- The RTU connects to physical equipment and reads status data such as the open/closed status from a switch or a valve, reads measurements such as pressure, flow, voltage or current.
- Master station and HMI Computer(s) : The database server serves as the master station. It is responsible for communication with the field equipment (RTUs, PLCs, etc) and then to the HMI software running on workstations in control room or elsewhere.
- Communication infrastructure : The remote management or monitoring function of a SCADA system is often referred to as telemetry. This system implements CDMA protocols to transfer data over the internet.
- **SCADA on mobile phone :** The system allows you to use your mobile phone to monitor and control your process from any location. More versatile than a pager system. You can get detailed alarm messages about any event that occurs in your business.

SCADA Functionality :

1. Data acquisition and display : Store binary and analog data into process data base
2. Alarm and Events : Record important changes and operator actions
3. History data base : Keep a record of the process values

4. Measured processing : Calculate derived values (limit supervision, trending)
5. Logging and reporting
6. Human Machine Interface (HMI) : Graphical object state presentation, lists, reports
7. Operator Command handling : Binary commands, set points recipes, batches, scripts (command procedures)

- Fig. 4.4.5 show a typical SCADA middleware or platform architecture.

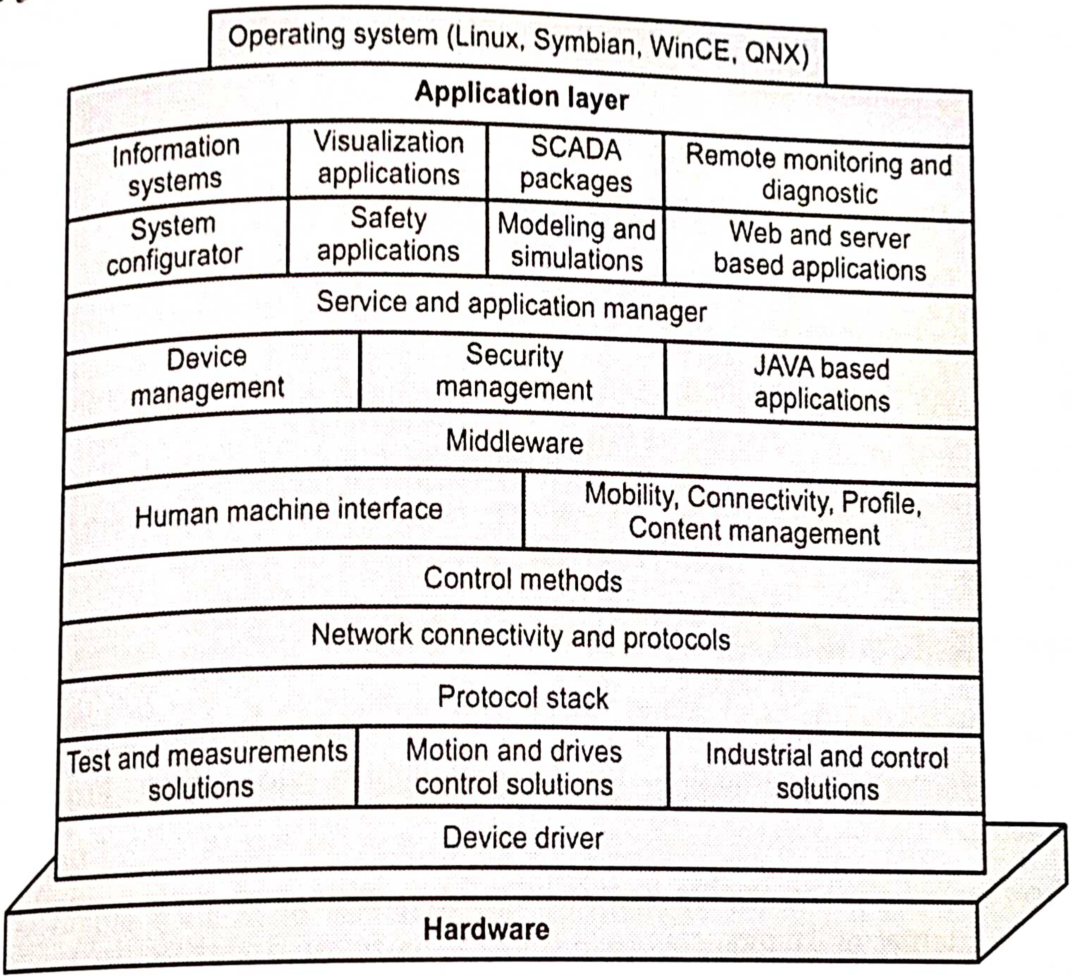


Fig. 4.4.5 : Middleware

- Middleware deals with the babble between distributed systems and has a similar objective in bringing linguistic or communication unity to disparate technological systems.
- Middleware is about integration and interoperability of applications and services running on heterogeneous computing and communications devices.
- The term middleware refers to a layer that is arranged on top of operating systems and communications stacks and thus hides heterogeneity from the applications through a set of common, well-defined interfaces.
- OLE for process control (OPC) middleware products are one of the important communications layer SCADA middleware that are designed to enhance any OPC standards-based applications. OPC is for windows only.

- WSN middleware is a kind of middleware providing the desired services for sensor-based pervasive computing applications that make use of a WSN and the related embedded operating systems or firmware of the sensor nodes.
- A complete WSN middleware solution should include four major components : Programming abstraction, system services runtime support and quality service (QoS) mechanism.

Benefits SCADA Systems Provide

a. Reduces operational costs

b. Provides immediate knowledge of system performance

c. Improves system efficiency and performance

d. Increases equipment life

e. Reduces costly repairs

f. Reduces number of man-hours (labor costs) required for troubleshooting or service

g. Frees up personnel for other important tasks

h. Facilitates compliance with regulatory agencies through automated report generating.

4.5 Home Automation

- Home automation is the automatic control of electronic devices in your home. These devices are connected to the Internet, which allows them to be controlled remotely.
- Interconnected devices enable to intelligently monitor and control smart homes in a future Internet of Things.
- Energy saving applications, for example, control indoor climate and electricity usage by employing context information to switch off appliances (e.g., lights, computers), reduce room temperature, close windows, or stop warm water circulation.
- Home automation works on three levels :
  1. **Monitoring :** Monitoring means that users can check in on their devices remotely through an app. For example, someone could view their live feed from a smart security camera.
  2. **Control :** Control means that the user can control these devices remotely, like planning a security camera to see more of a living space.
  3. **Automation :** Finally, automation means setting up devices to trigger one another, like having a smart siren go off whenever an armed security camera detects motion.

4.5.1 Smart Lighting

- Smart control the lights with automation signal system to save energy. Smart, connected lighting is the next - generation energy - efficient LED products with additional sensors to sense things such as occupancy and temperature.

