Unit III

4 Introduction and IOT Technologies behind Smart and Intelligent Devices

4.1 : IoT Concepts

Q.1 Define IoT. Explain characteristics of IoT.

Ans. : • 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.

- The internet of things refers to the capability of everyday devices to connect to other devices and people through the existing internet infrastructure.

Characteristics of IoT :

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.

Q.2 Demonstrate the IoT component with a neat diagram.

☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. : Fig. Q.2.1 shows IoT components.

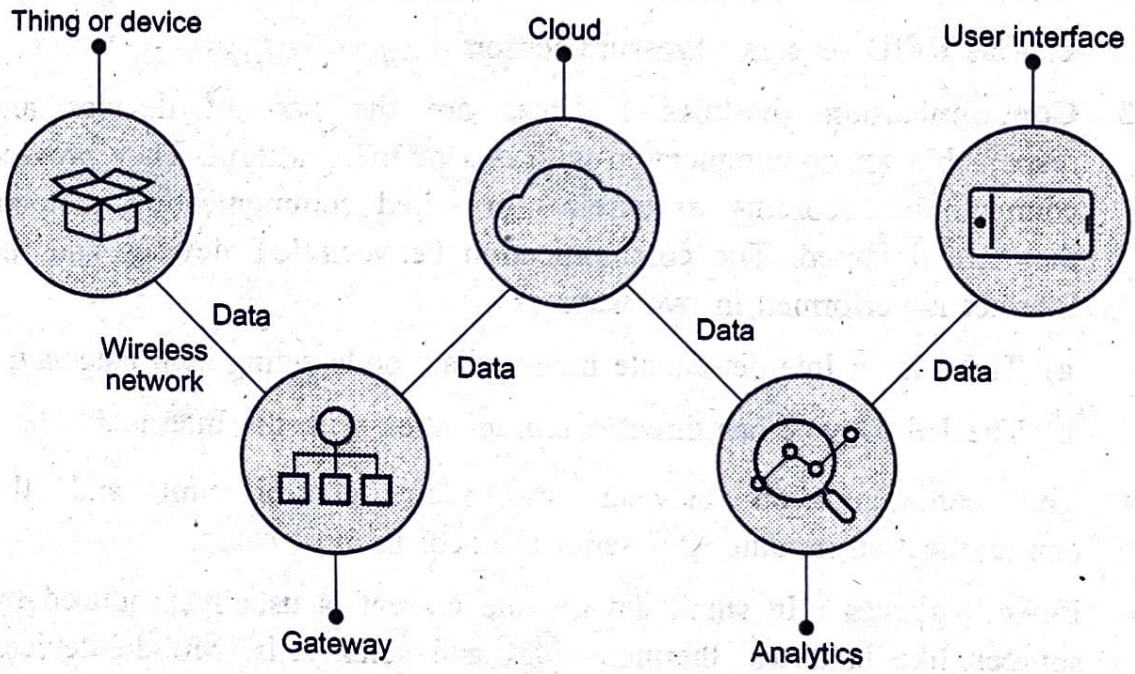

Fig. Q.2.1 IoT components

- 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.

Q.3 Explain working of IoT.

Ans. : 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.

- Fig. Q.3.1 shows working of IoT.

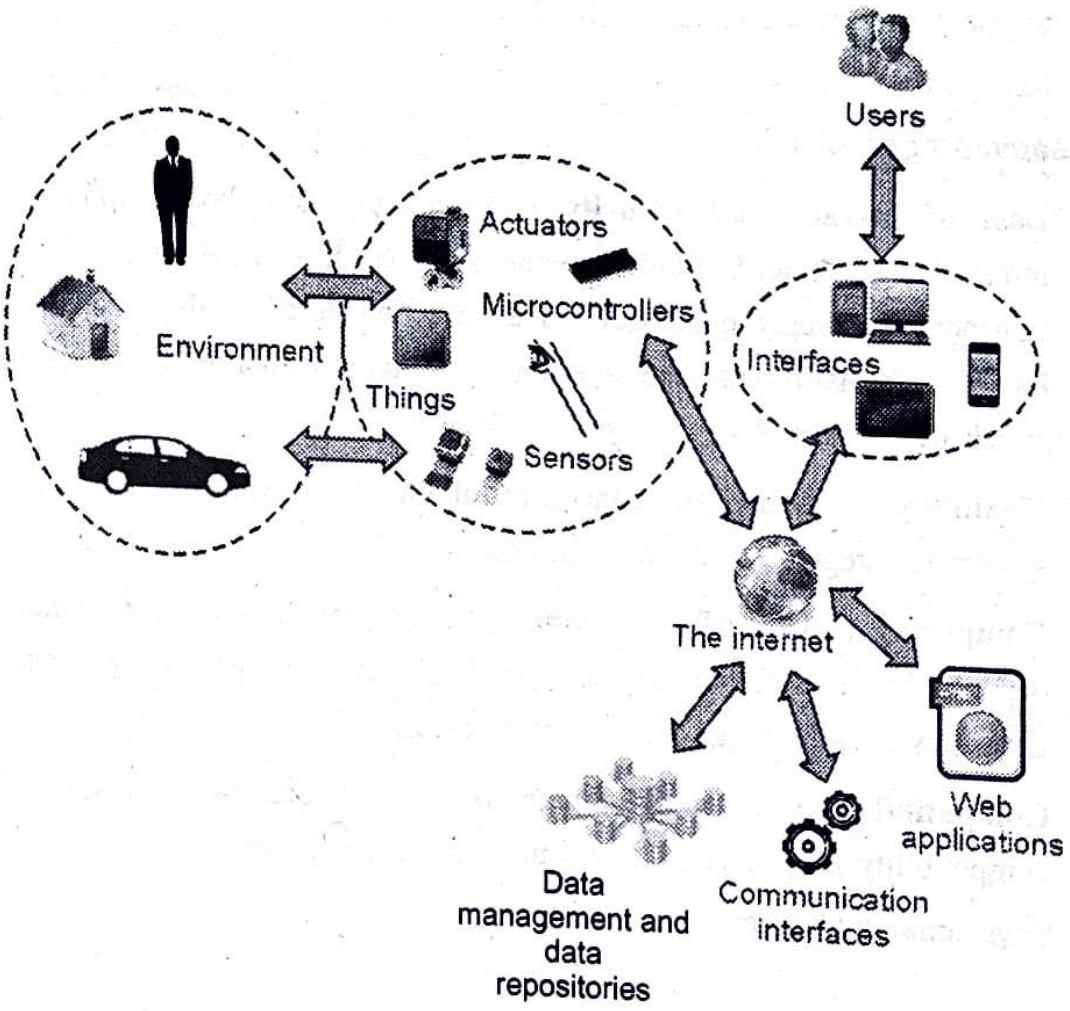

Fig. Q.3.1 Working of IoT

- 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.

Q.4 Explain advantages, disadvantages of IoT.

Ans. : 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.

Q.5 Define IoT. Explain any one application of IoT.

Ans. : Applications of IoT :

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.

Q.6 Describe an example of an IoT system in which information and knowledge are inferred from data.

Ans. : • A weather monitoring system where sensors sends raw data values, for humidity and temperature. Context is added to the data in form of tuples.

- This gives us information and knowledge can be obtained by continuous monitoring of the sensor data and adding alerts if the values exceeds a certain threshold.
- Another examples of IoT system in which information and knowledge are inferred from data is SMART HOME and SMART GRID.

Q.7 Write a short note on 5A and 3I characteristics of IoT.

Ans. : • 5A and 3I characteristics of the Internet of Things is anywhere, anytime, anyway, anything, anyhow and instrumented, interconnected, intelligently.

- To achieve such 5A and 3I capabilities, some common, horizontal, general-purpose technologies, standards and platforms, especially

middleware platforms based on common data representations just like the three-tiered application server middleware, HTML language and HTTP protocol in the Internet/web arena, have to be established to support various vertical applications cost effectively and new applications can be added to the platform unlimitedly.

- Most of the vertical applications of IoT utilize common technologies from the networking level and middleware platform to the application level, such as standard wired and wireless networks, DBMS, security framework, web-based three-tiered middleware, multitenant PaaS, SOA interfaces, and so on.

Q.8 Why do IoT systems have to be self adapting and self configuring ?

Ans. : • Internet of Things (IoT) can be considered a highly dynamic and radically distributed networked system, composed of a very large number of smart objects producing and consuming information.

- The main challenges associated with the IoT paradigm are : Dealing with rapidly changing environment, heterogeneity of devices forming the network and the lack of human capacity in managing those devices. These challenges cause increasing uncertainty at design-time about the operational context of devices in their run-time.

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.
- IoT devices may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions.

Self-configuration :

- The system is capable to readjust itself. Readjustment of the system is required if its environment changes or to reach an objective set for the system.
- Self-configuration primarily consists of the actions of neighbor and service discovery, network organization and resource provisioning.

4.2 : Introduction to IOT Communications

Q.9 Illustrate the various IoT communication APIs ?

☞ [SPPU : June-22, End Sem, Marks 8]

Ans. : IoT communication APIs are REST-based and WebSocket based communication APIs.

1. REST-based communication APIs :

1. **Client-Server :** Requires that a service offer one or more operations and that services wait for clients to request these operations.
2. **Stateless :** Requires communication between service consumer (client) and service provider (server) to be stateless.
3. **Cache :** Requires responses to be clearly labeled as cacheable or non-cacheable.
4. **Uniform interface :** Requires all service providers and consumers within a REST-compliant architecture to share a single common interface for all operations.
5. **Layered system :** Requires the ability to add or remove intermediaries at runtime without disrupting the system.
6. **Code-on-demand :** Allows logic within clients (such as Web browsers) to be updated independently from server-side logic using executable code shipped from service providers to consumers.

2. WebSocket based communication APIs :

- WebSocket support full-duplex, two-way communication between client and server.
- WebSocket APIs reduce the network traffic and latency as there is no overhead for connection setup and termination requests for each message.
- Fig. Q.9.1 shows WebSocket model.
- WebSocket uses a standard HTTP request-response sequence to establish a connection. When the connection is established, the WebSocket API provides a read and write interface for reading and

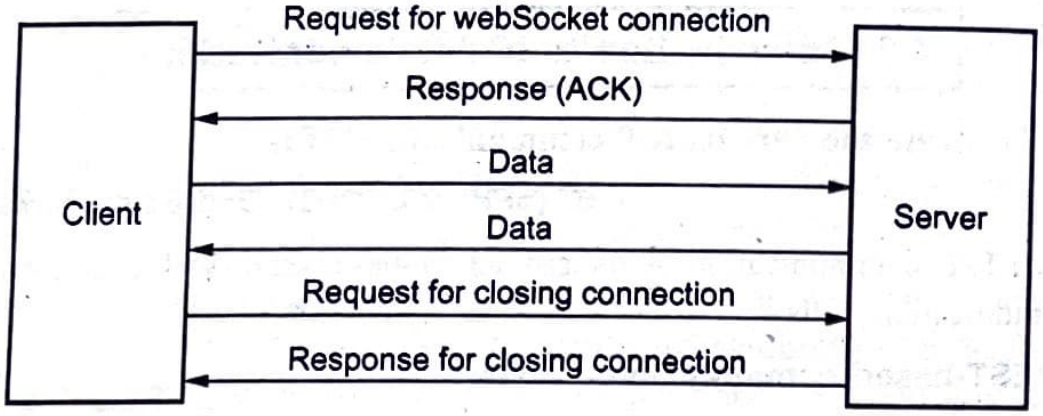

Fig. Q.9.1 Websocket model

writing data over the established connection in an asynchronous full duplex manner.

- WebSocket also provides an interface for asynchronously closing the connection from either side.

Q.10 Explain different types of IoT communication model.

Ans. : 1. 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. Q.10.1 shows Request/Response model.

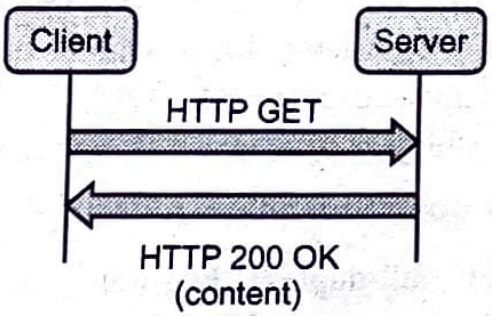

Fig. Q.10.1 Request/Response model

- 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.

2. Push/Pull model :

- Data procedure push the data to queues and consumers pull the data from the queues.
- Fig. Q.10.2 shows push-pull model.

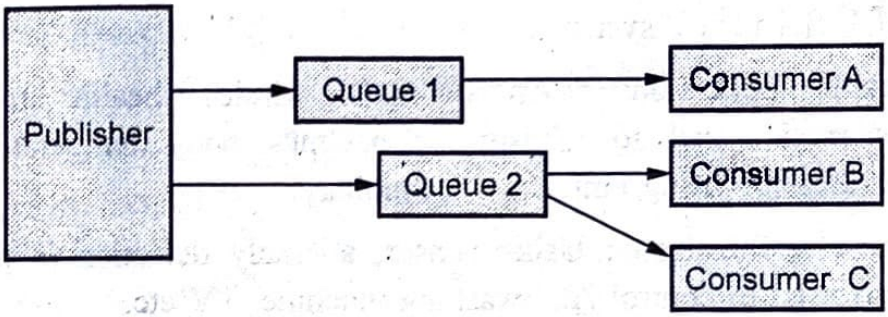

Fig. Q.10.2 Push-Pull model

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

3. Exclusive pair model :

- This communication model is full duplex, bi-directional communication model. It uses persistent connection between client and server.
- Fig. Q.10.3 shows exclusive pair model.

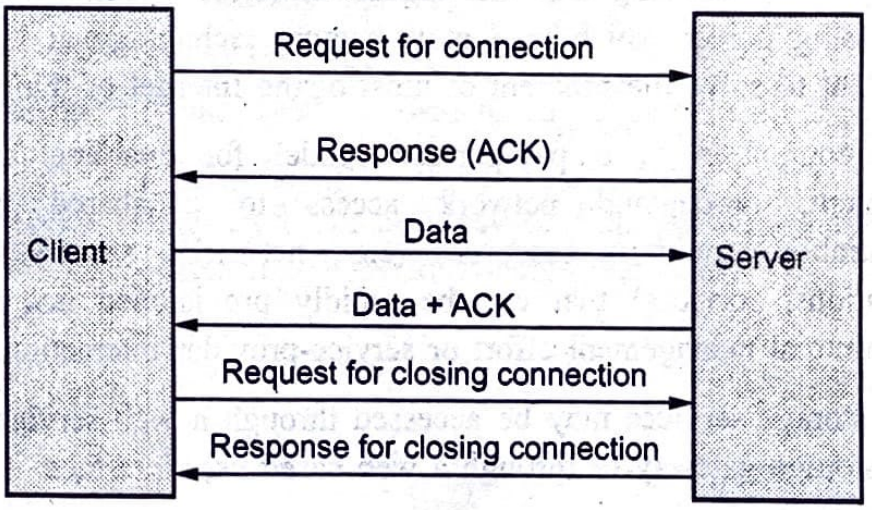

Fig. Q.10.3 Exclusive pair model

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

Q.11 Write short note on IoT enabling technology : WSN.

Ans. : • 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.

- Use of WSN in IoT system :
  a) Health applications : An automatic wireless health monitoring system is used to measure a patient's body temperature and heartbeat by using embedded technology.
  b) Home applications : Using sensor, anomaly detection is possible. Also used to control AC, washing machine, TV etc.
  c) Air pollution monitoring : WSN used to collect data on the air quality.
  d) Forest fire detection : WSN used to monitor fire at various locations.
  e) Landslide detection.
  f) Water quality monitoring.
  g) Industrial monitoring.

Q.12 Explain cloud computing as an IoT enabling technologies.

Ans. : • 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 :
  1. Infrastructure as a Service (IaaS) : Hardware is provided by an external provider and managed for user.
  2. Platform as a Service (PaaS) : In addition to hardware, operating system layer is managed for user.
  3. Software as a Service (SaaS) : Further to the above, an application layer is provided and managed for user, user won't see or have to worry about the layers.

Q.13 Write short note on big data analytics.

Ans. : • 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.

- Big data is a collection of data from many different sources and is often describe by five characteristics : Volume, value, variety, velocity, and veracity.
  1) **Volume :** The size and amounts of big data that companies manage and analyze.
  2) **Value :** The most important "V" from the perspective of the business, the value of big data usually comes from insight discovery and pattern recognition that lead to more effective operations, stronger customer relationships and other clear and quantifiable business benefits.
  3) **Variety :** The diversity and range of different data types, including unstructured data, semi-structured data and raw data.
  4) **Velocity :** The speed at which companies receive, store and manage data.
  5) **Veracity :** The "truth" or accuracy of data and information assets, which often determines executive-level confidence.

4.3 : Telemetry Vs IOT

Q.14 Discuss briefly Telemetry Vs IoT.

Ans. : • 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 : Applications of IOT Communications People, Processes and Devices

Q.15 What is asset management ? Explain.

Ans. : • 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.

Q.16 What is SCADA ? Discuss generation of SCADA. Draw and Explain block diagram of SCADA.

Ans. : • 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 exist in 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. Q.16.1 shows block diagram of SCADA.

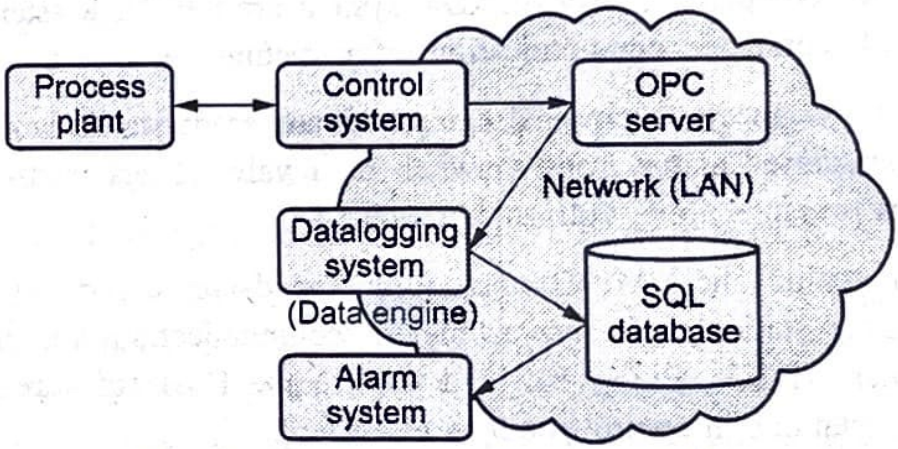

Fig. Q.16.1 Block diagram of SCADA

- 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.

4.5 : Home Automation

Q.17 What do you mean home automation ? On which levels IoT works ?

Ans. : • 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.

Q.18 Determine the IoT-levels for designing home automation IoT systems including smart lighting and intrusion detection ?

Ans. : • For designing home automation, IoT Level 1 is used.

- The device Functional Group (FG) contains devices for monitoring and control. In the home automation example, the device FG includes a single board minicomputer, a light sensor and relay switch.
- The communication FG handles the communication for the IoT system. The communication FG includes the communication protocols that form the backbone of IoT systems and enable network connectivity. The communication API home automation example is a REST based APIs.
- By analyzing and sensing the human movements and environment, the light can be controlled by the smart lightening system. For example, a person enters a room, the light turns on automatically and it turns off when a person leaves the room.
- For this purpose, solid state lightening, IP enabled light are included. These can be controlled via mobile or web application. E.g. Phillips hue lights intrusion detection includes the sensors and cameras used to raise alerts and detect intrusions via SMS, image, video and email. This will improve security.

Q.19 How IoT helps for smart lighting ?

Ans. : • 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.

- In automatic light control system, Light Dependent Resistor (LDR) sensor is used to detect bright /medium /dim /dark conditions.

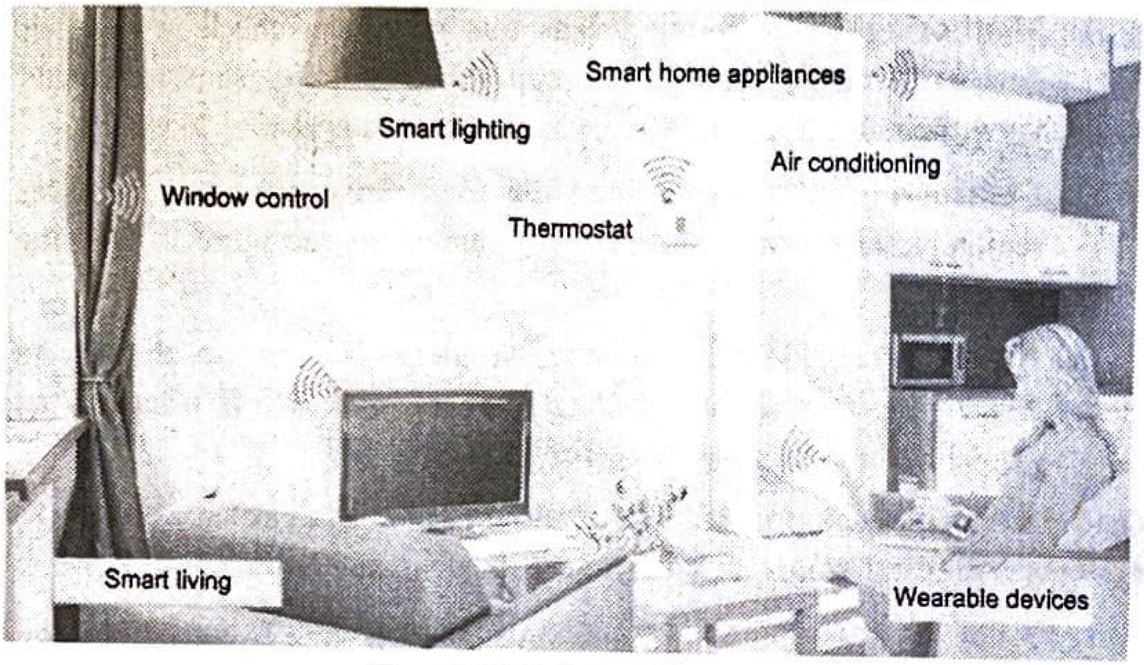

Fig. Q.19.1 Smart home

- 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.