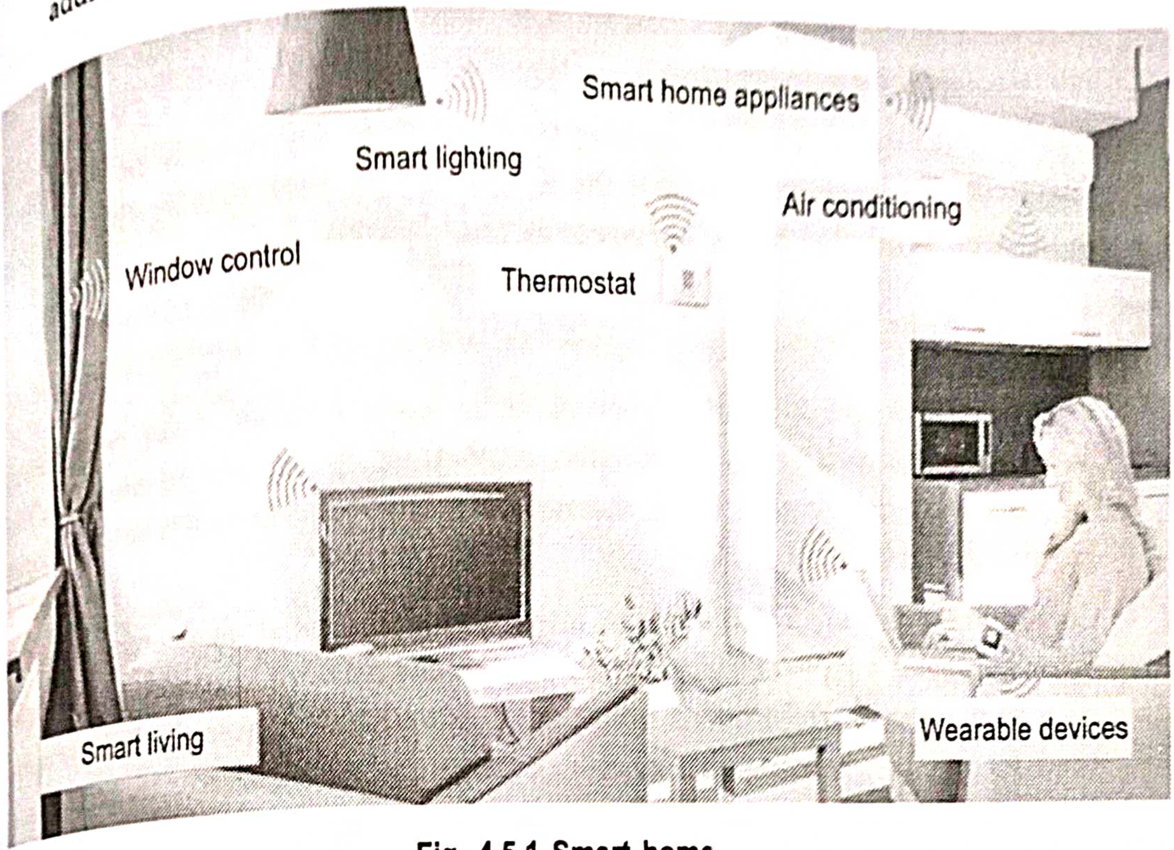


Fig. 4.5.1 Smart home

- In automatic light control system, Light Dependent Resistor (LDR) sensor is used to detect bright /medium /dim /dark conditions.
- It is simple enough to envision the addition of sensors and communications to create that initial concept of smarter, more adaptive lighting. If people are present, turn the lights on; if not, turn them off. Or use your smart phone to connect to the lighting system and tune it to the desired brightness level or to a particular color.
- Smart lighting is considered the one of the main solutions for energy reduction by means of controlling lighting level according to desired need with minimum energy consumption.
- Smart - lighting systems utilize motion and light sensors for performing the control algorithms.
- The system uses motion and light sensors for detecting the surrounding environment. There are lamps controlled with the specific lighting level in order to supply the adequate amount of lighting required without affecting the user visibility.

- Certainly the required lighting level is strongly dependent on the weather conditions. In clear weather at night might require more luminance than cloudy one, due to the reflection from the clouds.
- While during mist and foggy weathers require the highest possible lighting level, as the visibility reaches its lowest. On snowy weather it might require an intermediate level between clear and foggy.
- During night it requires high lighting levels, while at day it needs just fade level to provide guidance or turn off if the weather is clear. The lighting concentration in the yard is affected by the above conditions.

4.5.2 Smart Appliances

- The role and scope of smart appliances in the home (Washer, dryer, refrigerator, dishwasher, fridge, freezer, air conditioner, vacuum cleaner and so on) is on the increase with the market being estimated to have a year on year compound growth of slightly over 15 %.
- Connecting everyday objects to the internet is an essential element of the IoT. Some appliance suppliers use a low power wireless network to communicate over such as bluetooth, whilst others utilise the existing higher powered Wi-Fi network used for a tablet or computer wireless connectivity. Once a network is in place objects can populate the home environment and communicate with the user and each other.
- The ability of an object to respond to remote commands and change its behaviour makes it an active device, such as the new Hive heating thermostat or a Sky+ box.
- Where the remote object has no ability to respond to remote control requests then it is considered passive as with some fixed cameras, microphones or temperature sensors.
- IR Sensor : It will be activated in the automated mode to detect person entering or coming out of the room and set a counter based on that. If the counter show there is a person inside it will light up the room automatically and turn on the AC depending upon the temperature reading.
- Sensors provide data about motion, occupancy, glass breakage, door and window openings, water leaks, light intensity, temperature, energy consumption, camera, and even appliance plug insertion or removal.
- Controllers turn power on and off or adjust settings on appliances, furnaces, air conditioners, space heaters, fans, pool pumps, water heaters, lighting, home theatres, music, motorized blinds, door locks, and plug loads.

- To be deemed intelligent, an appliance's sensors and controllers should use internet protocol communication.
- Smart refrigerators can keep track of the items stored and send updates to the users when an item is low on stock.
- Smart TV allow user to search video and movies from the Internet on a local storage drive, search TV schedule, fetch news and other things from the Internet.
- OpenRemote is the professional open source middle-ware for an Internet of Things. Integrate any device or protocol, and design your own user interface and automation. Use our online designer, sync to the controller, and control with this app.
- OpenRemote is a state of the art open source software platform for building control and automation.
- OpenRemote allows for designing a fully customizable building and home control solution without the need to actually write code.

4.5.3 Intrusion Detection

- Intrusion Detection System (IDS) includes both hardware and software mechanisms and IDS is responsible for identifying malicious activities by monitoring network environment and system.
- The purpose of home intrusion detection system is to detect intrusions using sensors and raise alerts, if necessary.
- With the help of Light dependent resistor and PIR motion sensor, it detect the motions in the room. If a motion is detected, system capture the image with the help of a webCam and store locally. Now the alerts are sent to the user with the captured image.
- Fig. 4.5.2 shows block diagram of intrusion detection.

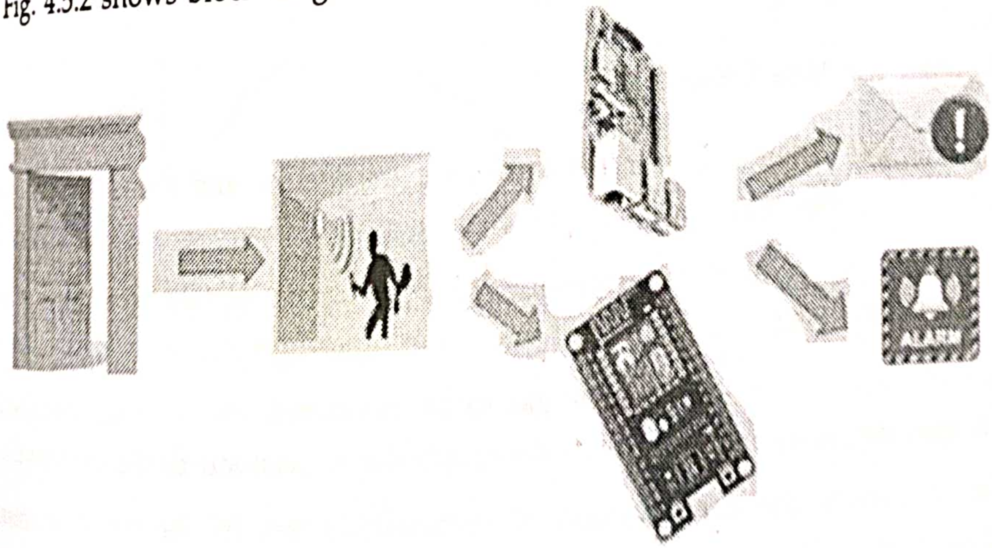


Fig. 4.5.2 Block diagram of intrusion detection

- To detect any form of intrusion in restricted areas and report it immediately, following concept is used.
  1. A PIR sensor is required to detect the presence of any human being in the room.
  2. An RFID is required to validate the presence of the person in the room by tallying his identity with those in the database.
  3. A camera is required to click the picture of the room and send it via email as an alarm.
  4. An internet connection is required to register all these movements on a website so that it can be accessed from any place and any device.
- The different input / output devices are controlled using TCP/IP over the IEEE 802.11 standard protocol. Data being gathered from sensors, such as PIR sensors, temperature sensors, IR transmitter and receiver is being processed on micro - controller as a server.
- Passive Infrared Sensor (PIR) Sensor : PIR sensor is an electronic sensing device that senses infrared (IR) light emitted from entities in its field of view and used to detect motion in its range. It is activated only in the security mode to detect any unwanted motion at the entrance. If any unwanted movement is detected then it will signal the microcontroller to take necessary steps.
- Alarm : It will only be activated in the security mode when some intruder is detected by the PIR motion sensor.
- Cloud controlled intrusion detection is possible by using location aware services. Here geo - location of each node is independently detected and stored in the cloud.
- Some intrusion detection system uses UPnP technology. It is based on image processing to recognize the intrusion.

4.5.4 Smoke for Gas Detection

- Smoke or gas detector sensor which detects the smoke and turns on the buzzer alarm and all these are update on the web page.
- MQ2 is a semiconductor type sensor, which can appropriately sense the presence of smoke, LPG, methane, butane, propane and other hydrocarbon.
- When it comes in contact with the gas to be monitored, the electrical resistance of the sensor decreases; enabling the microcontroller to respond to the situation.
- When it detects the concentration of combustible gas in the air it outputs its reading as an analog voltage. The sensor can measure concentrations of flammable

gas of 300 to 10,000 ppm. The sensor can operate at temperatures from 20 to 50° C and consumes less than 150 mA at 5 V.

- The MQ-2 smoke sensor reports smoke by the voltage level as output. The more smoke is there, the greater the voltage output. The MQ-2 also has a built-in potentiometer to adjust the sensitivity to smoke.
- By adjusting the potentiometer, one can change how sensitive it is to smoke, so there is a form of calibrating it to adjust how much voltage it will give in relation to the smoke it is exposed to.

4.6 Smart City

- The number of urban residents is growing by nearly 60 million every year. In addition, more than 60 percent of the world's population will be living in cities by 2050.
- Fig. 4.6.1 shows concept of smart city.