Q.20 Explain working of intrusion detection using IoT ?

Ans. : • 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. Q.20.1 shows block diagram of intrusion detection.

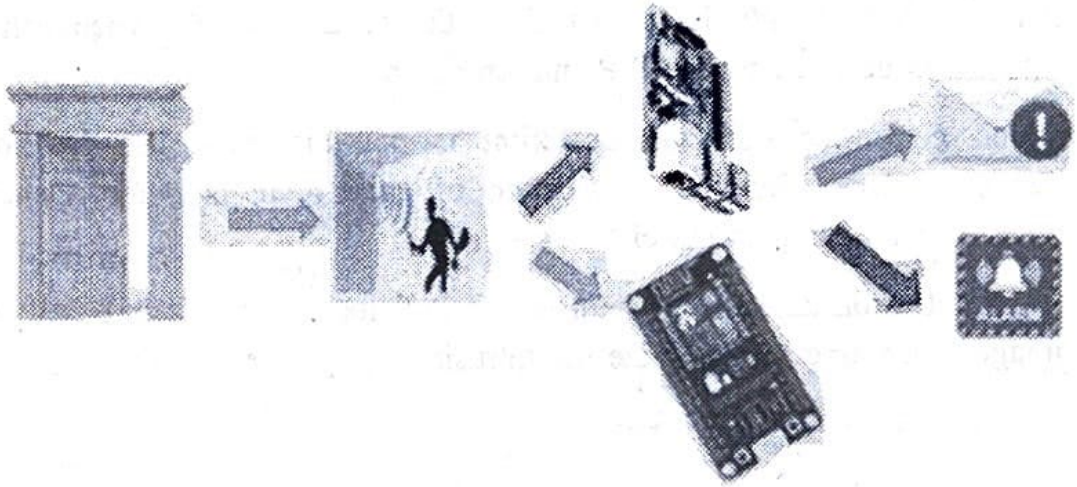

Fig. Q.20.1 Block diagram of intrusion detection

- 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 (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.

4.6 : Smart City

Q.21 What is smart parking ? Explain process specification of smart parking ? How it is implemented at various levels ?

Ans. : • 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. Q.21.1 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.

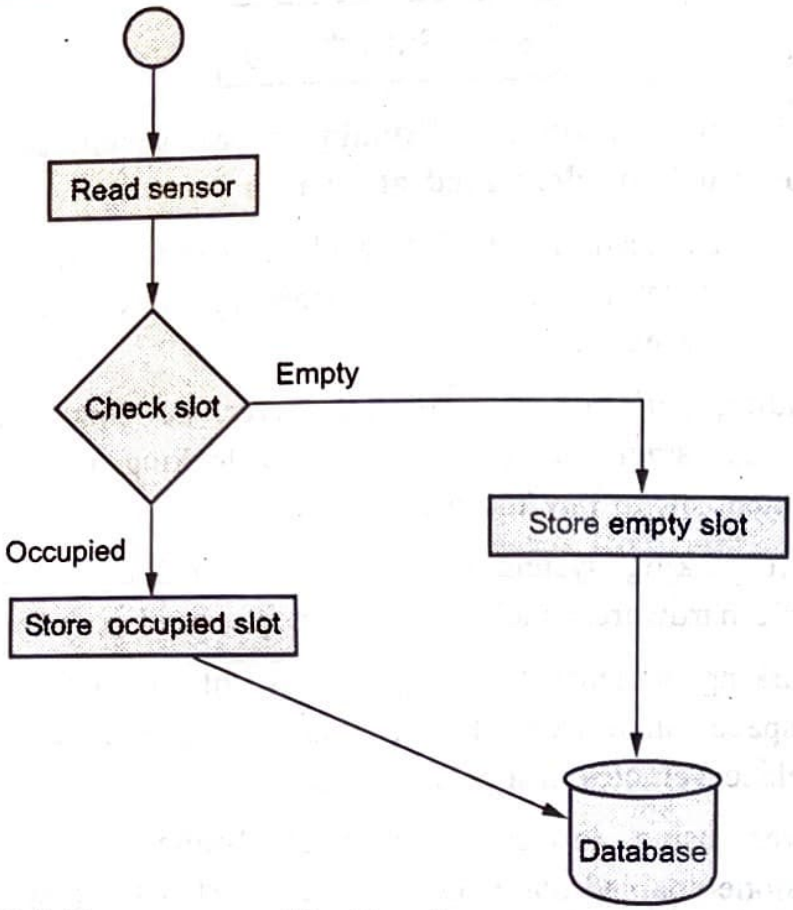

Fig. Q.21.1 Process specification for smart parking IoT system

- Fig. Q.21.2 includes four layers : A sensing, networking, middleware and application layer.
- 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.

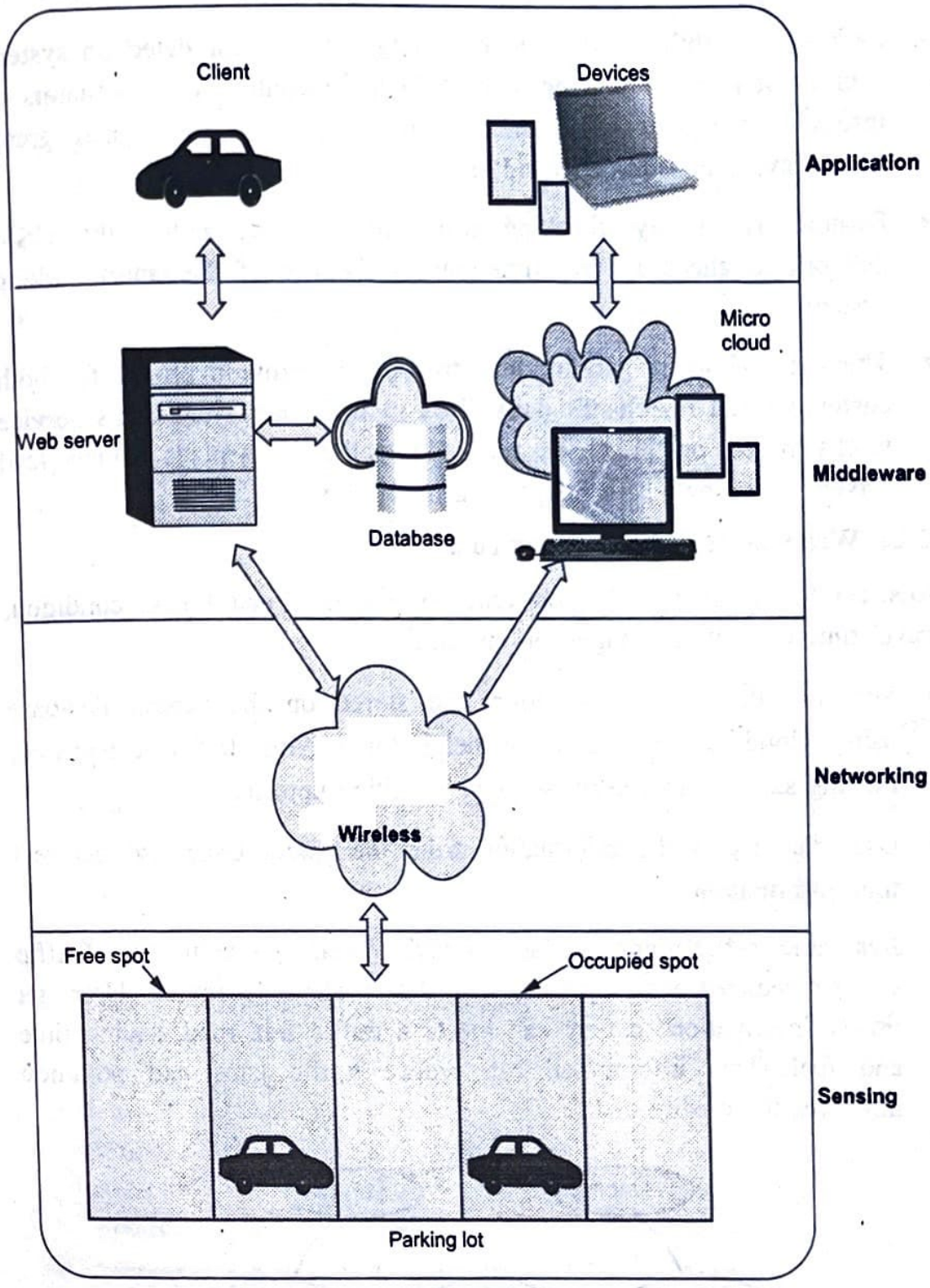

Fig. Q.21.2

- 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.

Q.22 Write short note on smart road.

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

- 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.

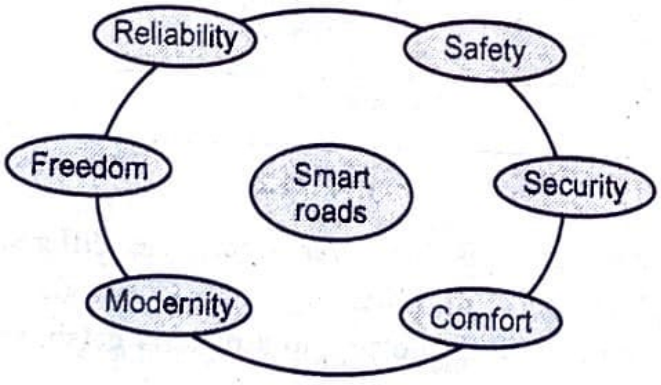

Fig. Q.22.1 Smart roads characteristics

4.7 : Logistics

Q.23 With the help of following sectors explain how IoT technology is impacting on the end-to-end value chain in the logistics sector :
i) Route generation and scheduling
ii) Fleet tracking
iii) Shipment monitoring
iv) Remote vehicle diagnostics.

[SPPU : June-22, End Sem, Marks 10]

Ans. : i) 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.

ii) 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.

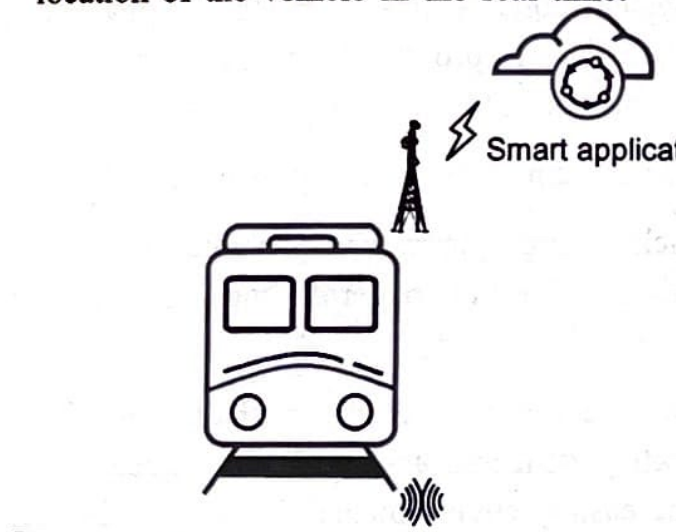

Fig. Q.23.1

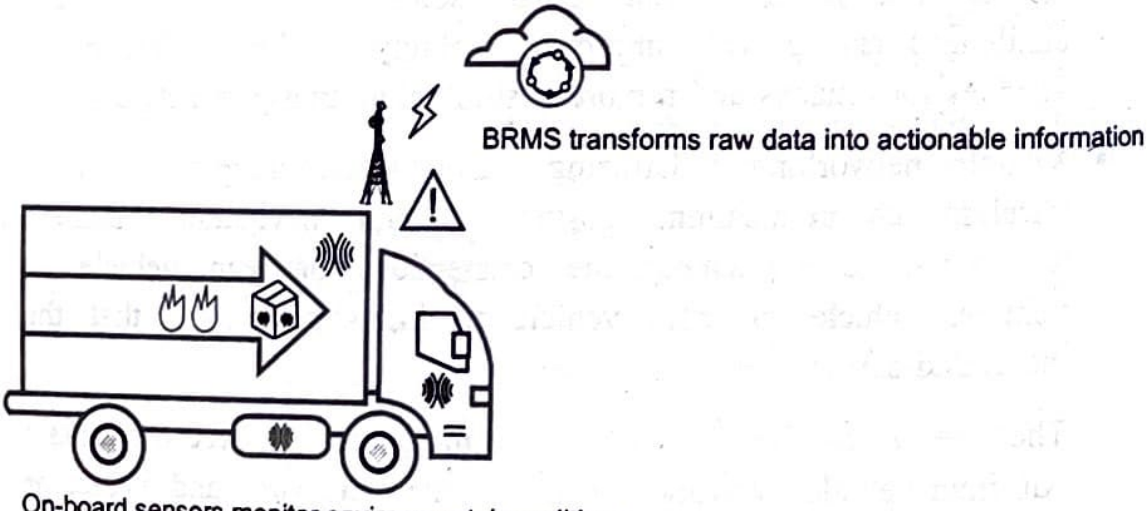

Fig. Q.23.2

- 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.

iii) 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.

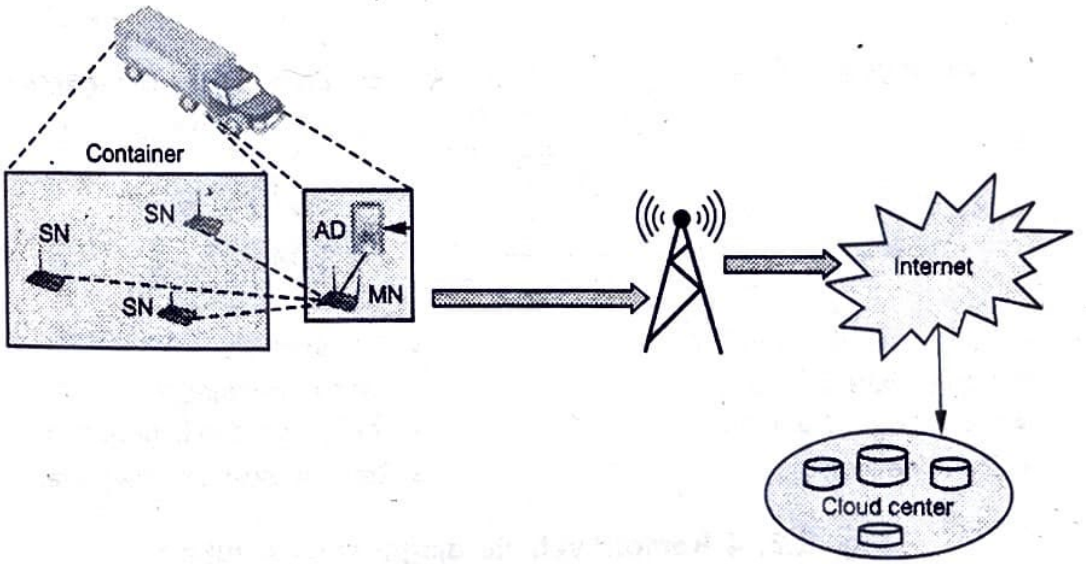

Fig. Q.23.3 Shipment monitoring system

- Required action will be taken after processing. It avoids food poisoning and financial loss of transporter.

iv) 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 Q.23.4 shows remote vehicle diagnostics.

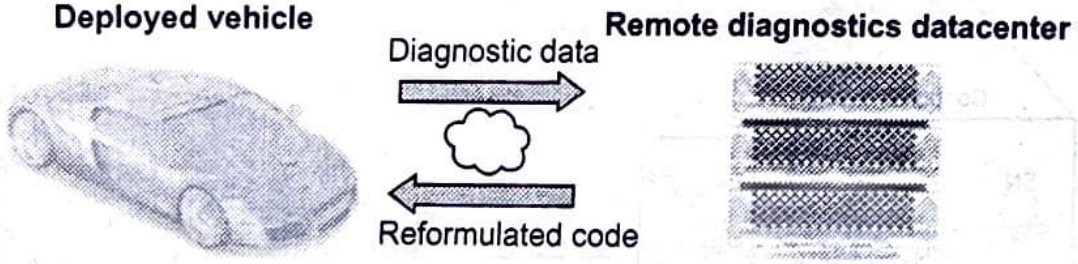

Fig. Q.23.4 Remote vehicle diagnostics solution

- 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.
- 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

Q.24 Write short note on smart vending machine.

Ans. : • 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.

Q.25 Discuss inventory management system using IoT.

Ans. : • 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.

4.9 : Industry

Q.26 Write short note on machine diagnosis and prognosis.

Ans. : • 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.

4.10 : Next Generation Kiosks

Q.27 What is kiosks ? Explain types of kiosks.

Ans. : • 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. Q.27.1 shows kiosks.

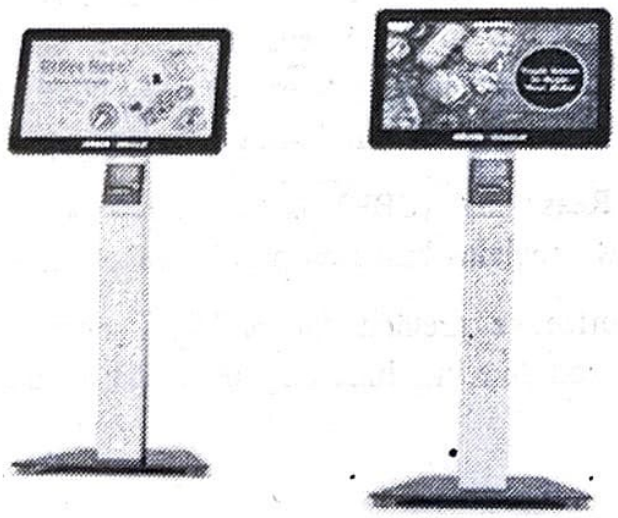

Fig. Q.27.1 Kiosks

- 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.
  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

Q.28 Write short note on : Cellular IOT connectivity services.

Ans. : • 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. Q.28.1 shows types of cellular IoT.

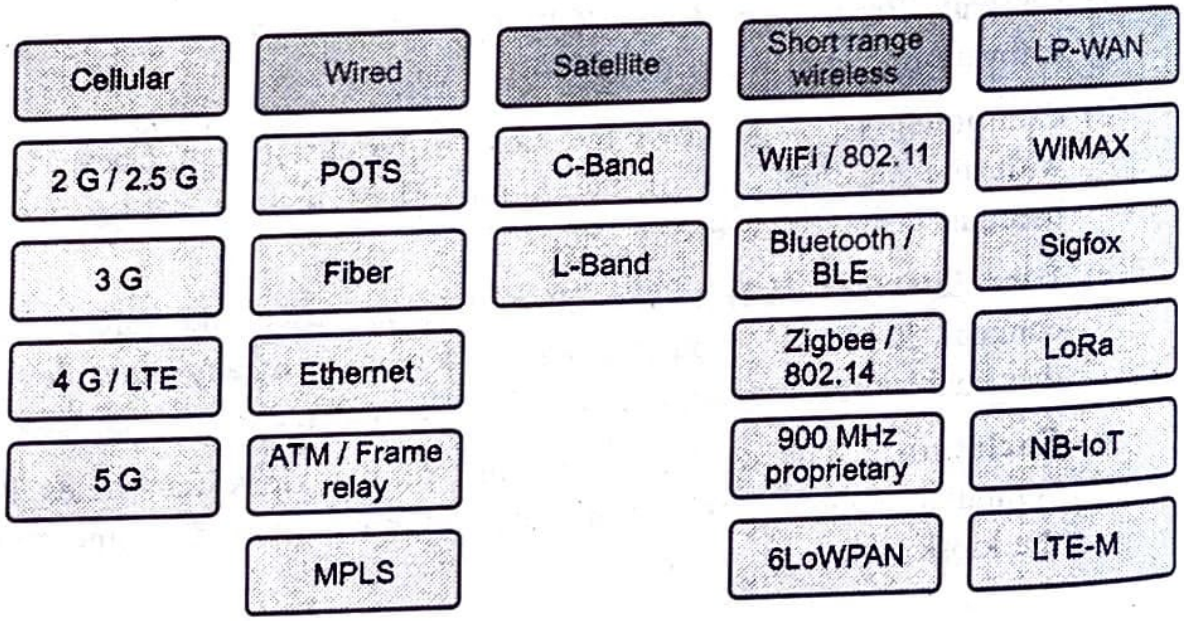

Fig. Q.28.1 Types of cellular IoT

- 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.