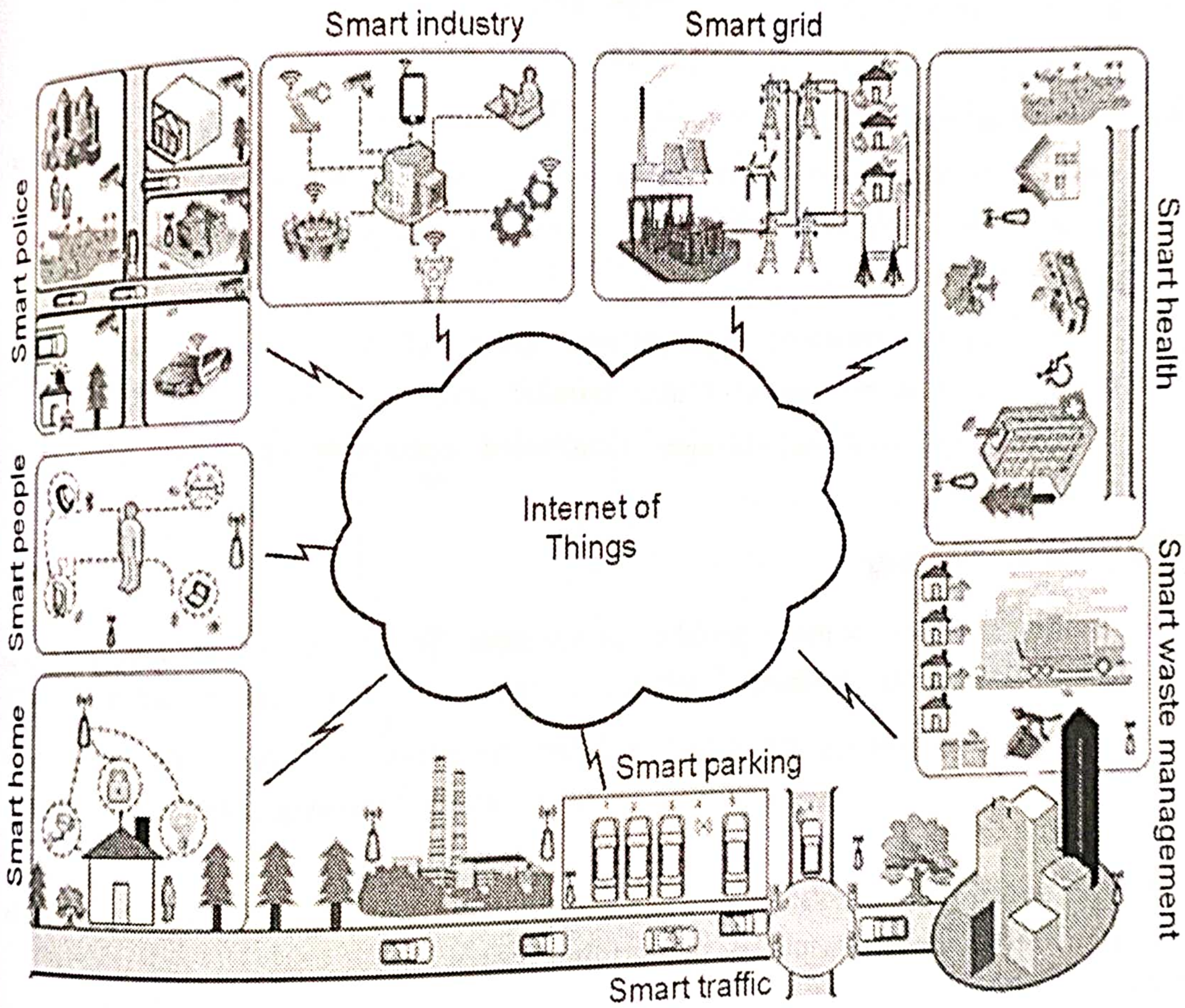


Fig. 4.6.1 Smart city

- As a result, people occupying just 2 percent of the world's land will consume about three-quarters of its resources. Moreover, more than 100 cities of 1 million people will be built in the next 10 years.
- Over the past decade, the city of Amsterdam, the Netherlands, has developed a vision for collaborating, envisioning, developing, and testing numerous connected solutions that could pave the way to a smarter, greener urban environment.
- Smart city includes :
  1. Smarter management of city infrastructure using big data analytics
  2. Collaboration across multiple and disparate agencies using cloud technologies
  3. Real - time data collection, enabling quick response using mobile technologies.
  4. Enhanced security : Improved public safety and law enforcement, and more efficient emergency response.
  5. Better city planning improved schematics, project management and delivery
  6. Networked utilities smart metering and grid management.
  7. Building developments more automation, and better management and security.
- With smart city applications producing continuous large data from heterogeneous sources, existing relational database technologies are inadequate to handle such huge amounts of data given the limited processing speed and the significant storage expansion cost.
- To address this problem, big data processing technologies, which are based on distributed data management and parallel processing, have provided enabling platforms for data repositories, distributed processing, and interactive data visualization.

4.6.1 Smart Parking

- Traffic congestion is major problem in big cities. Searching for a parking space is a routine (and often frustrating) activity for many people in cities around the world.
- After finding parking space to the driver, he parks the vehicle, it maybe spend small amount of time to looking for a city council parking attendant to pay the parking fees.
- The smart parking system is designed by making use of some IOT supportable hardware's such as raspberry pi, auridino boards etc.

- Smart parking systems typically obtains information about available parking spaces in a particular geographic area and process is real - time to place vehicles at available positions.
- It involves using low-cost sensors, real-time data collection, and mobile-phone-enabled automated payment systems that allow people to reserve parking in advance or very accurately predict where they will likely find a spot.
- When deployed as a system, smart parking thus reduces car emissions in urban centers by reducing the need for people to needlessly circle city blocks searching for parking.
- It also permits cities to carefully manage their parking supply smart parking helps one of the biggest problems on driving in urban areas; finding empty parking spaces and controlling illegal parking.
- Smart parking application can be accessed by drivers from smart phones, tables. Sensor is used for each parking slot, to detect whether the slot is empty or occupied.
- Local controller collect the information and send to server using Internet. Fig. 4.6.2 shows process specification for smart parking IoT system.
- Each parking slot contains the sensor and it reads at regular intervals. Sensor sends the status information to local processing centre.

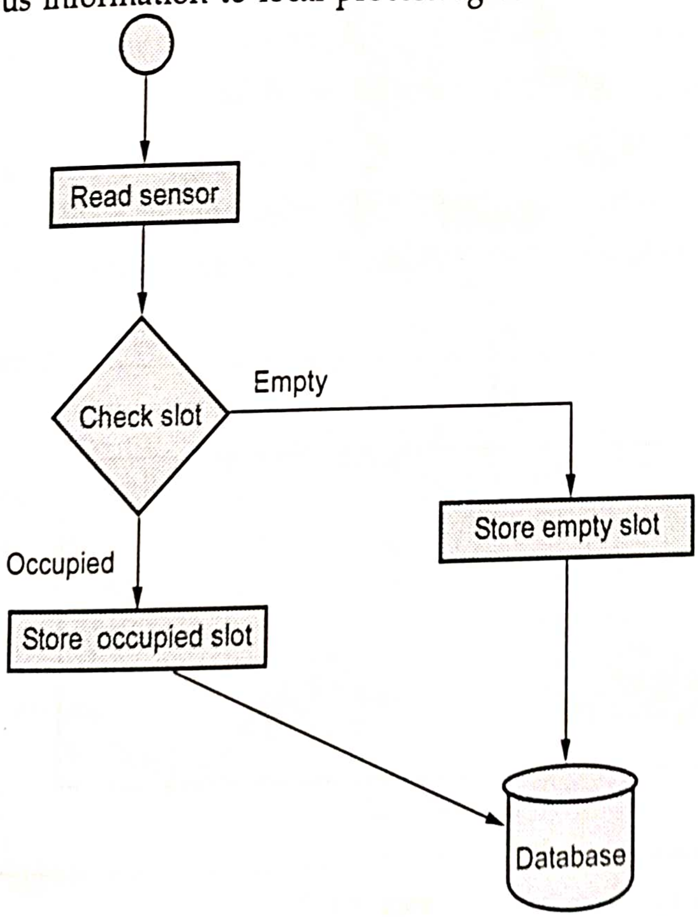


Fig. 4.6.2 Process specification for smart parking IoT system

- Fig. 4.6.3 includes four layers : A sensing, networking, middleware and application layer.