Q.29 What is piggybacking ? What is the necessity of security and privacy of IoT ?

☞ [SPPU : June-22, End Sem, Marks 9]

Ans. : • Piggybacking Attack : Piggybacking is using a wireless connection to access an internet connection without authorization. Its objective is to gain free network access which is often exploited to attempt malicious activities like data breaching and dissemination of malware. It can also lead to slower internet speed for all the systems connected to the network.

- Even if piggybacking isn't attempted with malicious intent, it's still illegal because the user is taking undue advantage of a service they haven't paid for.
- Piggybacking attacks were easier and more common in the past because Wi-Fi networks were unencrypted. Anyone within the signal's range could access a network without entering a security password. So, hackers just had to be in the range of a wi-fi hotspot's signal and select the chosen network from the options presented.
- However, in today's date, most Wi-Fi networks are encrypted and secured with passwords, making these attacks more challenging and less common. It's still possible for threat actors to access a network if they have the password or can crack the encryption.
- Privacy issue in IoT : The benefits of connected healthcare devices have been helping people in obtaining a better impression of their health. However, the benefits introduce prominent risks with the number of growing devices. The growth in the number of connected devices in the IoT ecosystem can present issues for security in IoT by offering more entry points for cybercriminals and hackers.
- The methods of data collection in the IoT lead us to privacy challenges such as obtaining consent for data collection, allowing users to control, customize and choose the data they share and ensuring the use of collected data is limited to the stated purpose.
- These challenges are made more difficult by the increased potential for misuse of personal data by the IoT developers that may lead to "profiling" through tracking of habits, behaviors and locations over a period of time.

- One of the most important concerns in understanding the issues of privacy in IoT would draw attention towards reasons for privacy concerns. The IoT ecosystem has intelligent artifacts present almost everywhere with flexibility for sampling process and information distribution from any location.
- In addition, the ubiquitous connectivity in IoT through the internet also plays a crucial role in amplifying privacy concerns. Without a unique mechanism for privacy protection, the ubiquitous connectivity of IoT could enable flexible access to personal information from any corner of the world.
- Security Issues in IoT : Hard-coded and embedded credentials in IoT devices provide an easy target for hackers to compromise the devices directly. Default passwords may enable hackers to enter the machine without any obstacles. One of the examples of such an attack refers to the Mirai malware, which infected IoT devices such as routers, video recorders and video cameras.

END...

Unit IV

5 IoT Systems, Network and Protocols

5.1 : Study of RF Wireless Sensors

Q.1 What is RFID ? Explain working of RFID.

Ans. : • Radio Frequency Identification (RFID) is a very simple and cost-effective way of item identification. RFID systems can be seen as a next-generation technology for bar-codes. RFID devices are wireless microchips used for tagging objects for automated identification.

- An RFID tag is a simplified, low-cost, disposable contactless smartcard. RFID tags include a chip that stores a static number (ID) and attributes of the tagged object and an antenna that enables the chip to transmit the store number to a reader.

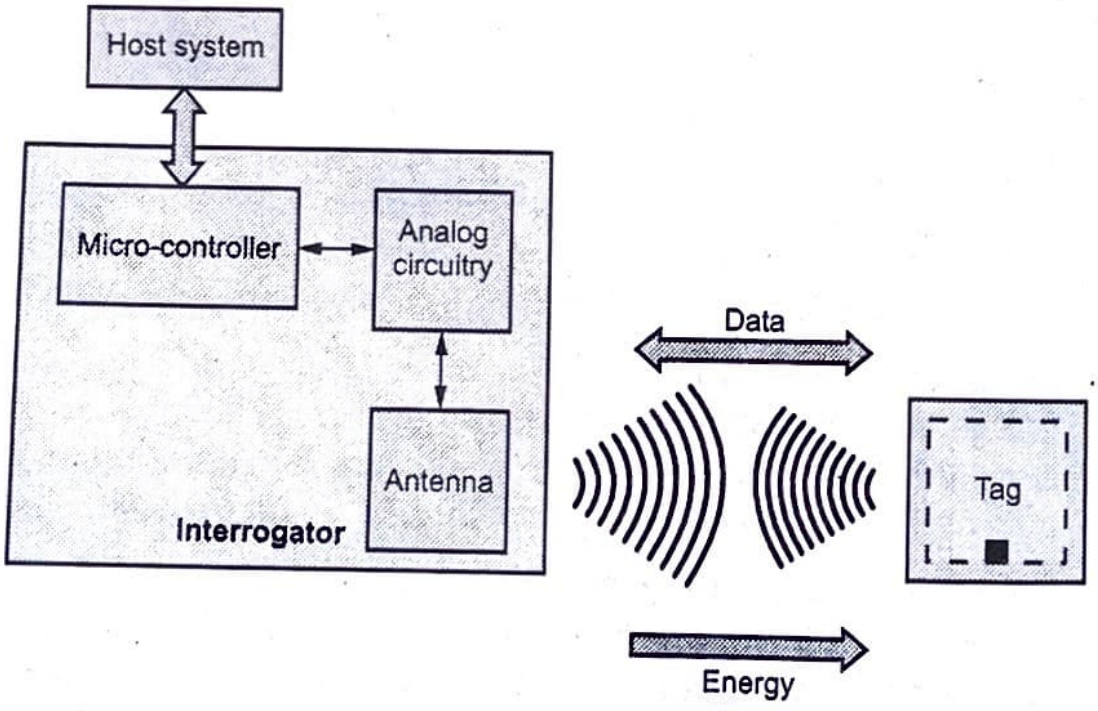

Fig. Q.1.1 Basic RFID system

- Tags are characterized by a unique identifier and are applied to objects. Readers trigger the tag transmission by generating an appropriate signal, which represents a query for the possible presence of tags in the surrounding area and for the reception of their IDs.
- Fig. Q.1.1 shows basic RFID system.
  (Refer Fig. Q.1.1 on previous page)
- RFID systems consist of a reading device called a reader and one or more tags. The reader is a powerful device with ample memory and computational resources.
- Passive tags have limited computational capacity, no ability to sense the channel, detect collisions and communicate with each other. They respond only at reader commands.
- Semi-passive tags have an on-board power source that can be used to energize their microchip. Active tags can sense the channel and detect collisions.
- Accordingly, RFID systems can be used to monitor objects in real-time, without the need of being in line-of-sight; this allows for mapping the real world into the virtual world.
- An RFID system involves hardware known as readers and tags, as well as RFID software or RFID middleware. Readers can also be mobile / hand-held.
- RFID systems operate in the Industry, Scientific and Medical (ISM) frequency band that ranges from 100 kHz to 5.8 GHz.
- **Reader functions :**

1. Remotely power tags
2. Establish a bidirectional data link
3. Inventory tags, filter results
4. Communicate with networked server(s)
5. Can read 100-300 tags per second.

Q.2 Explain RFID anti-collision protocols. What are the advantages of RFID over bar-codes ?

Ans. : RFID anti-collision protocols :

- Collision due to simultaneous tag responses is one of the key issues in RFID systems. Tag collision results in wastage of bandwidth, energy and increases identification delays.
- RFID readers must use an anti-collision protocol to minimize collisions and hence help reduce identification delays. Fig. Q.2.1 shows tag collision problem.

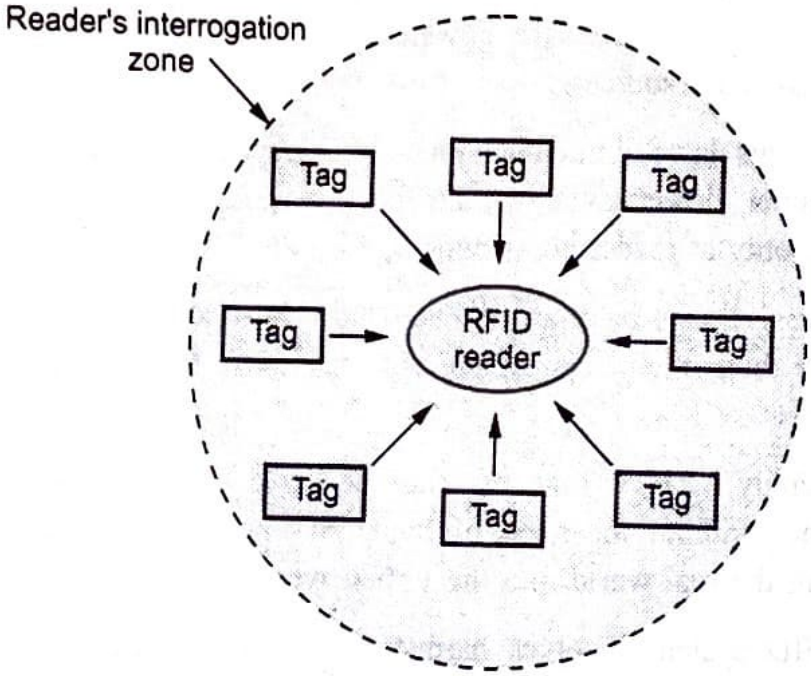

Fig. Q.2.1 Tag collision problem

- RFID anti-collision protocols are often categorized as Aloha based protocols and tree based protocols. In pure Aloha based RFID systems, a tag responds with its ID randomly after being energized by a reader.
- In Slotted Aloha (SA) based RFID systems, tags transmit their ID in synchronous time slots. The collision occurs at slots boundary only, hence there are no partial collisions.

RFID advantages over bar-codes :

1. No line of sight required for reading
2. Multiple items can be read with a single scan
3. Each tag can carry a lot of data (read/write)

4. Individual items identified and not just the category
5. Passive tags have a virtually unlimited lifetime
6. Active tags can be read from great distances
7. Can be combined with barcode technology.

Q.3 What is RFID middleware ? Explain in detail. Discuss benefits of RFID middleware.

Ans. : • RFID middleware needs to allow users to configure, deploy and issue commands directly to readers through a common interface. For instance users should be able to tell a reader when to "tun off" if needed. Fig. Q.3.1 shows RFID middleware.

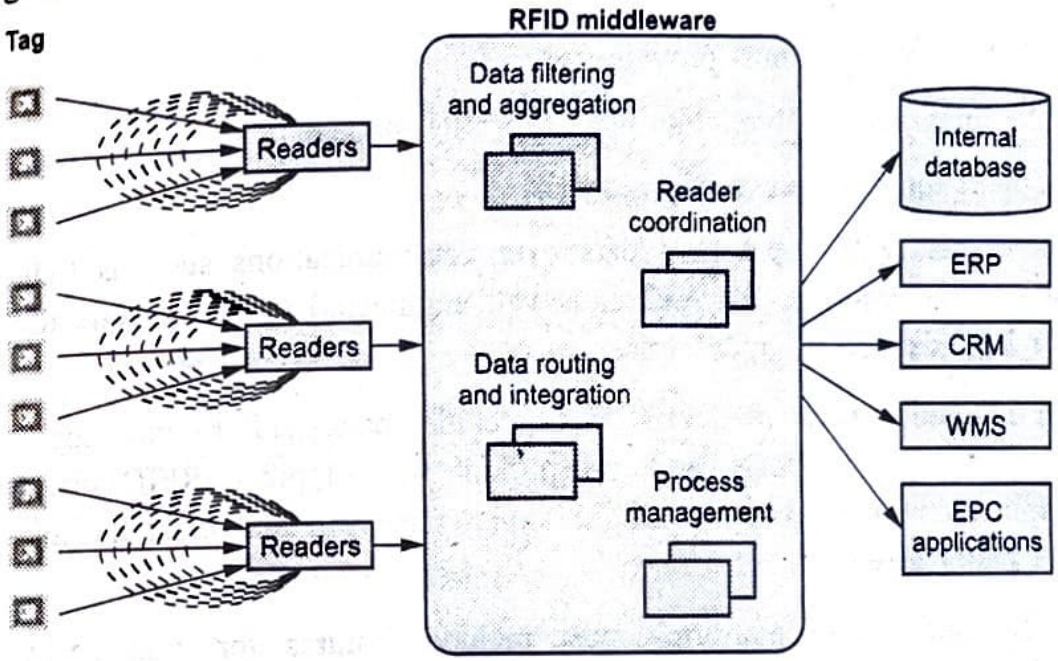

Fig. Q.3.1 RFID middleware

- After RFID middleware captures EPC data from readers, it must be able to intelligently filter and route the data to the appropriate destinations.
- Look for middleware that includes both low-level logic and more complex algorithms. Comprehensive solutions also offer tools for aggregating and managing EPC data in either a federated or central data source.
- RFID middleware solutions need to provide the messaging, routing and connectivity features required to reliably integrate RFID data into

existing SCM, ERP, WMS or CRM systems. Ideally through a Services-Oriented Architecture (SOA).

- A services-oriented architecture is essentially a collection of services. These services communicate with each other. The communication can involve either simple data exchange or two or more services coordinating some activity, such as order placement or inventory control.
- Middleware needs to provide a library of adapters to popular WMS and SCM applications (e.g., SAP or Oracle E Business Suite). Application Programming Interfaces (APIs) and adapters for using standard technologies like JMS, XML and SOAP to integrate with other third-party applications.
- RFID middleware must provide :

1. B2B integration features like partner profile management.
2. Support for B2B transport protocols.
3. Integration with a partner's data over communications such as EDI, Web-based systems like AS2 or a well engineered system specifically for EPC data RFID middleware.

- RFID middleware platforms that include packaged routing logic, product data schemas and integration with typical RFID-related applications and processes like shipping, receiving and asset tracking are major assets.
- RFID middleware platforms must include features for dynamically balancing processing loads across multiple servers and automatically rerouting data.

RFID middleware benefits

a. Minimized network traffic through intelligent filtering.
b. Lower reader-management costs through centrally coordinated readers.
c. Immediate visibility to pertinent RFID data through routing, filtering and track-and-trace tools.
d. Minimized on-going integration costs through standard APIs and prepackaged application integration tools.

e. Well-architected RFID middleware can enable more strategic opportunities that go way beyond these initial, rather obvious benefits.

Q.4 Draw and explain WSN architecture ?

☞ [SPPU : June-22, End Sem, Marks 9]

Ans. : • 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 now a days 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.
- A wireless sensor network 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.
- Fig. Q.4.1 shows WSN architecture.

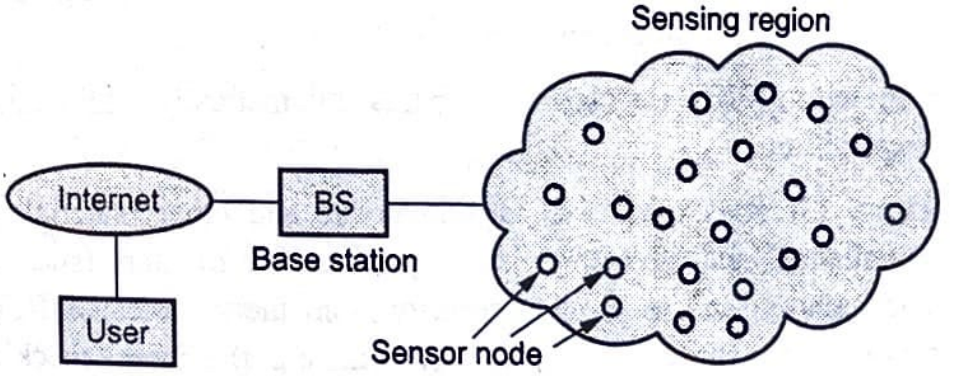

Fig. Q.4.1 WSN architecture

- A wireless sensor network consists of sensor nodes deployed in large quantities and support sensing, data processing, embedded computing and connectivity.

- When a large number of sensor nodes are deployed in a large area to monitor a physical environment, the networking of these sensor nodes is equally important A sensor node in a WSN not only communicates with other sensor nodes but also with a base station using wireless communication.
- The base station sends commands to the sensor nodes and the sensor node perform the task by collaborating with each other.
- The sensor nodes in turn send the data back to the base station. Base station also acts as a gateway to other networks through the internet.
- After receiving the data from the sensor nodes, a base station performs simple data processing and sends the updated information to the user using internet.
- If each sensor node is connected to the base station, it is known as single hop network architecture. Although long distance transmission is possible, the energy consumption for communication will be significantly higher than data collection and computation.

Q.5 Explain any four applications of RFID ?

☞[SPPU : June-22, End Sem, Marks 8]

Ans. :

1. **Agriculture :** RFID can be useful to track the movement and health of animals on a farm. It ensures that each animal on the farm is consuming the correct food. Monitoring your cattle's health manually can be costly as well time-consuming.

   However, with RFID, we can achieve this automatically and without much expenditure.

2. **Libraries :** Libraries use RFID tags in books and other materials to track circulation and inventory, store product information (such as titles and authors) and to provide security from theft. Because RFID tags can be scanned without physically touching the item, checking books in and out, plus doing laborious tasks such as shelf inventory, can be accomplished quickly and efficiently using RFID technology.
3. **Toll road payments :** Highway toll payment systems, such as E-Z pass in the eastern states, uses RFID technology to electronically

collect tolls from passing cars. Instead of stopping at the toll booth, cars pass directly through in the E-Z pass lane and the toll is automatically deducted from a pre-paid card.

4. **Passports :** A number of countries, including Japan, the United States, Norway, and Spain incorporate RFID tags into passports to store information (such as a photograph) about the passport holder and to track visitors entering and exiting the country.

Q.6 Define sensor network. Write advantage and disadvantage of wireless sensor network.

Ans. : • A sensor network comprises a group of small, powered devices, and a wireless or wired networked infrastructure. A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source.

- **Advantages of WSN**

1. WSN is a flexible network and can adapt to the changes
2. Wireless sensor networks save a lot of wiring cost
3. WSNs are easier to deploy and maintain and offer better flexibility of devices.

- **Disadvantages**

1. Limited computation and communication resources
2. WSN networks are not secure as compared to wired networks.

5.2 : Cellular Machine - to - Machine (M2M) Application Networks

Q.7 Define M2M. Explain reasons of shifting from M2M to IoT.

Ans. : • M2M communication is the communication among the physical things which do not need human intervention.

- 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 of communication. M2M is also named as Machine Type Communication (MTC) in 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 transport network.
- M2M is only a subset of IoT. IoT is a more encompassing phenomenon because it also includes Human-to-Machine communication (H2M).
- Radio Frequency 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 H2M communications.
- Reasons :

1. It support multiple application with multiple device.
2. It is information and service centric.
3. It support open market place.
4. IoT uses horizontal enabler approach.
5. It requires generic commodity devices.
6. Used in B2B and B2C.

Q.8 Explain machine to machine architecture.

☞ **[SPPU: June-22, End Sem, Marks 9]**

Ans. : • Fig. Q.8.1 shows M2M architecture.

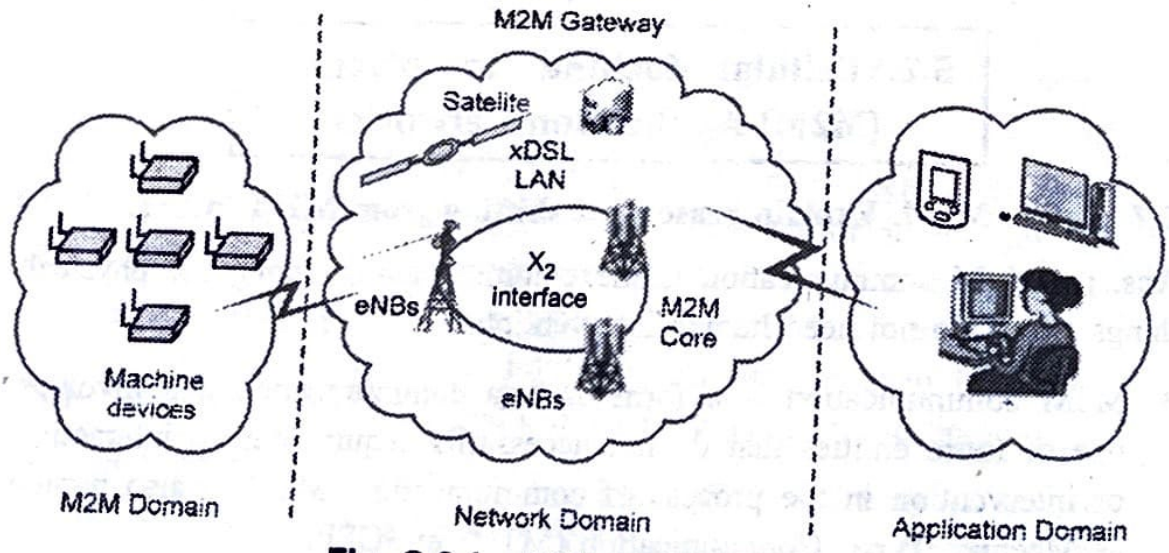

Fig. Q.8.1 : M2M architecture

- 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 area network.
2. **M2M area network :** A M2M area network provides connectivity between M2M devices and M2M gateways. Examples of M2M area networks include : Personal area network technologies such as IEEE 802.15, SRD, UWB, Zigbee, Bluetooth, etc. or local networks such as PLC, M-BUS, Wireless M-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 M2M applications.
4. **M2M applications server :** Applications that run the service logic and use service capabilities accessible via open interfaces.
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 the enterprise.