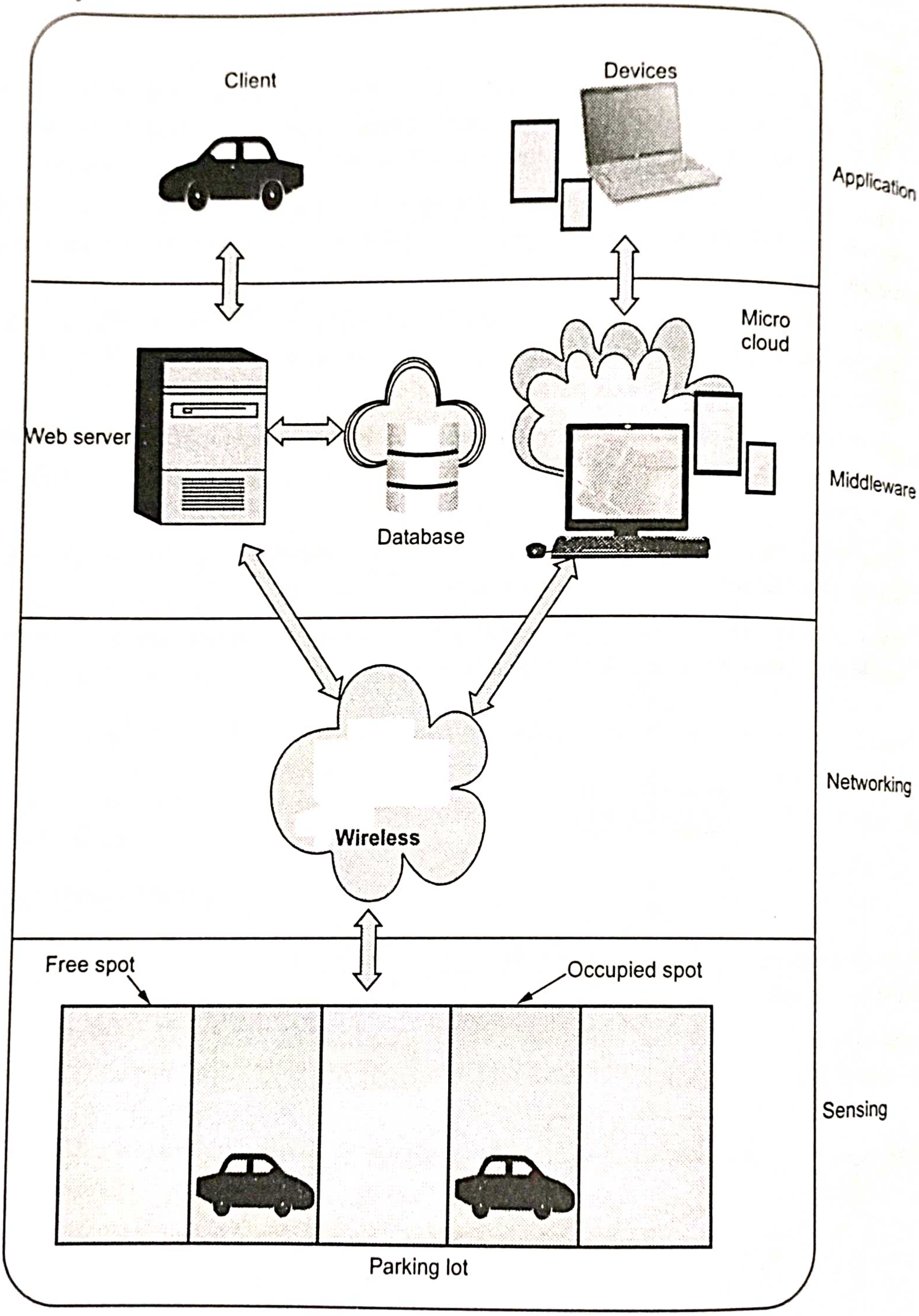


Fig. 4.6.3

- Sensing layer defines a platform where sensor devices are embedded into the parking lot to detect car presence/absence, and RFID devices located at the parking gates and strategic points of the parking are used to identify cars based on a unique mapping between RFID tags and car.
- Networking Layer : TCP/IP over Ethernet for connecting the gateway to the parking server and database and Internet access for remote access to the smart parking system from outside.
- Middleware layer hosts different databases and associated servers and manages all of the software intelligence provided by the smart parking system to provide smart services to users by enabling communication between the application layer where services are requested and the lower layers where smart devices are embedded into the parking lot to provide smart services.
- The application layer is the layer where the different services are defined and provided to different users. Client devices have been connected via the TCP/IP protocol to a parking database.
- Parking availability status by integrating into the car detection system sources of light on parking spots, which are controlled by actuators to inform of the status of a parking spot : e.g., red for occupied, green for empty, yellow for reserved and blue for out of service.
- Remote availability checking using the Internet and/or the GSM network to check in real time the availability of the smart parking system.
- The data of smart parking lots are able to provide profits for both customers and merchant's daily lives in the smart cities. This service works based on road sensors and intelligent displays which lead drivers to the best path for parking in the city.

4.6.2 Smart Lighting

- The street lighting is one of the largest energy expenses for a city. The street light section comprises of all the light lamps in an area with current sensors and RF module. 'N' street lights of this section communicates with local controller unit wirelessly through RF module (Zigbee). 'N' local controller unit communicates with main server through IoT due to its global coverage area.
- Smart light infrastructure is the backbone of the IoT in smart cities. Smart and wireless street light luminaries can act as service gateways for other street level IoT devices.
- Smart street lights are intelligent lights that gather dynamic data i.e. data that keep changing dynamically by time, through some sensors and generate required information for the request claimed by a citizen on road.

- Smart street light saves energy by sensing the surrounding through their sensors expecting some other sensor in some other device.

4.6.3 Smart Roads

- Sensor is installed on road to provides road traffic condition, travel time estimation, congestion and accident.

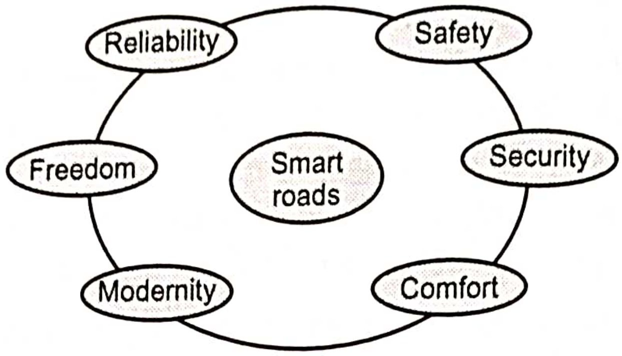


Fig. 4.6.4 Smart roads characteristics

- Sensor collect this information and stored on the central database using cloud. This information helps for solving traffic congestion, making safe driving, keeping road condition upto date.
- User can access the information from the cloud. User also get real time information.
- Real time traffic maps can be obtained to enable smooth flow. Traffic can be reduced with systems that detect alternate routes. User get timely information so they can locate a traffic free road, saving time and fuel. This information can reduce traffic jams and pollution improves the quality of life.

4.7 Logistics

4.7.1 Route Generation and Scheduling

- Modern transportation system collects data from various places and multiple sources. Collected data is processed and decision is taken according to this. This information is also provided to stakeholders.
- Data driven transportation system is provided by using this data.
- Route generation and scheduling system can generate end to end routes using combination of route patterns and transportation modes.

- Cities around the world face common transport challenges - from increasing congestion, safety concerns and aging infrastructure to a lack of funding and increasing environmental impacts. Like their colleagues in city administration and government, transport officials are starting to implement "smart solutions" to address these challenges and provide improved mobility in their cities, better services for citizens and a more cost-effective transport network.
- Vehicle networking : Utilizing the new technologies, such as wireless communication, positioning and navigation, context awareness, to implement the connections between vehicle to vehicle, vehicle to man, vehicle to infrastructure, so that the integrated service can be provided.
- The Internet of Vehicles (IoV) is an integration of three networks : an inter-vehicle network, an intra-vehicle network, and vehicular mobile Internet.
- The application of IoT technology in providing information services, improving traffic efficiency, enhancing traffic safety, implementing supervision and control and other aspects will make millions of people enjoy more comfortable, convenient and safe traffic service.

4.7.2 Fleet Tracking

- It is automated vehicle routing and scheduling. It supports driver compliance, safety and performance reporting.
- Vehicle fleet tracking system uses GPS technology to track the location of the vehicle in the real time.
- Fleet maintenance and fuel conservation capabilities. Track, schedule and route vehicles in real time.
- Proactively manage fleet maintenance and fuel economy. It is also possible to monitor driver behavior and performance (distance traveled, speed, location).