Q.9 List the key features of M2M.

Ans. : Key features of M2M :

1. **Low mobility :** M2M devices do not move and if moves only within a certain area.
2. **Time controlled :** Data can be send or receive only at certain pre-defined time periods.
3. **Time tolerant :** Sometimes data transfer can be delayed.
4. **Packet switched :** Network operator to provide packet switched service.
5. **Online small data transmissions :** Devices frequently send or receive small amounts of data.
6. **Low power consumption :** To improve the ability of the system to efficiently service M2M applications.

7. **Location specific trigger :** Intending to trigger M2M device in a particular area e.g. wake up the device.

Q.10 What are the six pillars of M2M ?

Ans. : 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 industrial assets.
2. RFID is a data-collection technology that uses electronic tags for storing data.
3. A sensor network monitors physical or environmental conditions, with sensor nodes acting co-operatively to form/maintain the network.
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 in vehicles.
6. Telemetry is usually associated with industrial, medical, and wildlife-tracking applications that transmit small amounts of vehicles data.

Q.11 Explain key application area of M2M.

Ans. :

1. **Security :** Surveillances, Alarm systems, Access control, Car/driver security
2. **Tracking and tracing :** Fleet management, Order management, Pay as you drive, Asset Tracking, Navigation, Traffic information, Road tolling, Traffic optimization/steering
3. **Payment :** Point of sales, Vending machines, Gaming machines.
4. **Health :** Monitoring vital signs, Supporting the aged or handicapped, Web Access Telemedicine points, Remote diagnostics.
5. **Remote maintenance/control :** Sensors, Lighting, Pumps, Valves, Elevator control, Vending machine control, Vehicle diagnostics.

6. **Metering** : Power, Gas, Water, Heating, Grid control, Industrial metering.
7. **Manufacturing** : Production chain monitoring and automation.
8. **Facility management** : Home / building / campus automation.

Q.12 Write difference between IoT and M2M ?

Ans. :

Sr. No.	Machine-to-Machine	Internet of Things
1.	It support single application with single device.	It support multiple application with multiple device.
2.	It is communication and device centric.	It is information and service centric.
3.	It support closed business operations.	It support open market place.
4.	M2M uses vertical system solution approach.	IoT uses horizontal enabler approach.
5.	It requires specialized device solutions.	It requires generic commodity devices.
6.	Used in B2B.	Used in B2B and B2C.

Q.13 How do data collection and analysis approaches are differ in M2M and IoT ?

Ans. : • M2M data is collected in point solutions and often in on-premises storage infrastructure. In context to M2M, the data in IoT is collected in the cloud (can be public, private or hybrid cloud). The various IoT Levels, and IoT components deployed in the cloud.

- The analytics component analyzes the data and stores the results in the cloud database. The IoT data and analysis results are visualized with the cloud based applications. The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes. Observer nodes can process information and use it for various applications,, however, observer nodes do not perform any control functions.

- In IoT, an air conditioner's sensor may collect the data on outside temperatures and change its temperature to increase or decrease according to the outside environment's temperature. Likewise, the refrigerators may change their temperature accordingly, too.
- In M2M, it is a direct communication system between the devices using wired or wireless communications channels without any human interaction. It collects the data and shares it with other connected devices. It is a technology that allows devices without the use of the internet to connect between devices.

5.3 : Network Device

Q.14 Explain IoT device life cycle.

Ans. : • IoT devices are generally more like single-purpose computers. The first life cycle, for example, includes four steps :

1. **Boot-up** : The device loads the firmware and starts to work as defined.
2. **Initialization** : Once boot-up is completed, the system reads the configuration, established connections, syncs up data, etc.
3. **Operation** : The device performs its designed purpose continually.
4. **Update** : New firmware is installed, the device reboots and then starts to load the new firmware.

- The device should complete its previous life cycle before starting the next life cycle every time the firmware is updated. Eventually, the device will be retired for whatever reason. When it does, it reaches the end of the device life cycle called termination.

Q.15 Draw and explain block diagram of IoT device.

Ans. : • IoT devices have unique identity and they are refer as "things" in IoT. Device can perform remote sensing, actuating and monitoring.

- IoT devices can exchange data between them and process data or send to centralized location for processing and storage. Fig. Q.15.1 shows block diagram of IoT device.

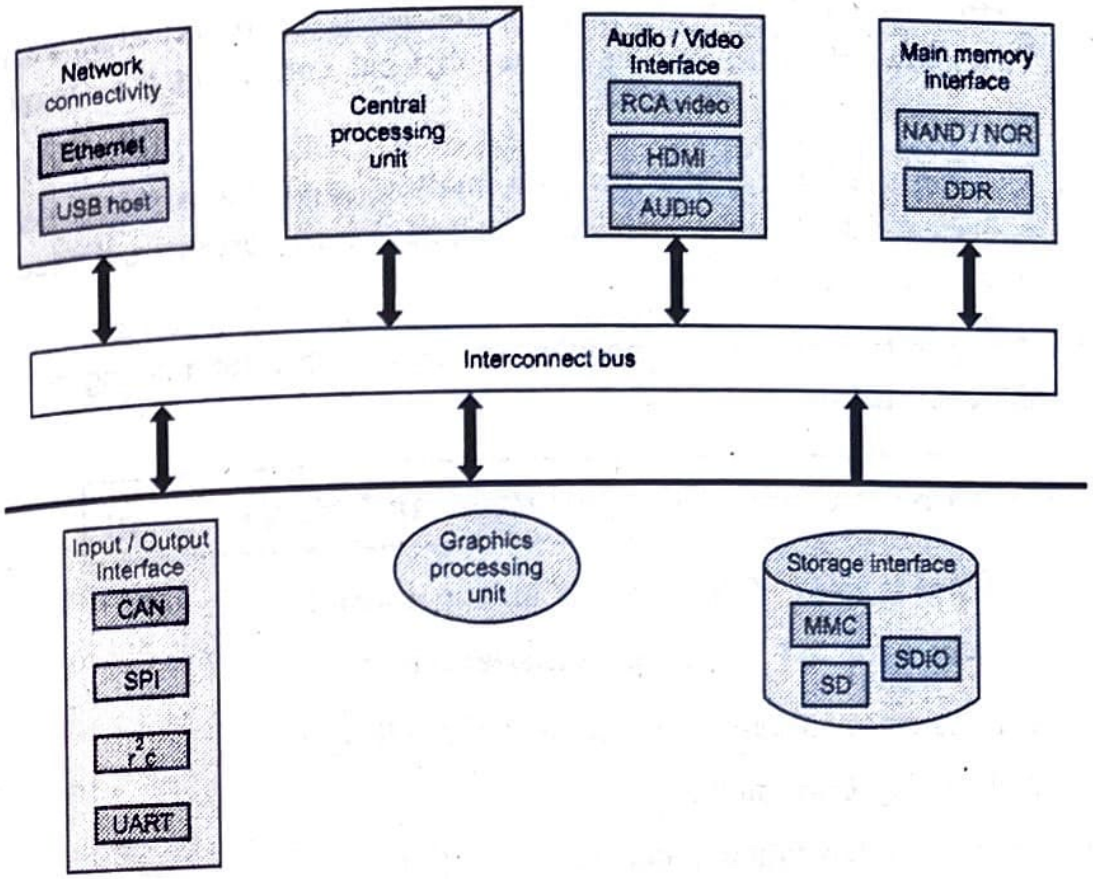

Fig. Q.15.1 Block diagram of IoT device

- IoT devices provide interface to various wire and wireless devices. Interface includes memory interface, I/O interface for sensors, Internet connectivity interface, storage interface etc.
- Using sensors, IoT collects various information like temperature, light intensity, humidity, air pressure. Some application used cloud based storage. Collected information is stored in cloud and transmitted to other devices.
- Various types of IoT devices are smart clothing, smart watch, wearable sensors, LED lights, automobile industry etc.
- **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.

- **Actuation :** IoT devices can have various types of actuators attached that allow taking actions upon the physical entities in the vicinity of the device.
- **Communication :** Communication modules are responsible for sending collected data to other device or cloud based servers and receiving data from other devices.
- Analysis and processing modules are responsible for making sense of the collected data.

5.4 : Device Configuration and Management

Q.16 What is need of IoT system management ?

Ans. : Need for IoT systems management :

- IoT system management is required for following :

a. Automating Configuration

b. Monitoring Operational and Statistical Data

c. Improved Reliability

d. System Wide Configurations.

e. Multiple System Configurations

f. Retrieving and Reusing Configurations

Q.17 What is SNMP ? List the advantages and disadvantages of SNMP.

Ans. : • SNMP is a well-known and widely used network management protocol that allows monitoring and con?guring network devices such as routers, switches, servers, printers, etc.

- SNMP component include Network Management Station (NMS), Managed Device, Management Information Base (MIB) and SNMP Agent that runs on the device.
- Simple Network Management Protocol (SNMP) is an application-layer protocol used to manage and monitor network devices and their functions.

- SNMP provides a common language for network devices to relay management information in a local area network (LAN) or wide area network (WAN).
- SNMP has a simple architecture based on a client-server model. The servers, called managers, collect and process information about devices on the network.
- The clients, called agents, are any type of device or device component connected to the network. They can include not just computers but also network switches, phones, printers, and so on.
- Some devices may have multiple device components. For example, a laptop typically contains a wired as well as a wireless network interface.

Strength of SNMP :

1. It is simple to implement.
2. Agents are widely implement.
3. Agent level overhead is minimal.
4. It is robust and extensible.
5. Polling approach is good for LAN based managed object.
6. It offers the best direct manager agent interface.
7. SNMP meet a critical need.

Limitation of SNMP :

1. It is too simple and does not scale well.
2. There is no object orietned data view.
3. It has no standard control definition.
4. It has many implementation specific (private MIB) extensions.
5. It has high communication overhead due to polling.

Q.18 What is NETCONF ? Explain NETCONF protocol layers.

Ans. : • Network Configuration Protocol (NETCONF) is a session-based network management protocol. NETCONF allows retrieving state or configuration data and manipulating configuration data on network devices.

- NETCONF is the standard for installing, manipulating and deleting configuration of network devices.
- Fig Q.18.1 shows NEFCONF protocol layers.

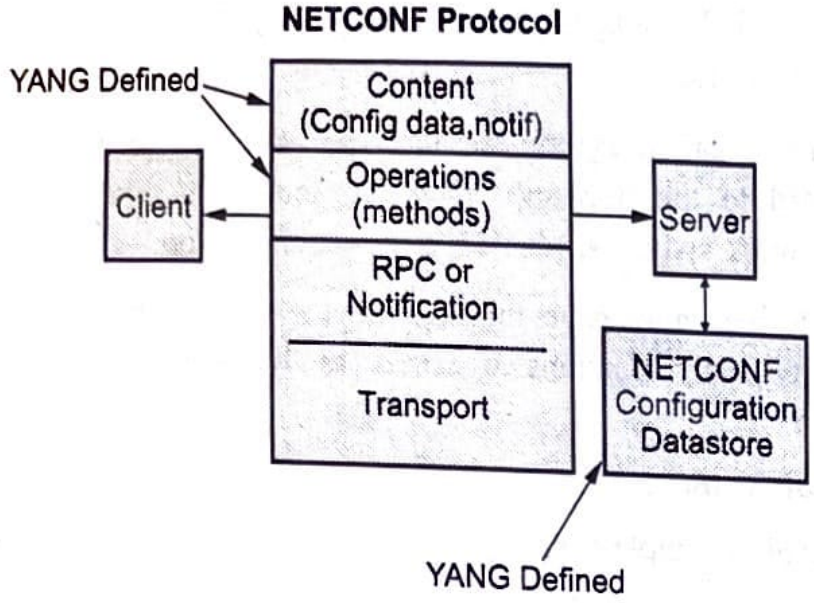

Fig. Q.18.1 NEFCONF protocol layers

- NETCONF is defined for transaction-safe configuration of devices. This means that scenarios like setting up initial configuration for a range of devices, changing ACLs and adding VPNs, can be performed automatically, while keeping flexibility and vendor independence.
- It uses an Extensible Markup Language (XML) based data encoding for the configuration data as well as the protocol messages.
- NETCONF uses a simple Remote Procedure Call (RPC) based mechanism to facilitate communication between a client and a server. The server is a network device and client can be a script or application running as part of a network manager.
- It uses Secure Shell(SSH) as the transport layer across network devices.
- NETCONF provides various operations to retrieve and edit configuration data from network devices.
- The Content Layer consists of configuration and state data which is XML-encoded.

- The schema of the configuration and state data is defined in a data modeling language called YANG.
- NETCONF provides a clear separation of the configuration and state data. The configuration data resides within a NETCONF configuration datastore on the server.
- All NETCONF devices must allow the configuration data to be locked, edited, saved and unlocked. In addition, all modifications to the configuration data must be saved across a reboot in non-volatile storage

Q.19 Write short note on YANG.

Ans. : • YANG is a data modeling language used to model configuration and state data manipulated by the NETCONF protocol.

- YANG is used to model both configuration and state data of network elements.
- YANG structures the data definitions into tree structures and provides many modeling features, including an extensible type system, formal separation of state and configuration data and a variety of syntactic and semantic constraints.
- YANG data definitions are contained in modules and provide a strong set of features for extensibility and reuse.
- YANG modules defines the data exchanged between the NETCONF client and server. A module comprises of a number of 'leaf' nodes which are organized into a hierarchical tree structure.

5.5 : Exchange Information in Real Time without Human Intervention

Q.20 Explain any two method of exchange information in real time without human intervention.

Ans. :

- Integration of different cyber-physical systems involves a development process that takes into account some solutions for intercommunicating and interoperating heterogeneous devices. Each device can be managed

as a thing within the Internet-of-Things concept by using web technologies.

1. Machine-Machine Interaction

- Reasons for requiring holistic information management :
  a) Increase of flexibility in complex production systems of manufacturing companies by enabling in-process planning, reconfiguration and control.
  b) Decentralization of responsibilities in terms of planning and execution of production tasks to reach the aimed flexibility and customization in production processes.
  c) Enabling methods of learning and the usage of enhanced process knowledge directly between machines and throughout the entire information and communication supply chain of a manufacturing enterprise.
- The most common representatives of the semantic approaches are the Data Distribution Service (DDS) for Real-Time Systems (RTS) and the OPC Unified Architecture (OPC UA) standard as a successor of the well-known and within the industrial reality well-established OLE for Process Control (OPC) standard

2. Field Bus Systems and the Industrial Ethernet

- A field bus is a serial bus system used in machines and systems to connect sensors and actuators (motors) to each other and to one or multiple masters. The hardware level determines fundamental bus properties, such as cable lengths and transmission capacity.
- Field bus protocols work according to master-slave principles and are intended to optimize the communication in centralized automation environments. Field bus systems emphasize on the networking with Programmable Logic Controllers (PLC) or Supervisory Control and Data Acquisition (SCADA) systems.
- In the traditional view, an industrial automation system, such as a manufacturing assembly line, needs an organized hierarchy of controller systems to function. In this hierarchy, there is usually a

Human Machine Interface (HMI) at the top, where an operator monitors or operates the system.

- This top-level system is typically linked to a middle layer of one or more programmable logic controllers (PLC), historically via a non-time-critical communications system (e.g., Ethernet), i.e., a serial network.
- At the bottom of the control chain is the Fieldbus that links the PLCs to the components that do the actual work, such as sensors, actuators, electric motors, console lights, switches, valves, and contactors.

5.6 : IoT Protocols

Q.21 Explain any four IoT network protocols ?

☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. : • The network layer is responsible for the delivery of packets from the source to destination.

- Network layer uses IP address to choose one host among millions of hosts. In network layer, datagram needs a destination IP address for delivery and a source IP address for a destination reply.

a. IPv4

- IP is used for communicating all Internet enabled devices. The transport layer is responsible for delivery of message from one process to another.
- The network does the host to destination delivery of individual packets considering it as independent packet. But transport layer ensures that the whole message arrives intact and in order with error control and process control.
- An IP address is a numeric identifier assigned to each machine on an IP network. IP address is a software address, not a hardware address, which is hard-coded in the machine or NIC.

- An IP address is made up of 32 bits of information. These bits are divided into four parts containing 8 bit each.
- IPv4 addresses are unique. Two devices on the internet can never have the same address at the same time.
- Packets in the IPv4 layer are called datagrams. A datagram is a variable length.

b. IPv6

- IPv6 addresses are 128 bits in length. Addresses are assigned to individual interface on nodes, not to the node themselves.
- A single interface may have multiple unique unicast addresses. The first field of any IPv6 address is the variable length format prefix, which identifies various categories of addresses.

c. 6LoWPAN

- IPv6 over Low power Wireless Personal Area Network enables IPv6 in low-power and lossy wireless networks such as WSNs.
- 6LoWPAN defines header compression mechanisms.

d. LoRaWAN

- This stands for Long Range Wide Area Network.
- Its range is approximately 2.5 km and can go up to 15 km.
- The data rate is very low, which is goes up to a maximum of 50 kbps.
- It can support many connected devices and is used in applications like smart city, supply chain management, etc.

Q.22 Explain link layer IoT protocols.

Ans. : • Link layer protocols decide how data is sent on physical medium. Link layer works within the local area network. Protocol of link layer is explained below :

a. 802.3 Ethernet

- This protocol is used for wired medium. Ethernet, in its most basic version runs at 10 Mbit/s. Ethernet has traditionally been used to network enterprise workstations and to transfer non-real-time data.

- The Ethernet standard allows for several different implementations such as twisted pair and coaxial cable. The maximum length of an Ethernet is determined by the nodes' ability to detect collisions.
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is the most commonly used protocol for LANs. 10BASE5 is generally used as low cost alternative for fiber optic media for use as a backbone segment with in a single building.

b. 802.11 Wifi

- Commonly referred to as Wi-Fi the 802.11 standards define a through-the-air interface between a wireless client and a base station access point or between two or more wireless clients.
- **802.11a :** The 802.11a standard uses the 5 GHz spectrum and has a maximum theoretical 54 Mbps data rate.
- **802.11b :** The 802.11 standard provides a maximum theoretical 11 Mbps data rate in the 2.4 GHz Industrial, Scientific and Medical (ISM) band.

c. 802.16 WiMax

- WiMAX refers to broadband wireless networks that are based on the IEEE 802.16 standard, which ensures compatibility and interoperability between broadband wireless access equipment.
- The 802.16a standard will support OFDM in the 2 to 11 GHz frequency range. The 802.16b standard will operate in the 5 GHz ISM band. A single WiMAX tower can provide coverage to a very large area as big as 3000 square miles.

d. IEEE 802.15.4 Zigbee

- ZigBee communications can reach up to 500 m, with a data rate of up to 250 kbs, for a typical power consumption of 125 to 400 μW.
- As ZigBee is based on IEEE 802.15.4, there is no wake-up signal, but slots for sleep or activity, or in asynchronous mode, devices sleeping anytime they have nothing to say, with an ever-vigilant co-ordinator.

e. Mobile Communication (2G/3G/4G)

- GSM frequencies originally designed on 900 MHz range, now also available on 800 MHz, 1800 MHz and 1900 MHz ranges. The backbone of a GSM network is a telephone network with additional cellular network capabilities.
- 4G is also called as long term evolution. It's promises data transfer rates of 100 Mbps.

Q.23 Explain the following IoT protocols.
a. XMPP b. AMQP c. MQTT d. 6LoWPAN

Ans. : a. XMPP (Extensible Messaging Presence Protocol)

- The XMPP is targeted at delivering instant messages and presence information. It is an open and XML -based protocol.
- Instant Messaging (IM) is a service, where communicating parties typically end users send messages in one- to-one or one -to -many fashion in near real - time.
- An open technology for real-time communication, which powers a wide range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data
- XMPP support server-to-server communication and client-to-server communication.

b. AMQP (Advanced Message Queuing Protocol)

- A protocol to communicate between clients and messaging middleware servers (brokers). The Broker is the AMQP Server.
- AMQP supports both publish-subscribe model and point-to-point communication, routing and queuing.
- AMQP divides the brokering task between exchanges and message queues, where the first is a router that accepts incoming messages and decides which queues to route the messages to and the message queue stores messages and sends them to message consumers.
- AMQP supports username and password authentication as well as SASL authorization. It also supports TLS encryption.

c. MQTT (Message Queue Telemetry Transport)

- MQTT is Open Connectivity for Mobile, M2M and IoT. MQTT is designed for high latency, low-bandwidth or unreliable networks. The design principle minimizes the network bandwidth and device resource requirements .
- MQTT is a lightweight broker-based publish/subscribe messaging protocol designed to be open, simple, lightweight and easy to implement.
- The MQTT protocol works by exchanging a series of MQTT control packets in a defined way. Each control packet has a specific purpose and every bit in the packet is carefully crafted to reduce the data transmitted over the network.
- A MQTT topology has a MQTT server and a MQTT client. MQTT control packet headers are kept as small as possible.
- Having a small header overhead makes this protocol appropriate for IoT by lowering the amount of data transmitted over constrained networks.
- MQTT is the protocol built for M2M and IoT which is used to provide new and revolutionary performance.

d. 6LoWPAN

- IPv6 over Low power Wireless Personal Area Network enables IPv6 in low-power and lossy wireless networks such as WSNs.
- 6LoWPAN defines header compression mechanisms

Q.24 Explain difference between CoAP and MQTT.