Benefits :

a) Accelerate delivery and dispatch rates.

b) Improve customer satisfaction.

c) Reduce fuel consumption and vehicle maintenance costs.

d) Ensure compliance with government and industry regulations.

e) Improve fleet productivity, uptime, and safety.

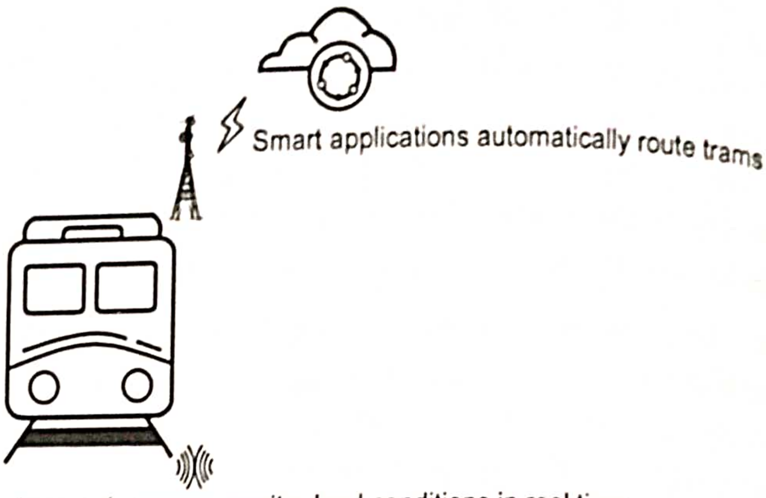


Fig. 4.7.1

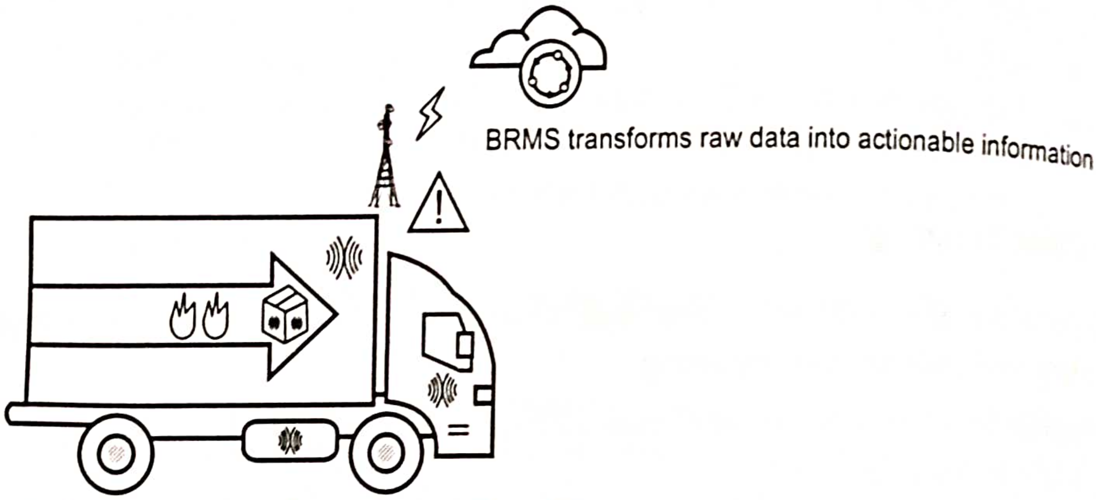


Fig. 4.7.2

4.7.3 Shipment Monitoring

- Shipment monitoring system is used by transportation system for monitoring the goods condition inside the containers. Fresh foods are transported from one place to another place so to prevent spoilage of food, IoT helps by monitoring.
- Fresh food can be damaged during transit due to unrefrigerated conditions and changes in environmental conditions such as temperature and humidity
- This monitoring system uses different types of sensors like temperature sensor, pressure sensor, humidity etc. These sensor collects the information from the container and send to the cloud. These information is processed to detect food spoilage.
- Required action will be taken after processing. It avoids food poisoning and financial loss of transporter.

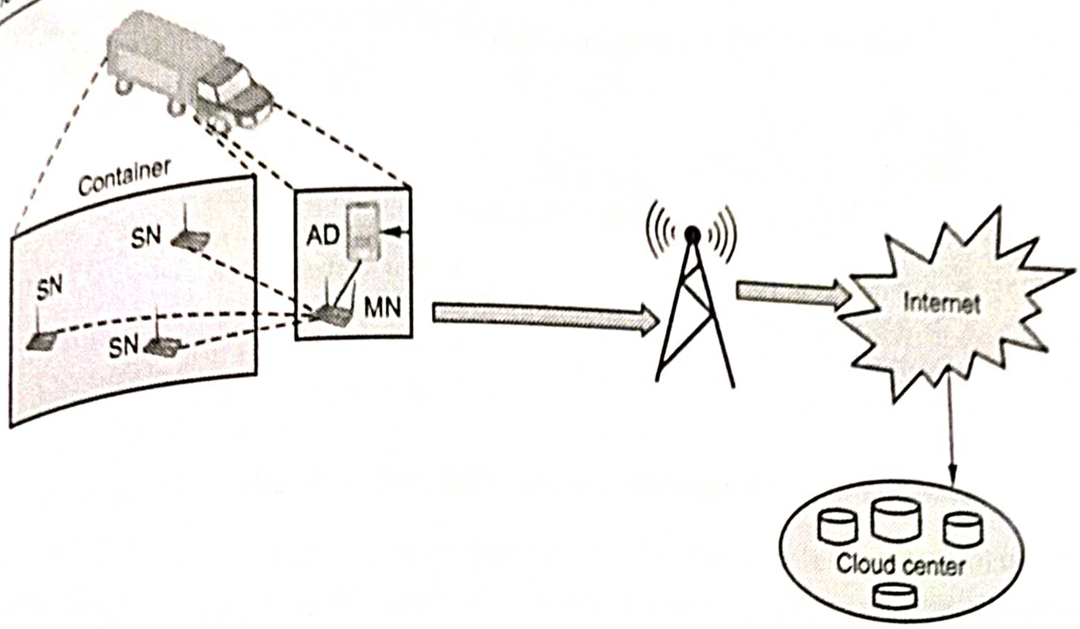


Fig. 4.7.3 Shipment monitoring system

4.7.4 Remote Vehicle Diagnostics

- Remote Vehicle Diagnostics Solution monitors the health of the vehicle, determines the root cause of the problem / failure and provides real time information of vehicle parameters to assess its performance against benchmarks.
- The solution monitors the health of the electric vehicle, commercial vehicle, utility vehicle and provides insight to field support staff to determine the root cause of the problem. It also enables the customers to access information about the vehicle. Commercial / Utility vehicles being driven across the country extensively over time for various purposes are in need of a diagnostic check which is automated through the offering.
- By monitoring all the aspects of the car is easier to detect any problem in advance by sending all sensor readings to a certified center where technicians and engineers will apply their expertise to find and predict imminent failures of key systems integrated in the vehicle.
- Modern commercial vehicles support on board diagnostic standard. Next generation vehicles will have sophisticated on-board connectivity equipment, providing wireless network access to the vehicle for infotainment and other telematics services. Fig 4.7.4 shows remote vehicle diagnostics.
- In vehicle, sensors connect to the vehicle terminal which is responsible for collecting, storing, processing and reporting information, and responding to commands from supervision platforms.