Ans. :

Sr. No.	CoAP	MQTT
1.	CoAP uses UDP protocol.	MQTT uses TCP protocol.
2.	It uses request / response messaging.	It uses publish / subscribe messaging.

3.	Communication model is one-to-one.	Communication model is many-to-many.
4.	**Advantages :** • Lightweight and fast • Low overhead • Support for multicasting	**Advantages :** • Simple management • Scalability • Robust communication
5.	**Weakness :** Not as reliable as TCP based MQTT.	**Weakness :** Higher overhead, no multicasting support.
6.	Security type is DTLS.	Security type is SSL/TLS.
7.	Effectiveness in LLN is excellent.	Effectiveness in LLN is low.

END...

Unit V

6 IOT Design and System Engineering

6.1 : IOT Requirements; Hardware and Software

Q.1 What is an Arduino ? Explain its feature.

Ans. : • Arduino is an open-source electronics platform based on easy-to-use hardware and software.

- Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online.
- The Arduino Uno can be powered via the USB connection or with an external power supply. The power source is selected automatically.

Features :

- Support fast computations, ARM based MCU
- AVR micro-controller clock is ATSAMSX8I
- Operating input voltages is 3.3 Volt
- It uses EEPROM, SRAM and Flash memory
- It also support USB and UART

Q.2 Briefly discuss pin of Arduino.

Ans. : • The pins on the Arduino can be configured as either inputs or outputs. Uno R3 includes 14-digital pins which can be used as an input otherwise output by using the functions like pin Mode (), digital Read(), and digital Write().

- These pins can operate with 5V, and every digital pin can give or receive 20mA, and includes a 20 k to 50 k ohm pull up resistor. The maximum current on any pin is 40mA which cannot surpass for

avoiding the microcontroller from the damage. Additionally, some of the pins of an Arduino include specific functions.

Arduino Pin Description

LED	It comes with built-in LED connected through pin 13. Providing HIGH/ LOW value to the pin will turn it ON / OFF.
Vin	It is a 5V input / supply voltage pin to the Arduino Board through a USB port. USB (5V), Vin (7V to 20V) pin, or DC power jack are the 3 ways to provide the power for the board. More voltage provided damages the board.
GND	Ground pins.
Reset	Used to the program running on the board.
PWM	Pins (3,5,6,9,10, 11) is provided by PWM which provides 8-bit output PWM. SPI. It is known as Serial Peripheral Interface. Four pins 10(SS), 11(MOSI), 12(MISO), 13(SCK) provide SPI communication with the help of SPI library.
AREF	Analog Reference (AREF) pin is used for providing a reference voltage to the analog inputs.
TWI	A4, A5 pins are used for Two-Wire Interface (TWI). TWI communication is accessed through wire library.
Rx	It is used to receive data. i.e. used of serial communication.
TX	It is used to transmit data. i.e. used of serial communication
External Interrupts	Pins 2 and 3 are used for providing external interrupts by providing LOW or changing value.

Q.3 What is Raspberry Pi ?

Ans. : Raspberry Pi is the name of a series of single-board computers made by the Raspberry Pi Foundation. The original Pi had a single core 700 MHz CPU and just 256 MB RAM, and the latest model has a quad-core 1.4 GHz CPU with 1 GB RAM.

Q.4 What are the different Raspberry Pi model types ?

Ans. : The Raspberry Pi models are of two types :

1. Model A (Introduced later as a hardware-reduced model)
2. Model B (Introduced first and is the full hardware model)

Q.5 Describe features of Raspberry Pi board.

Ans. : • Features of Raspberry Pi board (Model B - 2 Version) :

1. This second generation Raspberry Pi has an upgraded Broadcom BCM2836 processor, which is a powerful ARM Cortex-A7 based quad-core processor that runs at 900 MHz. The board also features an increase in memory capacity to 1 GB.
2. Ethernet port
3. Two USB ports
4. Two video output options : HDMI or composite
5. 3.5 mm audio output jack
6. 26-pin GPIO header with 0.1" spaced male pins that are compatible with our 2x13 stackable female headers and the female ends of our premium jumper wires.
7. Display Serial Interface (DSI) 15 way flat flex cable connector with two data lanes and a clock lane.

Q.6 How is Raspberry Pi is different from a desktop computer ?

Ans. : • In Raspberry Pi, operating system is installed on SD card whereas in desktop computer, operating system is installed in hard disk.

- Raspberry Pi does not have their own CPU and RAM.
- Processing power of Raspberry Pi is less as compared to desktop computers.
- Raspberry Pi uses less power than desktop computers.

Q.7 Explain difference between Model A and Model B of Raspberry Pi.

Ans. : Difference between Model A and Model B of Raspberry Pi :

Parameters	Model A	Model B
GPU type	VideoCore IV	VideoCore IV
USB port	1	2
Memory	256 MB	512 MB
Ethernet port	No Ethernet port	10/100 Ethernet
SoC Type	Broadcom BCM2837B0	Broadcom BCM2837B0
Number Of Cores	4	4
Type	It is hardware-reduced model	It is full hardware model

Q.8 What is Raspberry Pi ? Explain about its versions and various interfaces in detail.

Ans. : • A Raspberry Pi is a credit card-sized computer originally designed for education, inspired by the 1981, BBC Micro.

- Creator Eben Upton's goal was to create a low-cost device that would improve programming skills and hardware understanding at the pre-university level.
- The Raspberry Pi is slower than a modern laptop or desktop but is still a complete Linux computer and can provide all the expected abilities that implies, at a low-power consumption level.

Versions	Remarks
Raspberry Pi 1	• The original Raspberry Pi had 256 MB of RAM, which increased to 512 MB in a later revision. • It has a 26-way GPIO connector.
Pi Zero	• The Pi Zero includes the GPIO connector, but the header pins are not soldered.

Raspberry Pi 2	• The Raspberry Pi 2 swapped the single-core processor for a much faster quad-core processor and increased the memory to 1 GB RAM
Raspberry Pi 3	• The Raspberry Pi 3 changes the processor to an even more powerful 64-bit processor. • It also adds Wi-Fi and bluetooth which previously needed to be added as a USB device. • The Raspberry Pi 3 Model B was launched in February 2016.

- To get the Raspberry Pi working an SD card needs to be prepared with the Linux operating system installed.
- Raspberry Pi users have made many creative and impressive projects using this device. It can also be programmed to assist in 'housekeeping' your network by functioning as NAS, LDAP server, web server, media server, DNS server etc.
- The Raspberry Pi Foundation recommends Python. Any language which will compile for ARMv6 can be used. It installed by default on the Raspberry Pi : C, C++, Java, Scratch and Ruby.

Q.9 Draw and explain Raspberry Pi block diagram and its components.

Ans. : Fig. Q.9.1 shows the Raspberry Pi board.

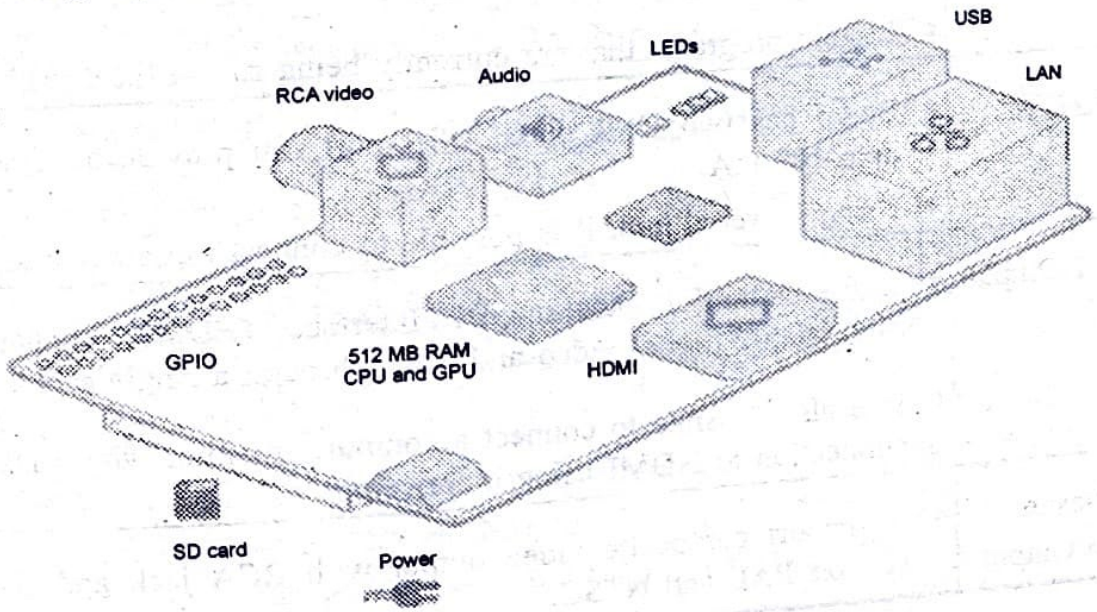

Fig. Q.9.1 Block diagram

- The Raspberry Pi does not have a separate CPU, RAM or GPU. Instead they are all squeezed into one component called a system on chip or SoC unit.
- Raspberry Pi is open hardware with the exception of its primary chip, the Broadcomm SoC which runs the main components of the board - CPU, graphics, memory, USB controller etc.
- All of these Raspberry Pi models share the following features :
  1. **Operating systems :** Raspbian RaspBMC, Arch Linux, Rise OS, Open ELEC Pidora
  2. **Video output :** HDMI Composite RCA
  3. **Supported resolutions :** 640x350 to 1920x1200, including 1080p, PAL and NTSC standards
  4. **Power source :** Micro USB

Components	Description
Processor	• Raspberry Pi uses an ARM processor which is also installed in a wide variety of mobile phones. • This CPU is single core, however it does have a co-processor to perform floating point calculations.
Memory	• Model B Raspberry Pi has 512 MB SDRAM (Synchronous Dynamic RAM). • It store programs that are currently being run in the CPU.
USB ports	• Board has two USB ports. USB port can provide a current upto 100 mA. • Using powered hub, it is possible to connect more devices.
HDMI Output	• High Definition Multimedia Interface (HDMI) supports high-quality digital video and audio through a single cable. • It is also possible to connect a computer monitor with a DVI connection to HDMI using a converter.
Composite Video Output	• It support composite video output with RCA jack and also support PAL and NTSC.

	• The TVDAC pin can be used to output composite video
Audio Output	• Audio output jack is 3.5 mm. • This jack is used for providing audio output to old television along with the RCA jack for video
GPIO Pins	• Both models have a total of 26 GPIO pins, organized into one pin header, named the P1 header • The newer Raspberry Pi adds 8 more GPIO pins in a new pin header called P5 • Not all the GPIO pins are programmable. Some of them are 5.0 VDC or 3.3 VDC positive power pins, some of them are negative ground pins and a few of them are marked DNC (do not connect). • The P1 header has 17 programmable pins and the P5 header adds 4 more. • Reading from various environmental sensors. Writing output to dc motors, LEDs for status.
Power Input	• Micro-USB connector is used for power input.
Status LED	• It has five status LED.
CSI	• Camera Serial Interface (CSI) can be used to connect a camera module to Raspberry Pi.
SD Card Slot	• This card is used for loading operating system.

Q.10 What is the use of GPIO pins ?

Ans. : • The Raspberry Pi comes with a set of 26 exposed vertical pins on the board. These pins are a General Purpose Input/Output(GP10) interface that is purposely not linked to any specific native function on the Raspberry Pi board.

- Instead, the GPIO pins are there explicitly for the end user to have low-level hardware access directly to the board for the purposes of attaching other hardware boards, peripherals, LCD display screens and other hardware devices to the Pi.

- The Raspberry Pi draws its power from a microUSB port and requires a micro USB to AC adapter. Because the Pi is a micro computer and not simply a cell phone getting a battery topped off, you need to use a high quality charger with stable power delivery that provides a consistent 5 V with at least 700 mA minimum output for older model units and 2.5 A for the Pi 3.

Q.11 What are the criteria's for selection of controllers in Embedded Products ? ☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. : • Power efficiency : There is a trade-off between processing performance and power consumption : A device with higher processing power will consume more energy.

- Hardware architecture : A microcontroller's packaging directly influences its size and performance. Dual in-line packaging is the most common type.
- Memory : The amount of memory (RAM and ROM) we need will depend on the programs you will be running. More programs need more random access memory.
- Hardware interface : The nature of the task will dictate the need for hardware interfaces such as USB, Wi-Fi, Bluetooth, audio, video, or camera.
- Software architecture : Some microcontrollers are operable on multiple OSs, and others are not.
- Cost : Microcontrollers fall within a wide price range, from a hundred units for a few rupees to a few rupees per unit.
- Security : Hacking which targets IoT devices is rising, a threat that is especially relevant to microcontrollers used in automobiles. In response, microcontroller makers are implementing layers of security such as cryptography and physical security.
- Temperature tolerance : Depending on the environment in which your microcontrollers operate, we may want devices that withstand extreme temperature. There will be a trade-off between temperature tolerance and cost.

6.2 : Study of IOT Sensors

Q.12 Define sensor. What is active and passive sensor ?

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.).

- 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 power source.

Q.13 Explain specification of sensor.

Ans. : Specifications 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 can make.
3. **Sensitivity :** The ratio between the change in the output signal to a small change in input physical signal. Slope of the input-output fit line.
4. **Repeatability / Precision :** The ability of the sensor to output the same value for the same input over a number of trials.
5. **Bandwidth :** The frequency range between the lower and upper cut-off frequencies, within which the sensor transfer function is constant gain or linear.

Q.14 Explain sensor components.

Ans. : • Fig. Q.14.1 shows sensor node. A basic sensor node comprises five main components.

1. **Controller :** A controller to process all the relevant data, capable of executing arbitrary code.
2. **Memory :** Some memory to store programs and intermediate data; usually, different types of memory are used for programs and data.

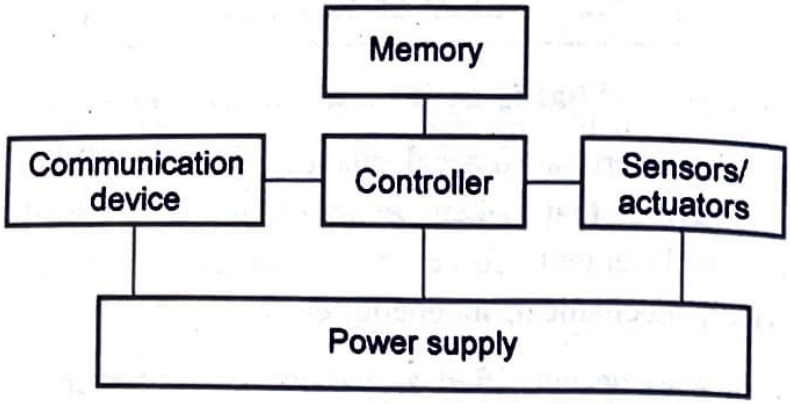

Fig. Q.14.1 Components of sensor node

3. **Sensors and actuators :** The actual interface to the physical world : Devices that can observe or control physical parameters of the environment.
4. **Communication :** Turning nodes into a network requires a device for sending and receiving information over a wireless channel.
5. **Power supply :** As usually no tethered power supply is available, some form of batteries is necessary to provide energy. Sometimes, some form of recharging by obtaining energy from the environment is available as well.

Q.15 Explain various types of sensors.

Ans. : Sensors can be roughly categorized into three categories :

1. **Passive, omnidirectional sensors :** These sensors can measure a physical quantity at the point of the sensor node without actually manipulating the environment by active probing. In this sense, they are passive. Moreover, some of these sensors actually are self-powered in the sense that they obtain the energy they need from the environment.
   - Typical examples for such sensors include thermometer, light sensors, vibration, microphones, humidity, mechanical stress or tension in materials, chemical sensors sensitive for given substances, smoke detectors, air pressure and so on.
2. **Passive, narrow-beam sensors :** These sensors are passive as well, but have a well-defined notion of direction of measurement. A typical example is a camera, which can "take measurements" in a given direction, but has to be rotated if need be.

3. **Active sensors :** This last group of sensors actively probes the environment, for example, a sonar or radar sensor or some types of seismic sensors, which generate shock waves by small explosions. These are quite specific, triggering an explosion is certainly not a lightly undertaken action and require quite special attention.

- **Active sensors :** Require an external source of power (excitation voltage) that provides the majority of the output power of the signal
- **Passive sensors :** The output power is almost entirely provided by the measured signal without an excitation voltage.
- **Digital sensors :** The signal produced or reflected by the sensor is binary.
- Analogue sensors produce a continuous output signal or voltage which is generally proportional to the quantity being measured.

Q.16 Explain the difference between actuators and sensor.

Ans. :

Sr. No.	Actuators	Sensor
1.	It is output device.	It is input device.
2.	Converts an electrical signal to a physical output.	Converts a physical parameter to an electrical output.
3.	A component of a machine that is responsible for moving and controlling mechanism.	A device that detects events or changes in the environment and send that information to another electronic device.
4.	It helps to control the environment or physical changes.	It help to monitor the changes in the environment.

6.3 : IOT Design

Q.17 Explain IoT design methodology steps.

Ans. : • The rise of the Internet of Things has led to an explosion of new sensor computing plat - forms. The complexity and application domains of

IoT devices range from simple self - monitoring devices in vending machines to complex interactive devices with artificial intelligence in smart vehicles and drones.

- As IoT developers wish to meet more aggressive platform objectives and protect market share through feature differentiation, they must choose between low-cost, and low-performance CPU-based Commercial - Off - The - Shelf (COTS) systems, and high-performance custom platforms with hardware accelerators such as GPU and FPGA.
- An IoT platform facilitates communication, data flow, device management, and the functionality of applications. The goal is to build IoT applications within an IoT platform framework. The IoT platform allows applications to connect machines, devices, applications, and people to data and control centers.
- Home automation can be described as introduction of technology within the home environment to provide convenience, comfort, security and energy efficiency to its occupants.
- A home automation system can involve switching off electrical appliances like air-conditioners or refrigerators when a desired temperature has been reached, then switching on again when the temperature has crossed a certain value
- Fig Q.17.1 shows design methodology steps.

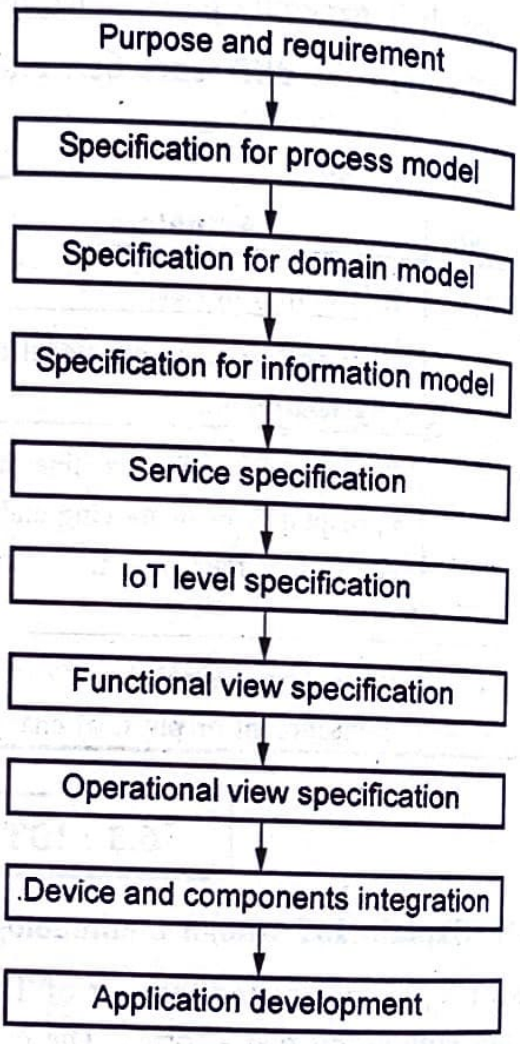

Fig. Q.17.1 Design methodology steps

- Sensors : Sensors are the eyes of a home automation system. They "see" the environment and convert what they find into an electrical quantity that can be measured by a microcontroller or system processor.
- Remote Connectivity : Depending on need and various design considerations, users may need to be able to control the system and appliances remotely.

Q.18 Explain IoT Information model specification.

☞ **[SPPU: June-22, End Sem, Marks 9]**

Ans. : • An abstract description (UML diagram or ontology) for explaining information about elements or concepts defined in the IoT Domain Model.