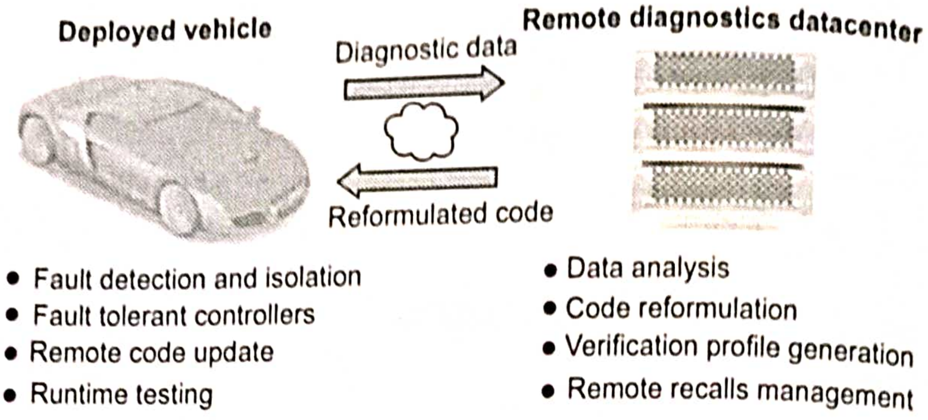


Fig. 4.7.4 Remote vehicle diagnostics solution

- The vehicle terminal consists of the microprocessor, data storage, GPS module, wireless communication transmission module, real time clock and data communication interface.

4.8 Retail

4.8.1 Inventory Management

- Retail involves the sale of goods from a single point (malls, markets, department stores etc) directly to the consumer in small quantities for his end use.
- Retail is a challenging business but the pressures of today's economic conditions are resulting in even more selective consumer shopping and spending.
- The effect of internet of things on inventory management is the next huge thing in progress when it comes to Business Process Management (BPM).
- In any typical business, the process of ordering, storing, tracking and managing good is a day to day requirement. As with all high investment top-tier businesses, this process becomes more complex with increasing amount of supply and demand.
- This process involves huge transaction of monetary resources and hence it is impervious that a high preference is given to this in a BPM. Inventories that are mismanaged can create significant financial problems for a business, leading to a inventory shortage.
- Existing technologies such as bar coding and Radio-Frequency Identification (RFID) already let retailers monitor their inventories.
- IoT will enable this to be taken to the next level with significantly more data coming in the monitoring systems and products moving through the supply chain.

- This can considerably improve supply chain efficiencies and enable leaner inventories. Large retailers such as **Walmart** are already using IoT for supply chain and inventory management.
- Tracking is done using RFID readers attached to the retail store shelves .

4.8.2 Smart Payments

- Smart payment system uses Near Field Communication (NFC) and Bluetooth communication.
- Near Field Communication (NFC) technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart.
- NFC operates at 13.56 MHz and transfers data at up to 424 kbits/second.
- NFC is available as standard functionality in many mobile phones and allows consumers to perform safe contactless transactions, access digital content, and connect electronic devices simply.
- An NFC chip in a mobile device can act as a card or a reader or both, enabling consumer devices to share information and to make secure payments quickly.
- Using smart phone applications, payments can be made using a simple tap or waving the card within the proximity.
- Service providers can integrate payment option into smart phones using an NFC tag embedded inside the device. Apple pay, Google wallet (Android pay) and Samsung pay are the most popular among smart phone payment systems.
- Data transfer using smart device are possible using NFC technology like Android beam. Two users can share documents, photos, resumes and business cards by just waving their smart phone.

4.8.3 Smart Vending Machines

- Smart vending is about building remote management systems and telemetry tools, which integrate monitoring, transmission and delivery of operational data from each vending machine via the Internet.
- Smart vending solution offers its customer's flexible payment options and monitors the machines remotely and in real time.
- Smart phone applications that communicate with smart vending machine allow user preferences to be remembered and learned with time.
- For instance, Innovations like RFID based "smart" shelves continuously scan items on the shelf and notifies the appropriate systems. During low or out of stock

situations they create automatic replenishment alerts and send automatic orders directly to central warehouse and to manufacturers.

- Smart vending machine provided following :
  1. Achieve high levels of efficiency in the management of their assets.
  2. Offers its customer's flexible payment options : RFID/NFC Card; - Mobile Payments; - Smartphone payments; Cash; Debit and Credit Card.
  3. Monitor the machines remotely and in real time.
  4. Simplifies business since the vending machines contain multiple sensors that alert the owners about their location, the state inventory and eventual maintenance issues.

4.9 Industry

4.9.1 Machine Diagnosis and Prognosis

- Machine fault diagnostic and prognostic techniques have been the considerable subjects of condition-based maintenance system in the recent time due to the potential advantages that could be gained from reducing downtime, decreasing maintenance costs, and increasing machine availability.
- A failure in industrial equipment results in not only the loss of productivity but also timely services to customers, and may even lead to safety and environmental problems.
- IoT play an important role in both diagnosis and prognosis. Critical manufacturing processes and equipment must be continuously monitoring for any variations or malfunctions. A slight shift in performance can affect overall product quality or manufacturing equipment health.
- With group of sensing nodes monitoring various manufacturing equipments and processes and transmitting data in periodic manner, situations may arise where the engineer might want to query data from some specific nodes to estimate current status of particular process or equipment.
- There can be situation of unforeseen malfunctioning or variations beyond prescribed tolerance bands. A mechanism is hence required to define tolerance bands for each sensing module. When measurements at particular node exceed the tolerance, the node must breach the periodic cycle to send an alarm about the emergency.
- Case Based Reasoning (CBR) is normally used method to find solution to new problems based on previous experience.

- CBR is an effective method for problem solving for quantitative mathematical model i.e. machine diagnostic and prognosis.

4.9.2 Indoor Air Quality Monitoring

- To work in healthy environment in factory, indoor air quality is monitored. Factory provides safety environment to workers.
- Generating harmful gases (CO, NO and NO_2) in the factory, creates problem for workers. To avoid this, sensor is used to monitor/sense the air quality of room. Various gas sensor are used by factory for controlling air quality.
- Air quality is measured at different locations. Anything serious happen or threshold level of air quality is changed, sensor send alert to authority and it also give the alarm.