- The information model models domain model concepts that are to be explicitly represented and manipulated in the digital world. In addition the information model explicitly models relations between these concepts.
- Fig Q.18.1 shows information model. The information model is a meta model that provides a structure for the information. This structure provides the basis for defining the functional interfaces.
- IoT Information Model is represented using Unified Modeling Language (UML) diagram. The IoT Information Model maintains the necessary information about Virtual Entities and their properties or attributes.
- The information model for an object can contain information about the objects structure and resource types. This can enable APIs to automatically be composed by middleware and automatically consumed by application software.
- Additional metadata can indicate context, such as geographical location, and bindings, such as message protocols and event handlers, as well as access control information.
- The IoT Information Model describes Virtual Entities and their attributes that have one or more values annotated with meta-information or metadata. The attribute values are updated as a result of the associated services to a Virtual Entity.

- The physical interaction is the result of the intention of the human to achieve a certain goal. Fig. Q.20.2 shows IoT domain model.

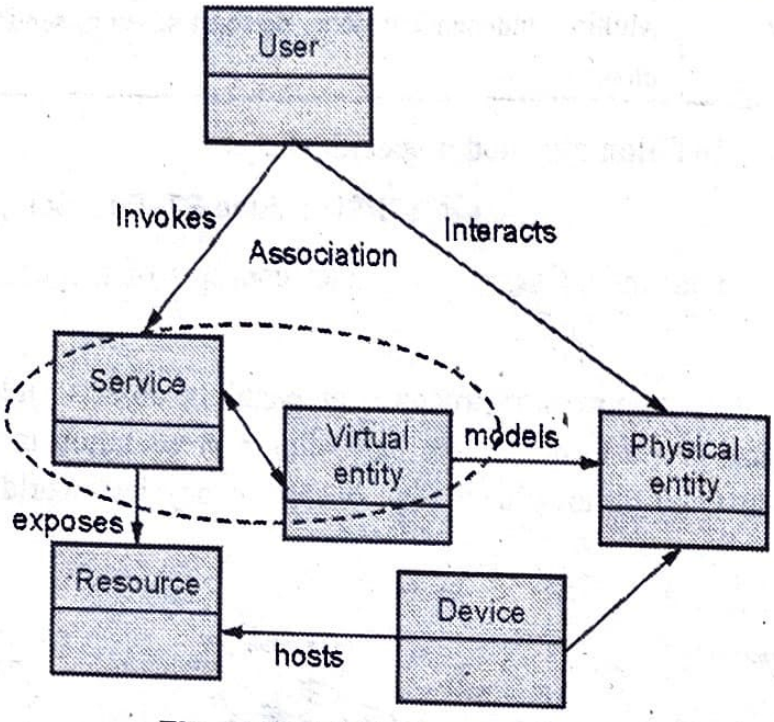

Fig. Q.20.2 IoT Domain model

- A Physical entity, as the model shows, can potentially contain other physical entities; for example, a building is made up of several floors, and each floor has several rooms.
- A Physical entity is represented in the digital world as a Virtual entity. A Virtual entity can be a database entry, a geographical model, an image or avatar, or any other Digital Artifact.

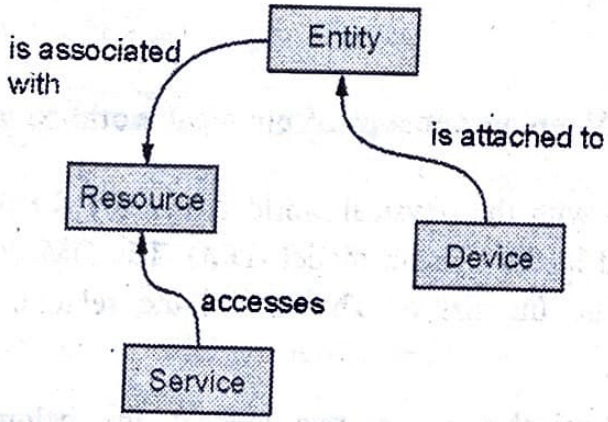

Fig. Q.20.3 Key concepts and interaction in IoT model

- The relations between services and entities are modeled as associations. These associations could be static, e.g. in case the device is embedded into the entity; they could also be dynamic, e.g., if a device from the environment is monitoring a mobile entity. These identified concepts of the IoT domain and the relations between them are depicted in Fig Q.20.3.
- One physical entity can be represented by multiple virtual entities, each serving a different purpose. For the IoT domain Model, three kinds of device types are the most important :
  1. **Sensors :** These are simple or complex devices and contain a transducer that converts physical properties such as temperature into electrical signals. These devices include the necessary conversion of analog electrical signals into digital signals.
  2. **Actuators :** These devices that involve a transducer that converts electrical signals to a change in a physical property.
  3. **Tags :** Tags in general identify the Physical entity that they are attached to.
- Home Automation System Example :
  1. **Physical entity :** Room in the home and room temperature
  2. **Device :** Single board mini computer with sensor and relay switch
  3. **Resources :** Operating system which runs on mini computer
  4. **Services :** Mode selection, controller service which runs services on the device, retrieve the room temp.

Q.21 Explain IoT operational view specification.

☞ **[SPPU: June-22, End Sem, Marks 9]**

Ans. : • Deployment and operational view depends on the specific actual use case and requirements. Smart object in the IoT uses different methods for communication using different technology.

- Hence the deployment and operation view is very important to address how actual system can be realized by selecting technologies and making them communicate and operate in a comprehensive way.
- It provides an IoT Reference Model with a set of guidelines to application users. The different design choices that they have to face while designing the actual implementation of their services.

- The viewpoints used in the deployment and operation view are the following :
  1) The IoT domain model diagram is used as a guideline to describe the specific application domain.
  2) The functional model is used as a reference to the system definition.
  3) Network connectivity diagrams can be used to plan the connectivity topology to enable the desired networking capability of the target application; at the deployment level, the connectivity diagram will be used to define the hierarchies and the type of the sub-networks composing the complete system network;
  4) Device descriptions can be used to map actual hardware on the service and resource requirements of the target system.

6.4 : SIM Card Technology

Q.22 Explain Various IoT sim card technologies.

☞ [SPPU : June-22, End Sem, Marks 9]

Ans. : • Fig. Q.22.1 shows IoT SIM card.

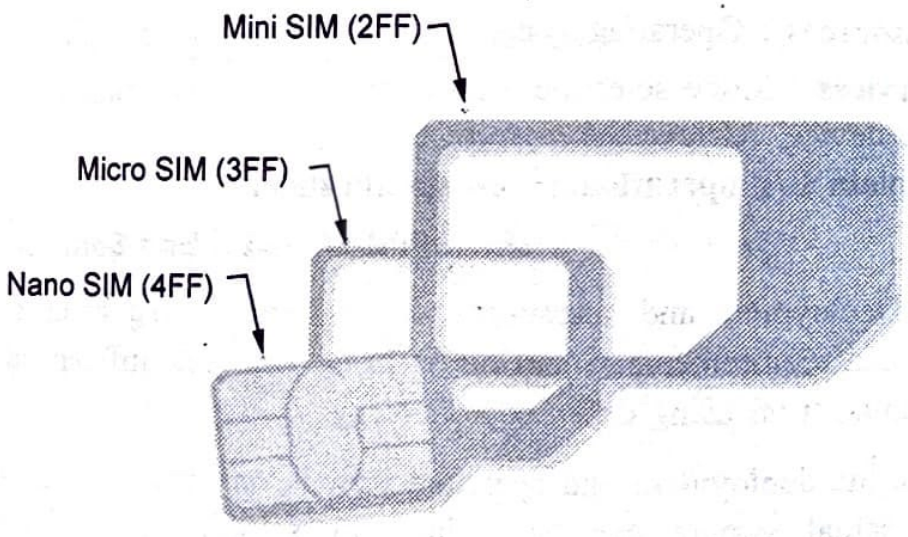

Fig. Q.22.1 IoT SIM card

1. Full - Size (1FF) : This is the largest M2M SIM card, about the size of a credit card. For the most part, it has been phased out by smaller, modern SIMs.

2. Mini - SIM (2FF) : This is the industry standard SIM card size, measuring 25 mm × 15 mm × 0.76 mm. It's typically used in devices like vehicles, vending machines and payment points.
3. Micro - SIM (3FF) : The micro-SIM is half the size of the mini and is used in portable devices like tablets, GPS, mHealth and other mobile IoT devices.
4. Nano - SIM (4FF) : The nano-SIM is 40 % smaller than the micro variation, making, it great for small IoT devices. These SIMs have relatively little protection so they're not recommended for harsh environments.
5. eSIM (MFF2) : Embedded SIMs, also known as eSIMs, measure only 6 mm × 5 mm × 1 mm. These are the most popular IoT SIM because of their convenient size and durability. The card is not removable or interchangeable.

- SIM cards typically store a set of authentication cardentials which help keep their data secure.

Q.23 What are the application of SIM card ?

Ans. : • Applications :

1. Wearables - Smart watches and fitness trackers are already popular and smart glasses are beginning.
2. Home automation devices - From smart lighting, to thermostat control and even windows, fridges and alarms.
3. Agricultural sensors - Have revolutionized the way that farms are managed, with livestock tracking and weather and soil monitoring.
4. Healthcare monitors - Provide doctors with a patients physical data - like blood pressure and heart rate - So they can make more informed recommendations remotely.
5. Logistics and fleet management sensors - Allow businesses to track locations and progress in real time.

6.5 : IOT Security

Q.24 What are different security parameters considered while designing any IoT system ? ☞ **[SPPU : June-22, End Sem, Marks 9]**

Ans. : • IoT enables a constant transfer and sharing of data among things and users. In such a sharing environment, authentication, authorization, access control and non-repudiation are important to ensure secure communication.

- The high level of heterogeneity, coupled to the wide scale of IoT systems, is expected to magnify security threats of the current Internet. The high number of inter-connected devices arises scalability issues.
- IoT systems integrate in a seamless way physical objects, data and computing devices into a global network of information about "smart things".
- Fig. Q.24.1 shows high level security challenges of IoT.

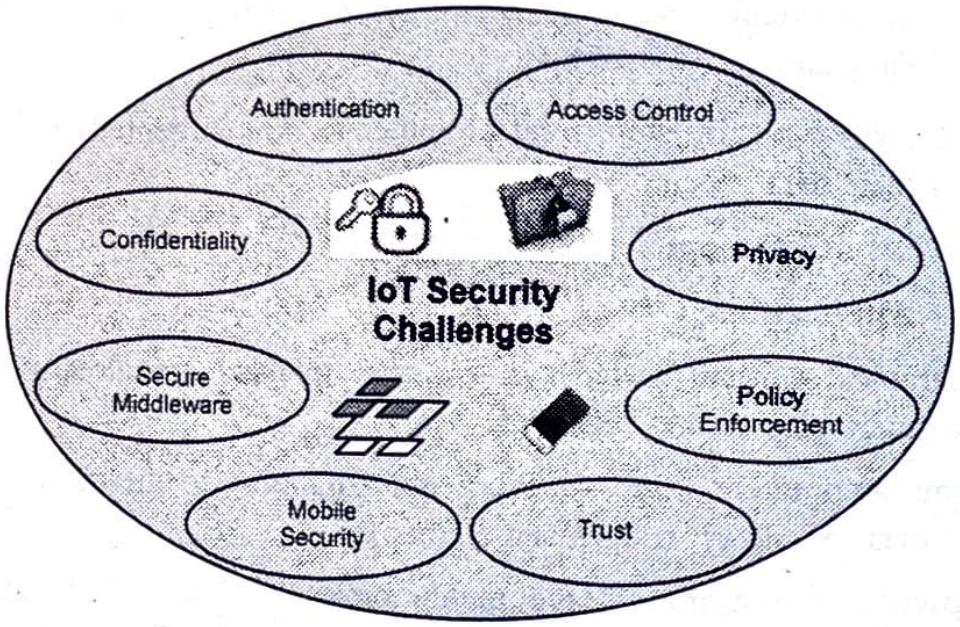

Fig. Q.24.1 IoT security challenges

- Access control refers to the permissions in the usage of resources, assigned to different actors of a wide IoT network.
- System safety is highly application - or application domain-specific. Trust Model that provides data integrity and confidentiality, and endpoint authentication and non-repudiation between any two system-entities that interact with each other.
- The trust requirements in IoT are related to identify management and access control issues. The IoT-A Privacy Model depends on the following functional components : Identity Management, authentication, authorization, trust and reputation.

- Communication security : IoT systems are heterogeneous. Not only because of the variety of the entities involved, but also because they include devices with various capabilities in terms of communication and processing.
- Communication security model must not only consider the hetereogenity of the system, but it also should guarantee a balance between security features, bandwidth, power supply and processing capabilities.
- IoT devices face many threats, including malicious data that can be sent over authenticated connections, exploiting vulnerabilities. Such attacks frequently exploit many weaknesses, including but not limited to :

  a) Failure to use code signature verification and secure boot and

  b) Poorly implemented verification models which can be bypassed.
- Attackers often use those weaknesses to install backdoors, sniffers, data collection software, file transfer capabilities to extract sensitive information from the system, and sometimes even Command & Control (C&C) infrastructure to manipulate system behavior.
- The security challenges are as follows :

  a. Devices are not reachable : Most of the time a device is not connected.

  b. Devices can be lost and stolen : Makes security difficult when the device is not connected.

  c. Devices are not crypto-engines : Strong security difficult without processing power.

  d. Devices have finite life : Credentials need to be tied to lifetime.

  e. Devices are transportable : Will cross borders.
- IoT system has a cloud database that is connected to all your devices. These devices are connected to the internet and it could be accessed by the cybercriminals and hackers. As the number of connected devices increases, chances for hackers to breach the security system gets increased.

Q.25 Explain vulnerabilities of IoT.

Ans. : • IoT devices are vulnerable largely because these devices lack the necessary built-in security to counter threats. Aside from the technical aspects, users also contribute to the device's vulnerability to threats. Here are some of the reasons these smart devices remain vulnerable :

1. Limited computational abilities and hardware limitations.
2. Heterogeneous transmission technology.
3. Components of the device are vulnerable.
4. Users lacking security awareness. Lack of user security awareness could expose smart devices to vulnerabilities and attack openings.

- An IoT device can have one or multiple vulnerabilities that make it an easy target for hackers to gain access to a network and move laterally to more critical devices or systems.
- IoT vulnerabilities due to participation of the number of layers, hardware sublayers and software in applications and services.
- The nature of IoT Vulnerabilities varies, for example, sensors, machines, automobiles, wearables, and so on. Each faces different kind of vulnerabilities and has complex security and privacy issues.

Q.26 Explain various possible attacks on IoT layers.

Ans. : • Various possible attacks in different layers of IoT.

- There are various attack surfaces available for attackers, protection needs to be considered at three different layers :
  1) **Edge protection :** Ensures device, mobile app and web app integrity to prevent devices from becoming attack entry points.
  2) **Network protection :** Secures communication channels to prevent man-in-the-middle attacks.
  3) **Cloud protection :** Assures data privacy and prevents data leakage.

Q.27 What are security principles of IoT ?

Ans. : • The security of the Internet of Things, the following principles can be established.

a) **Identity** : Trust is always tied to an identity. Therefore every device needs a unique identity that can't be changed. The device must also be able to prove its identity at all times.

b) **Positive intention** : The device and linked service have positive intentions.

c) **Predictability and transparency** : The functional scope of the service provided by devices is known to its full extent. There are no undocumented (secret) functions. The behaviour of the system can be checked at any time by independent third parties.

d) **Reputation** : An increasing number of positive interactions between the things gradually form a reputation based intelligent network.

Q.28 Explain key elements of IoT security.

Ans. : • Fig. Q.28.1 shows key elements of IoT security.

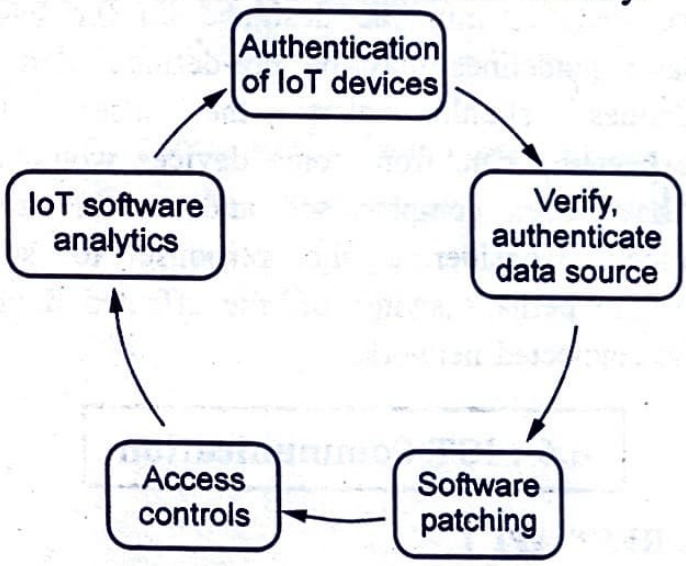

Fig. Q.28.1 Elements of IoT security

- **Authenticate IoT devices** before they integrate with the centralized network. This step avoids the risk of spoofing attacks on the IoT device which appears as a legitimate device on your network. Attacked devices collect data from other networked device or transmit malicious data to remaining devices on the network.
- It is essential to authenticate and verify software source running on your IoT device. Software not authenticated faces the risk of being compromised and the device cannot detect such tampering issues unless software is supported with a digital signature of the vendor.

- **Software patching** avoids the IoT device from being compromised. However, software updates from authenticated sources must be accepted only. Software patches minimize risks of data loss or interference with business operations. For instance, a device is put for updating; all local data is written on a central network, other devices know when the updating device goes offline and the update is performed, verified before returning back to the operational mode.
- **Access controls secure** IoT devices as well as the enterprise. Users are assigned roles to perform specific operations. Roles include querying current state of the IoT devices, software updates on these devices and change device configurations. Other systems present on the network work on the principle of least privilege that allows users only a minimal set of privileges to perform business functions and technical processes. This method restricts damage caused due to a security breach of user's personal data.
- **IoT software** analytics must be designed on the basis of anomaly detection. Basic guidelines may be pre-defined, and variation from these guidelines should alert the user. For instance, higher-than-expected traffic from some devices would alert users that the devices have been compromised and are in use even after a malicious attack. Considering the response to such anomalous behavior, you can perhaps switch off the affected devices or remove them from the connected network.

6.6 : IOT Communication

Q.29 What is a REST API ?

Ans. : • REST or RESTful API design (Representational State Transfer) is designed to take advantage of existing protocols.

- While REST can be used over nearly any protocol, it usually takes advantage of HTTP when used for Web APIs.
- REST has the ability to handle multiple types of calls, return different data formats and even change structurally with the correct implementation of hypermedia.

- This freedom and flexibility inherent in REST API design allow you to build an API that meets your needs while also meeting the needs of very diverse customers.
- Unlike SOAP, REST is not constrained to XML, but instead can return XML, JSON, YAML or any other format depending on what the client requests.
- And unlike RPC, users aren't required to know procedure names or specific parameters in a specific order.
- However, there are drawbacks to REST API design. You can lose the ability to maintain state in REST, such as within sessions, and it can be more difficult for newer developers to use.
- It's also important to understand what makes a REST API RESTful, and why these constraints exist before building your API.
- Important REST principles are as follows :
  1. **Stateless :** No client context stored on the server, each request is complete.
  2. **Cacheable :** Responses explicitly indicate their cacheability.
  3. **Layered system :** Client cannot tell if connected directly to the server (e.g. reverse proxies).
  4. **URIs :** Resources are identified using Uniform Resource Identifiers(URIs).

END...

Unit VI

7 IOT Applications

7.1 : IOT Verticals

Q.1 Write a short note on IoT vertical applications.

☞ [SPPU : June-22, End Sem, Marks 6]

Ans. : • IoT verticals include agriculture and farming, energy, oil and gas, enterprise, finance, healthcare, industrial, retail and transportations. In addition, energy is about managing smart meters, smart buildings and smart cities, while oil and gas is more about process and asset management in the petroleum industry.

- Fig. Q.1.1 shows IoT vertical applications.
- In the vertical business model, the IoT device, the gateway and the cloud-based service are all provided and controlled by the same company. This approach has the advantage for the end-user that there are no compatibility issues to deal with among the various elements and a single point of contact to deal with if anything goes wrong.
- The disadvantages are that the end-user is entirely dependent on the vendor for improvements, enhancements, or upgrades to the offering.
- An IoT home-security system that monitors an empty house for intruders, for instance, has the same hardware as one that monitors an elderly person's activity, if the person falls or loses consciousness. But if someone wants a system that will do both, they are dependent on the system vendor to offer those features when dealing with a vertically defined business.
- Vertical business models can also result in users needing several different systems to achieve a spectrum of tasks, each with its own gateway and cloud operations.

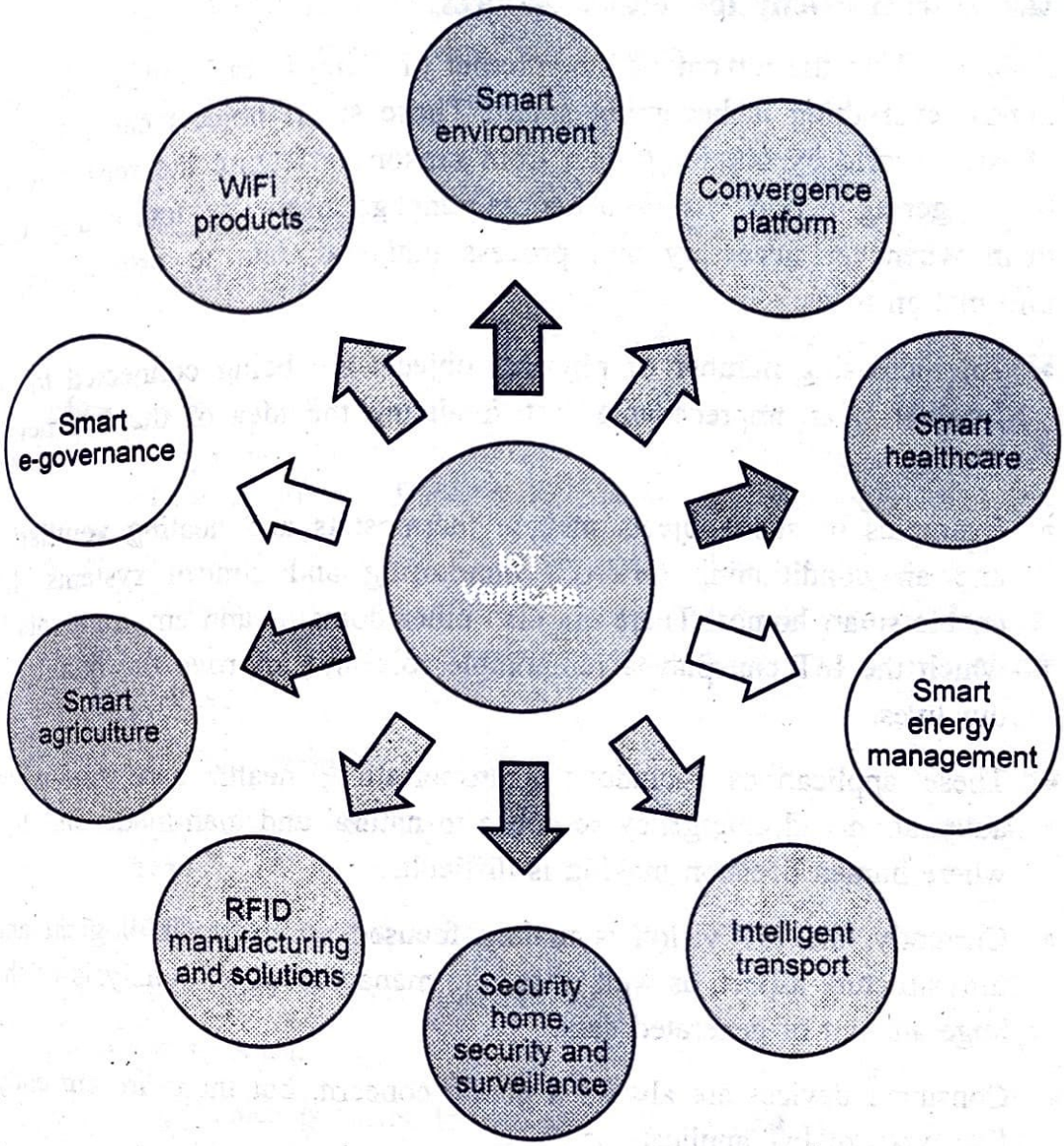

Fig. Q.1.1 IoT vertical applications

- Most of the first IoT offerings to come to market follow this vertical model.
- The motivation behind a horizontal model is to foster rapid growth and innovation in the industry by allowing multiple providers to work with a common framework. The idea is that by making the gateway and cloud resources something that can be assumed to be in place and have known and open functionality, innovators can concentrate their efforts on creating devices and services.

Q.2 Discuss briefly IoT hosted services.

Ans. : • With the advent of the Internet of Things era, homes, cities and almost everything is becoming smart. Those smart objects can sense the physical world by obtaining data from sensors, affecting the sensed world by triggering actions using actuators, engage users by interacting with them whenever necessary and process gathered data to provide useful information to us.

- An increasing number of physical objects are being connected to the Internet at an unprecedented rate realizing the idea of the Internet of Things.
- Examples of such objects include thermostats and heating ventilation and air conditioning (HVAC) monitoring and control systems that enable smart homes. There are also other domains and environments in which the IoT can play a remarkable role and improve the quality of our lives.
- These applications include : Transportation, health care, industrial automation and emergency response to natural and man-made disasters where human decision making is difficult.
- Currently, the IoT vision is mainly focused on the technological and infrastructure aspect, as well as on the management and analysis of the huge amount of generated data.
- Consumer devices are always a public concern, but there are currently five types of IoT applications :
  - **a) Consumer IoT :** Such as light fixtures, home appliances and voice assistance for the elderly.
  - **b) Commercial IoT :** IoT applications in the healthcare and transport industries, such as smart pacemakers, monitoring systems and vehicle to vehicle communication (V2V).
  - **c) The Industrial Internet of Things :** IIoT includes digital control systems, statistical evaluation, smart agriculture and big industrial data.
  - **d)** Infrastructure IoT enables the connectivity of smart cities through infrastructure sensors, management systems and user-friendly user apps.

e) Military Things (IoMT) applying IoT technologies in the military field, such as robots for surveillance and human-wearable biometrics for combat.

7.2 : IoT Application Development

Q.3 Explain voice application for IoT device.

☞ **[SPPU : June-22, End Sem, Marks 6]**

Ans. : IoT applications development is also called **M2M app development.** IoT is a connectivity of all physical devices which are connected through internet and able to exchange (send and receive) data.

- The objects include vehicles, smart phones, gadgets, wearable devices, home appliances and many other physical devices as well as human. IoT app works as a bridge enables physical devices to communicate with each other.
- **Example :** Voice App for IoT Device

  There will be three types of voice communication in IoT environments :

  1. Bi - directional voice communication
  2. Mono - directional voice communication
  3. Voice recognition.
- Reasons that voice is suited to a range of IoT applications :
  1. Speech is the natural mode of communication for humans. It is both intuitive and easier to convey commands verbally.
  2. Voice recognition is particularly appealing when the human's hands or eyes are otherwise occupied.
  3. Voice telephony is an efficient means of bi - directional voice communication with machines that can listen and respond without the need for complex commands.
  4. Cost saving factors : Voice integration could potentially challenge the need for a touch screen on many devices, as it reduces the cost for devices that will be dormant for the majority of the time.

- The IoT market is broad and encompasses a range of consumer, commercial and industrial applications where voice can play a role. There are significant differences between the drivers for implementing voice into consumer products and from those that drive the same technology in the consumer market.

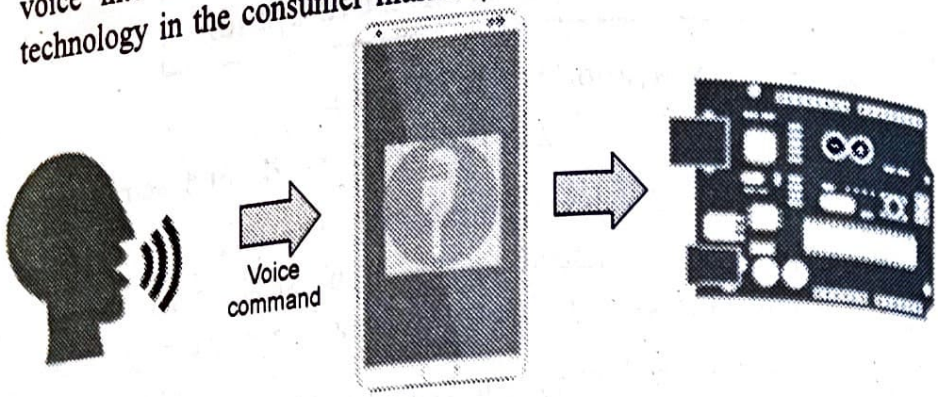

Fig. Q.3.1

- Voice is a feature that does not need to make any consideration for infrastructure, other than the need for an Internet connection.
- Consumer applications for voice include virtual assistants on smartphones as well as devices that do not include integrated telephony functions, such as wearable devices with minimal screen real - estate.
- Devices in this category include smartwatches and fitness wearables that can offer hands - free voice activation of a multitude of functions, through to smart televisions and games consoles.

Alexa Voice Service (AVS) Integration for AWS IoT

- Alexa Voice Service (AVS) Integration for AWS IoT is a new feature that cost - effectively brings Alexa Voice to any connected device without incurring messaging costs.
- AVS for AWS IoT has three components :
  1. A set of reserved MQTT topics to transfer audio messages between Alexa enabled devices and AVS.
  2. A virtual alexa enabled device in the cloud that shifts tasks related to media retrieval, audio decoding, audio mixing and state management from the physical device to the virtual device.
  3. A set of APIs that support receiving and sending messages over the reserved topics, interfacing with the device microphone and speaker and managing device state.

Q.4 What is Django ? Explain Django architecture and template system.

Ans. : • Django is a open source Python web development framework. Django is based on the well known **model-template-view** architecture. It provides a unified API to a database back end.

- Django is often referred to as an MTV framework. In the MTV development pattern :
  1. M stands for "Model," the data access layer. This layer contains anything and everything about the data : How to access it, how to validate it, which behaviors it has and the relationships between the data.
  2. T stands for "Template," the presentation layer. This layer contains presentation-related decisions : How something should be displayed on a Web page or other type of document.
  3. V stands for "View," the business logic layer. This layer contains the logic that accesses the model and defers to the appropriate template(s). You can think of it as the bridge between models and templates.
- Django was built using Python, an object-oriented applications development language which combines the power of systems languages, such as C/C++ and Java, with the ease and rapid development of scripting languages, such as Ruby and Visual Basic.

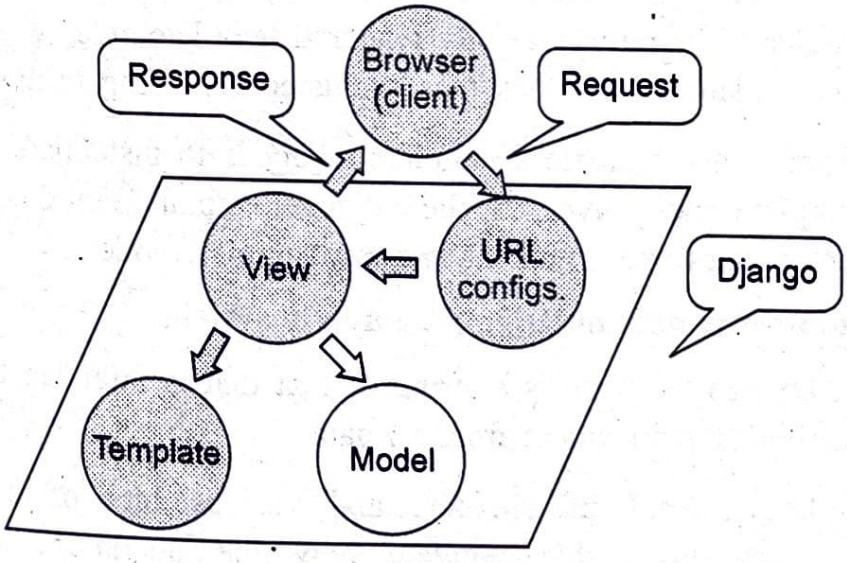

Fig. Q.4.1 Django architecture

- DJANGO MVC - MVT Pattern : The Model-View-Template (MVT) is slightly different from MVC. In fact the main difference between the two patterns is that Django itself takes care of the controller part (Software code that controls the interactions between the model and view), leaving us with the template.

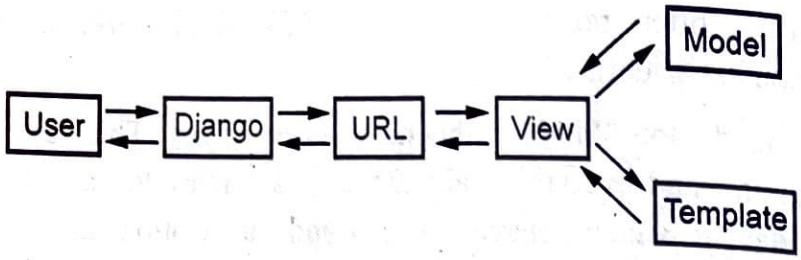

Fig. Q.4.2 MVT/MVC

- A Django template is a string of text that is intended to separate the presentation of a document from its data.
- A template defines placeholders and various bits of basic logic (i.e., template tags) that regulate how the document should be displayed.
- To use the template system in Python code, just follow these two steps :
  1. Create a template object by providing the raw template code as a string. Django also offers a way to create template objects by designating the path to a template file on the filesystem; we'll examine that in a bit.
  2. Call the render() method of the template object with a given set of variables. This returns a fully rendered template as a string, with all of the variables and block tags evaluated according to the context.
- The easiest way to create a template object is to instantiate it directly. The template class lives in the "django.template" module, and the constructor takes one argument, the raw template code.

Q.5 Write a short note on Django template system.

Ans. : • A Django template is a string of text that is intended to separate the presentation of a document from its data.

- A template defines placeholders and various bits of basic logic (i.e. template tags) that regulate how the document should be displayed.

- To use the template system in Python code, just follow these two steps :
  1. Create a template object by providing the raw template code as a string. Django also offers a way to create template objects by designating the path to a template file on the filesystem; we'll examine that in a bit.
  2. Call the render() method of the template object with a given set of variables. This returns a fully rendered template as a string, with all of the variables and block tags evaluated according to the context.
- The easiest way to create a template object is to instantiate it directly. The template class lives in the "django.template" module, and the constructor takes one argument, the raw template code.

7.3 : IoT Connectivity

Q.6 What is IoT connectivity ? Explain elements of IoT connectivity.

Ans. : • IoT connectivity is typically how we refer to the methods used to connect IoT devices, methods including applications, sensors, trackers, gateways and network routers.

- Elements of connectivity are as follows :
  - **a) Power consumption :** How much battery does it consume ?
  - **b) Range :** How wide is the area it covers ?
  - **c) Bandwidth :** How much data does it transmit ?
  - **d) Reliability :** How reliable is the connectivity and what is your network operator coverage ?
  - **e) Cost :** How expensive is the connectivity ?
- Cellular IoT connectivity : Cellular connectivity also referred to as satellite connection. It is typically used in machine-to-machine (M2M) IoT connectivity.
- WiFi : When it comes to connecting IoT devices, WiFi can work well for smaller gadgets and appliances within a certain coverage range.
- Bluetooth had a competitive bandwidth of 2 Mbps but only has low range capabilities of below 30 ft (10 m). Bluetooth connectivity is a

great IoT connectivity option if you're looking to send information across a close range, with medium to low bandwidth.

- LoRa is Long Range, low data rate, low power wireless platform technology for building IoT network. LoRa is a patented digital wireless data communication IoT technology developed by Cycleo of Grenoble, France.
- LoRaWAN is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery-operated things in a regional, national or global network.

7.4 : IOT Software Providers

Q.7 What is Amazon Web Services ?

Ans. : • Amazon Web Services (AWS) is a collection of remote computing services (web services) that together make up a cloud computing platform, offered over the Internet by Amazon.com.

- The AWS cloud infrastructure is built around regions and availability zones (Azs). A region is a physical location in the world where we have multiple Azs. Azs consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities.
- These Azs offer you the ability to operate production applications and databases that are more highly available, fault tolerant and scalable than would be possible from a single data center.
- The AWS cloud operates 42 AZs within 16 geographic regions around the world, with five more availability zones and two more regions coming online in 2017.
- Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains.

Q.8 Elaborate on the Amazon web services for IoT.

Ans. : • AWS offers Internet of Things (IoT) services and solutions to connect and manage billions of devices. Collect, store and analyze IoT data for industrial, consumer, commercial and automotive workloads.

- AWS IoT allows Internet-connected devices such as sensors, embedded devices, and applications to connect and communicate over the AWS cloud. IoT applications collect the information and process, it sends messages in JSON format on MQTT topics.
- AWS IoT will integrate with Lambda, Amazon Kinesis, Amazon S3, Amazon Machine Learning and Amazon DynamoDB to build IoT applications, manage infrastructure and analyze data. Fig. Q.8.1 shows AWS IoT.

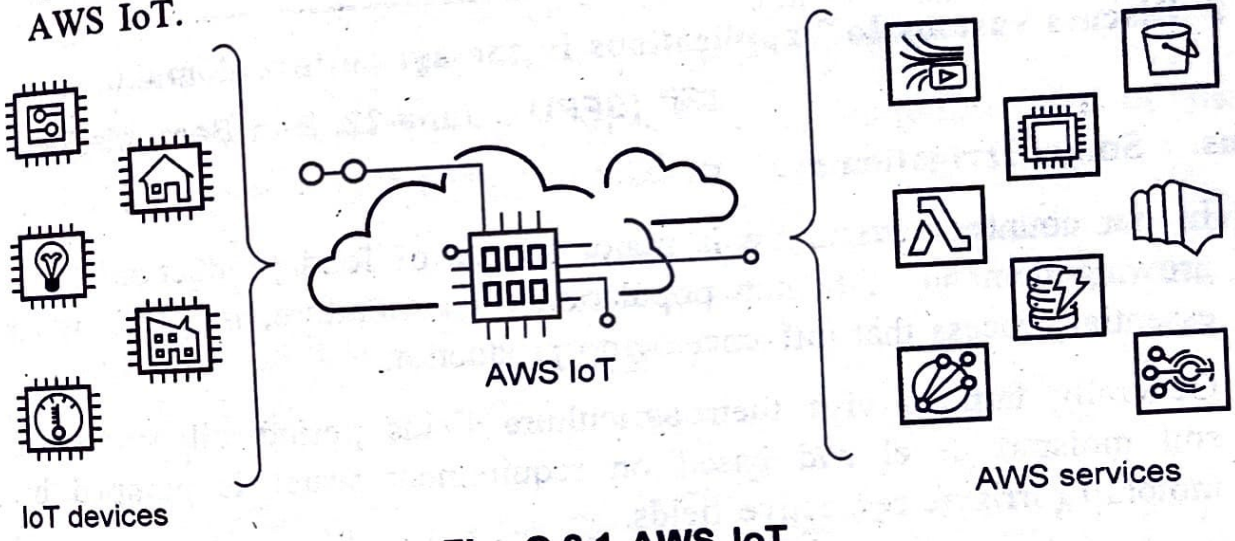

Fig. Q.8.1 AWS IoT

- Every MQTT can trace the device when it gets updated. When a message is sent across on the MQTT topic, it's passed to the MQTT message broker which distributes that message on the MQTT topic to the users who have subscribed to that topic.
- The communication via the Internet-connected devices and the AWS IoT is secured through X.509 certificates. AWS IoT certificate has to be registered and activated using AWS IoT, to communicate with AWS IoT device we can then copy it onto your device which acts as a credential.
- AWS IoT Core supports following protocols :
  a) MQTT (Message Queuing and Telemetry Transport)
  b) MQTT over WSS (Websockets Secure)

c) HTTPS (Hypertext Transfer Protocol - Secure)

d) LoRaWAN (Long Range Wide Area Network)

- The AWS IoT Core message broker supports devices and clients that use MQTT and MQTT over WSS protocols to publish and subscribe to messages. It also supports devices and clients that use the HTTPS protocol to publish messages.
- AWS IoT Core for LoRaWAN helps you connect and manage wireless LoRaWAN devices. AWS IoT Core for LoRaWAN replaces the need for you to develop and operate a LoRaWAN Network Server (LNS).

7.5 : Review of Various IoT Application Domains including Agriculture

Q.9 Discuss various IoT applications in the agriculture domain.

☞ [SPPU : June-22, End Sem, Marks 6]

Ans. : Smart Irrigation :

- In our country, agriculture is major source of food production to the growing demand of human population. In agriculture, irrigation is an essential process that influences crop production.
- Generally farmers visit their agriculture fields periodically to check soil moisture level and based on requirement water is pumped by motors to irrigate respective fields.
- The smart irrigation system was developed to optimize water use for agricultural crops. The system has a distributed wireless network of soil-moisture and temperature sensors placed in the root zone of the plants.
- Wireless Transmitter Unit (WTU) is comprised of a soil moisture sensor, a temperature sensor, a microcontroller, a RF transceiver and power source. Several WTUs can be incorporated in field to form a distributed network of sensors.
- Input to the micro controller is the reading of the moisture sensor and depending upon the threshold value a high or a low.

- If the soil moisture value is below the threshold or the temperature exceeds the threshold value, then the motor is turned on till the levels of moisture and temperature are optimized. Otherwise the motor is off. The sensor values and motor status is displayed on an Android App.

Green House Control :

- In modern greenhouses, several measurement points are required to trace down the local climate parameters in different parts of the big greenhouse to make the greenhouse automation system work properly.
- The most important factors for the quality and productivity of plant growth are temperature, humidity, light and the level of the carbon dioxide.
- Continuous monitoring of these environmental variables gives information to the grower to better understand, how each factor affects growth and how to manage maximal crop productiveness.
- Wireless Sensor Network (WSN) can form a useful part of the automation system architecture in modern greenhouses.
- Wireless communication can be used to collect the measurements and to communicate between the centralized control and the actuators located to the different parts of the greenhouse.
- Fig. Q.9.1 shows greenhouse with sensor.