4.10 Next Generation Kiosks

- A kiosk is a small, stand-alone booth typically placed in high-traffic areas for business purposes. It typically provides information and applications on education, commerce, entertainment, and a variety of other topics.
- When considering the hardware to manage Kiosk, following points are considered :
  a) Remote access : the ability to access Kiosks remotely, it allows to manage the kiosks without spending any additional time or money sending someone out to the field.
  b) Display : with screen resolution always improving, organization want to ensure that, display output can at minimum handle 4K resolution.
  c) External devices : some kiosks such as ones used for pay stations and self-service ordering require the integration of a credit card reader.
  d) Software compatibility : Some kiosks run multiple software applications and also want to ensure that the hardware running in kiosks is compatible with the major operating systems.
- Fig. 4.10.1 shows kiosks.
- Types of kiosks.
  1. Touch Screen Kiosks : This is a stand-alone device that features a touchscreen interface and uses highly advanced programming software. Such kiosks are often used in the retail or consumer industry, and are placed in high traffic areas where people can get information with the touch of a finger.
  2. Internet Kiosks : These kiosks offer internet access to the public. They are usually installed at the airport, hotel lobbies, or apartment offices.

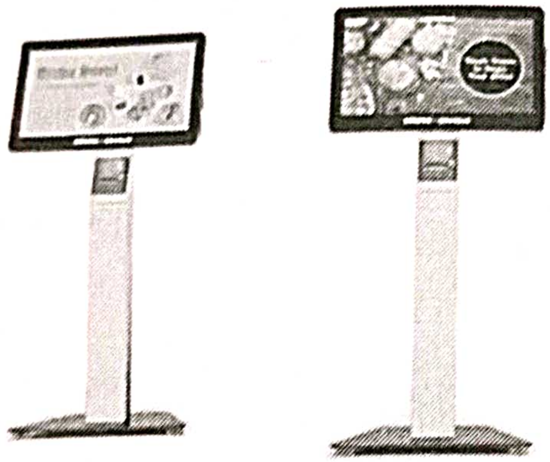


Fig. 4.10.1 Kiosks

3. Photo Kiosks : Some of the most common types of photo kiosks are instant print stations, digital order stations, movie ticketing, DVD vending, building directory and public transport ticketing kiosks.

- A successful self-service kiosk implementation incorporates traditional interaction with customers as well as the digital interaction provided by the kiosk. Additionally, self-service kiosks can be tailored to many forms, including standing kiosks and ruggedized tablets in bolted bases. The way they are implemented depends on the unique needs of a business.
- Kiosks includes following parts :
  a) Central Processing Unit (CPU) : The machine that allows software applications to work.
  b) Components : This allows the kiosk to be customized. They assist with the functionality of the kiosk. They include card readers, barcode scanners, receivers, etc.
  c) User interface (UI) : The UI allows the user and software to connect. It can be a touch screen or keyboard or any other device that enables the user to interact with the machine.
  d) Enclosure : This is the outer shell of the kiosk that holds the computer, components, display and all other internal elements of the kiosk.

4.11 Cellular IoT Connectivity Services

- Cellular IoT is the technology that connects physical objects to the Internet utilising the same cellular network currently used by smartphones. In other words, this technology can connect IoT devices using existing mobile networks. Thus, it eliminates the need to invest and develop a separate dedicated network infrastructure just for IoT devices.

- Cellular networks connect iPhone to Google Maps, Instagram, and Email; they carry user voice through the air. Cellular IoT provides an alternative to low power, wide area networks like the non-cellular LoRaWAN and Sigfox technologies, which operate in unlicensed bands.
- Cellular networks capable of facilitating massive flows of data. New cellular-enabled sensors can transfer reasonable amounts of data across considerable distances without draining the battery.
- The idea behind Cellular IoT enablement is to use cellular networks, including 3G, 4G/LTE or 5G, for connecting devices like streetlights, agricultural, and healthcare equipment.
- Fig. 4.11.1 shows types of cellular IoT.

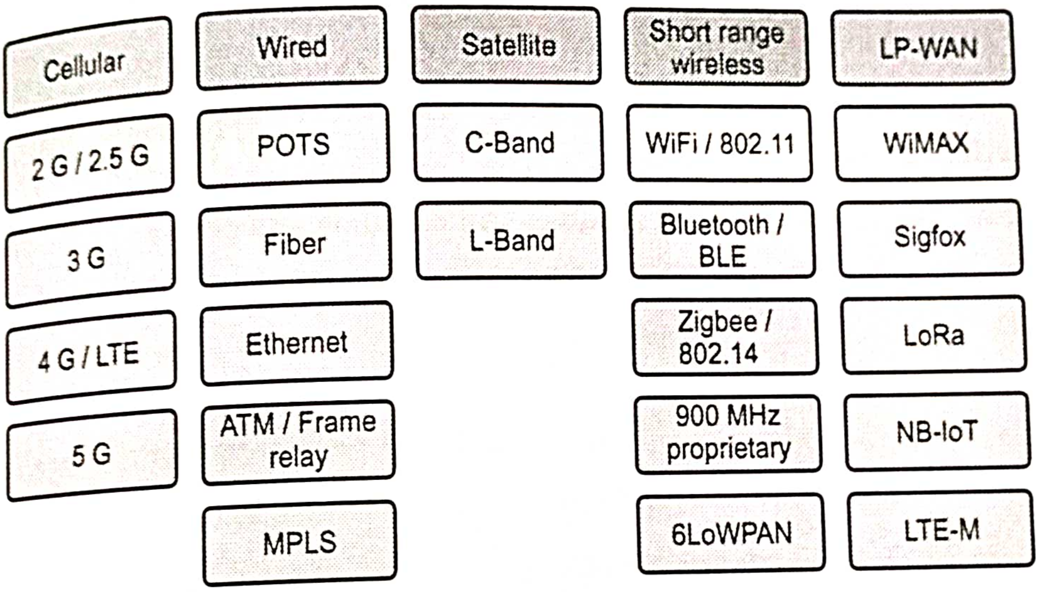


Fig. 4.11.1 Types of cellular IoT

- Two key technologies of cellular IoT : LTE-M and NB-IoT.
- While 2G/3G protocols are perfectly adequate for many IoT applications, modern IoT generally relies on LTE-M or NB-IoT.
- **LTE-M stands for "Long-Term Evolution for Machines"** and allows for IoT devices to piggyback on existing LTE networks. It was designed in a power-conscious manner for applications that require low-to-medium data throughput.
- With a bandwidth of 1.4 MHz, LTE-M provides great range but less throughput than LTE. The LTE-M also offers cell tower handoff features, making it a great mobility solution. Asset tracking, wearables, home security, and home/business monitoring are all great examples of use cases for LTE-M in the IoT.

- NB-IoT stands for "Narrowband-IoT" and is great for areas without robust LTE coverage or when bandwidth requirements are relatively minimal. It uses just a narrow band of the full bandwidth available.
- NB-IoT devices consume very little power and provide less data throughout than LTE-M. Compared to LTE-M's bandwidth of 1.4 MHz, NB-IoT operates on 200 KHz, providing longer range and better indoor penetration.
- Certain use cases like smart cities, parking garages, indoor deployments, and agricultural settings are great examples of suitable NB-IoT implementations.
- Benefits
  a) Coverage : Cellular networks are ubiquitous, mature, and reliable.
  b) Global reach : There is no other network technology with the reach of cellular.
  c) Security : SIM-based authentication and utilization of VPN tunnels makes cellular the most secure option.
  d) Installation : Works out-of-the-box without requiring local installation or technical expertise.
  e) Low/No power : Cellular modules can consume less power.