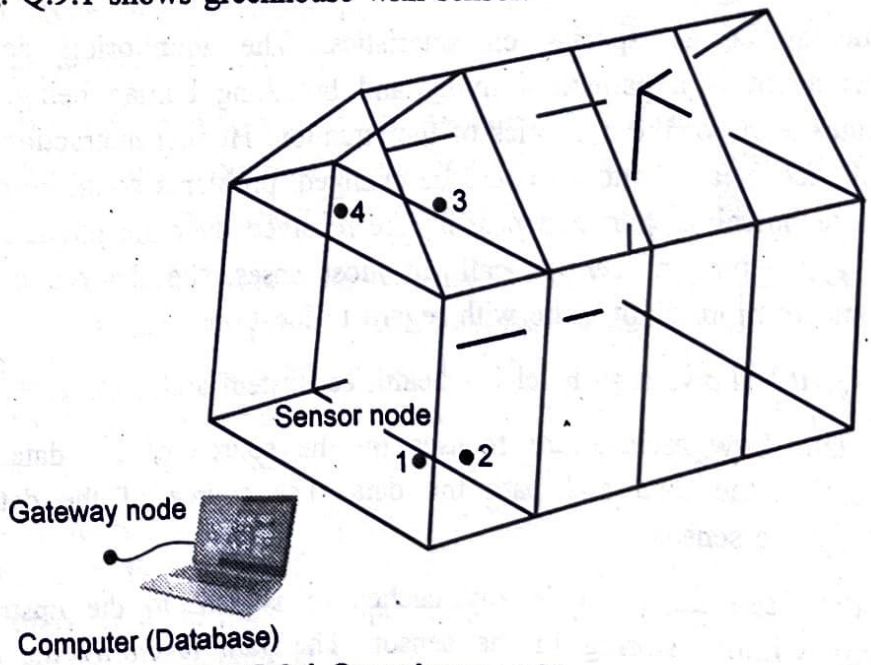

Fig. Q.9.1 Greenhouse with sensor

- Basic factors affecting plant growth are sunlight, water content in soil, temperature, CO_2 concentration etc. These physical factors are hard to control manually inside a greenhouse and there is a need for automated design arises.
- Data collected from various sensor is stored on the centralized server and this server process the data.

7.6 : Healthcare

Q.10 What is the E-healthcare system ? How IoT is important in E-health monitoring application ?

☞ **[SPPU : June-22, End Sem, Marks 6]**

Ans. : • The World Health Organization (WHO) defines E - health as : E - health is the transfer of health resources and health care by electronic means. It encompasses three main areas : The delivery of health information, for health professionals and health consumers, through the internet and telecommunications.

- E - health provides a new method for using health resources - such as information, money, and medicines and in time should help to improve efficient use of these resources.
- E - health brings special characteristics. The monitoring device's environment is a patient; a living and breathing human being. This changes some of the dynamics of the situation. Human interaction with the device means batteries could be changed, problems could be called in to technical support and possibly be resolved over the phone rather than some type of service call. In most cases, the devices on the patient are mobile not static with regard to location.
- Fig. Q.10.1 shows high level E - health ecosystem architecture.
- The data flow architecture focuses on the source of the data, the destination the data and path the data. The source of the data is typically the sensor.
- The data can be either locally cached or is sent to the upstream systems without storing in the sensor. The path taken by the data

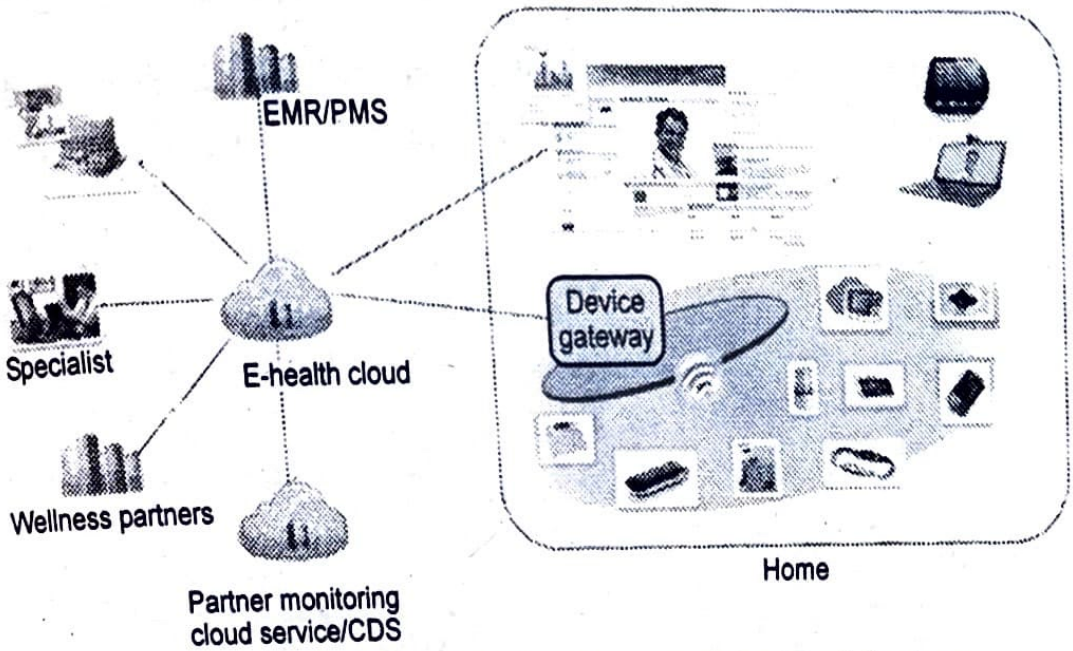

Fig. Q.10.1 High level E - health ecosystem architecture

includes a gateway, which can also cache some of the data and do distributed processing.

- Intermediate hubs can also store and process the data to filter out or make certain decisions. A distributed rules engine is used to make distributed decisions at the closest point of care. This enables data traffic to be filtered and processed efficiently without having every data being processed by the cloud service.
- The development of wireless networks has led to the emergency of a new type of E - healthcare system, providing expert-based medical treatment remotely on time.
- With the E - healthcare system, wearable sensors and portable wireless devices can automatically monitor individual's health status and forward them to the hospitals, doctors and related people.
- The system offers great conveniences to both patients and health care providers. For the patients, the foremost advantage is to reduce the waiting time of diagnosis and medical treatment, since they can deliver the emergent accident information to their doctors even if they are far away from the hospital or they don't notice their health condition.
- In addition, E - health system causes little interruption to patient's daily activities. For the health care providers, after receiving the abnormal signals from the patients, appropriate treatment can be made, which saves medical resources.

- Furthermore, without direct contact with medical facilities, medical personnel or other patients, the patients are unlikely to be infected with other diseases.

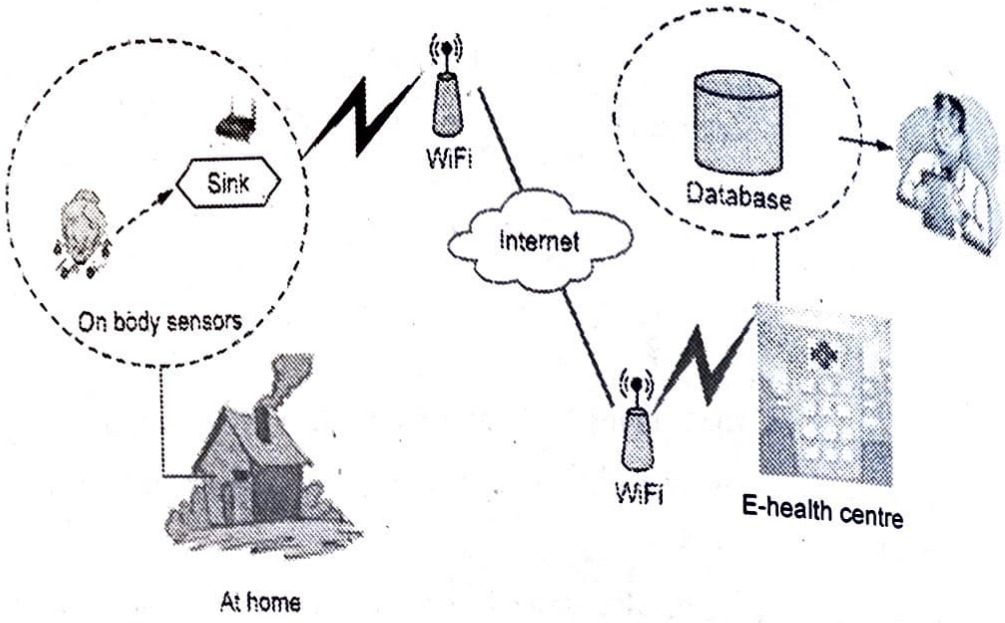

Fig. Q.10.2

- However, to ensure the security and privacy of patient's medical records encounters a lot of challenges :
  1. How to achieve the confidentiality and integrity of patient's information,
  2. The security of wireless body area network,
  3. The privacy and unlink ability of patient's health status,
  4. The undeniability and unlinkability of doctor's treatment,
  5. The location privacy of patients, the fine - grained access control of patient's medical record, the mutual authentication between patients and hospitals, etc.
- It would be useful to create an up-to-date bibliography on secure E - healthcare systems.

7.7 : Manufacturing

Q.11 Discuss various IoT applications in automotive applications.

☞ **[SPPU : June-22, End Sem, Marks 5]**

Ans. : • Today, users of IoT devices can evaluate engine performance, control air temperature and measure physical health indicators with only a few clicks.

- Conventional perceptions of the automotive industry are radically changing with IoT development. Predictive maintenance, Wi-Fi capabilities powered by 3G/4G/5G functionality, Car2Car connectivity and advanced fleet management are only a few examples of how IoT-based solutions are shaping the new automotive age.
- The automobile industry is one of the fastest-growing markets for IoT-based solutions. The number of installed connectivity units in vehicles is likely to increase by 67 % between 2018 and 2020.
- Predictive maintenance technology is based on the use of IoT connectivity tools that collect data on the performance of different parts, transfer that data to the cloud in real time and evaluate the risks of potential malfunction of a car's hardware or software. After information is processed, a driver is notified and advised of any necessary service or repair to avoid potential incidents.
- Fig. Q.11.1 shows battery working.

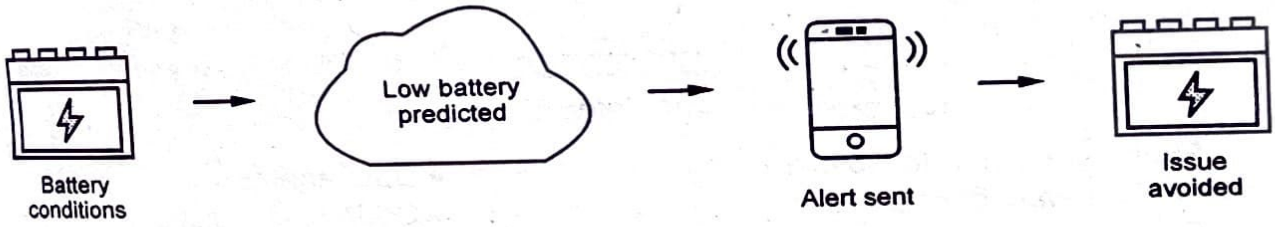

Fig. Q.11.1 Battery working

- Predictive maintenance can facilitate vehicle use by both private owners and dealerships with large fleets of vehicles. It enables end-users to get the right information in advance. With IoT connectivity tools, you can forget about unplanned stops or breakdowns during the ride.

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. Q.11.2 shows remote vehicle diagnostics.

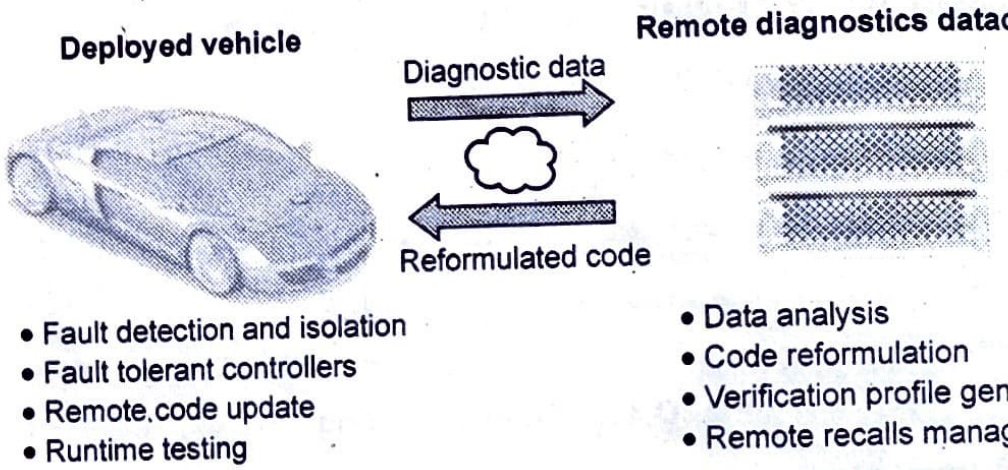

Fig. Q.11.2 : Remote vehicle diagnostics solution

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

7.8 : Wearable Computing Devices

Q.12 Write short note on wearable electronic.

Ans. : • Wearable electronic devices are small devices worn on the head, neck, arms, torso, and feet.

- Current smart wearable devices include :
  1. Head - Helmets, glasses
  2. Neck - Jewelry, collars
  3. Arm - Watches, wristbands, rings
  4. Torso - Clothing, backpacks
  5. Feet - Socks, shoes.
- Smart glasses help us enjoy more of the media and services we value and when part of an IoT system, they allow a new approach to productivity.
- Smart watches not only help us stay connected, but as a part of an IoT system, they allow access needed for improved productivity.

Q.13 What are challenges in the healthcare system ?

Ans. : Some challenges in the healthcare system are as follows :

1. **Smarter hospital :** Smarter hospital is an important improvement of smart healthcare system. A natural problem is how to build a smarter hospital for greatly improving medical services and patient experience.
2. **Data integration / realtimeness :** How to combine heterogenous health data sources in a unified and meaningful way enables the discovery and monitoring of health data from different sources. It is also important for smart healthcare to ensure the data realtimeness.
3. **Medical resource shortness :** There are not enough medical resources for the population. For example, there are fewer doctors and high-level healthcare institutions but more patients.
4. **"Low" usage of community health service centers :** In contrast with community health service centers, people prefer the high-level healthcare institutions. This results in the low usage of community service centers.

5. **Bad health habits :** The citizens have some bad health habits that contribute to poor health, for instance, smoking and no sport.
6. **Lack of information sharing :** hospitals are not sharing enough information. This leads to the following two problems at least. First, the health information records of patients cannot be queried. Second, there is lack of medical cooperation between hospitals.

7.9 : Vehicle to Vehicle Communication

Q.14 Explain vehicle to vehicle communication.

[SPPU : June-22, End Sem, Marks 5]

Ans. : • Vehicle-to-vehicle communication is the wireless transmission of data between motor vehicles.

- The technology behind V2V communication allows vehicles to broadcast and receive omni-directional messages, creating a 360-degree "awareness" of other vehicles in proximity. Vehicles equipped with appropriate software can use the messages from surrounding vehicles to determine potential crash threats as they develop.
- Fig. Q.14.1 shows V2V communication.

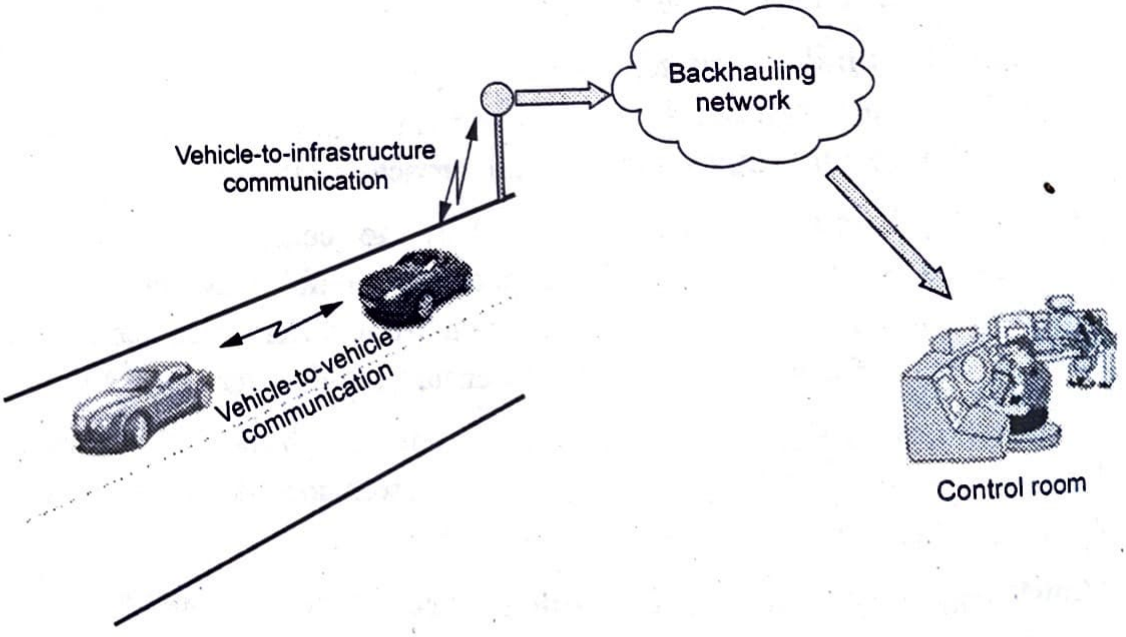

Fig. Q.14.1 V2V communication

- The technology can then employ visual, tactile and audible alerts or, a combination of these alerts to warn drivers. These alerts allow drivers the ability to take action to avoid crashes.
- The implementation of V2V communication and an intelligent transport system currently has three major roadblocks : The need for automotive manufacturers to agree upon standards, data privacy concerns and funding.
- It is unclear whether creation and maintenance of the supporting network would be publicly or privately funded. Automotive manufacturers working on ITS and V2V include GM, BMW, Audi, Daimler and Volvo.

END...

JUNE - 2022 [END SEM][5869]-369 | Solved Paper

Course 2019

Time : $2\frac{1}{2}$ Hours] **[Maximum Marks : 70**

Instructions to the candidates :

1) ***Attempt Questions Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q7 or Q.8.***
2) ***Draw neat and Clean Diagram.***
3) ***Assume suitable data, if necessary.***

Q.1 a) *Illustrate the various IoT communication APIs ?* **(Refer Q.9 of Chaper - 4)** **[8]**

b) *With the help of following sectors explain how IoT technology is impacting on the end-to-end value chain in the logistics sector :*

i) Route generation and scheduling

ii) Fleet tracking

iii) Shipment monitoring

iv) Remote vehicle diagnostics **(Refer Q.23 of Chaper - 4)** **[10]**

OR

Q.2 a) *Demonstrate the IoT component with a neat diagram.* **(Refer Q.2 of Chaper - 4)** **[9]**

b) *What is piggybacking ? What is the necessity of security and privacy of IoT ?* **(Refer Q.29 of Chaper - 4)** **[9]**

Q.3 a) *Draw and explain WSN architecture.* **(Refer Q.4 of Chaper - 5)** **[9]**

b) *Explain any four IoT network protocols.* **(Refer Q.21 of Chaper - 5)** **[8]**

OR

Q.4 a) *Explain machine to machine architecture.* **(Refer Q.8 of Chaper - 5)** **[9]**

b) *Explain any four applications of RFID.*
(Refer Q.5 of Chaper - 5) **[8]**

Q.5 a) *Explain IoT information model specification.*
(Refer Q.18 and Q.20 of Chaper - 6) **[9]**

b) *Explain various IoT sim card technologies.*
(Refer Q.22 of Chaper - 6) **[9]**

OR

Q.6 a) *What are the criterias for selection of controllers in embedded products ?* **(Refer Q.11 of Chaper - 6)** **[9]**

b) *What are different security parameters considered while designing any IoT system ?* **(Refer Q.24 of Chaper - 6)** **[9]**

Q.7 a) *Discuss various IoT applications in the agriculture domain.*
(Refer Q.9 of Chaper - 7) **[6]**

b) *What is the E-healthcare system? How IoT is important in E-health monitoring application.*
(Refer Q.10 of Chaper - 7) **[6]**

c) *Discuss various IoT applications in automotive applications.*
(Refer Q.11 of Chaper - 7) **[5]**

OR

Q.8 a) *Write a short note on IoT vertical Applications.*
(Refer Q.1 of Chaper - 7) **[6]**

b) *Explain voice application for IoT device.*
(Refer Q.3 of Chaper - 7) **[6]**

c) *Explain vehicle to vehicle communication.*
(Refer Q.14 of Chaper - 7) **[5]**

END...