Internet of Things Question Bank Aswers
Q1-21 and 23 (mid term)

Q.1 What is internet of things (IOT). What are components required to design IOT device and which device we called Iot device explain with example

→ (1) The internet of things is a collection of diverse technologies that interact with the physical world.

(2) internet of things refers to the network of physical devices, vehicles, home appliances and other items embedded with sensors and actuators, softwares and connectivity.

(3) This allows them to connect and exchange data with each other and with other system over the internet

(4) components required to design Iot devices:

(a) Sensors and actuators:

(1) sensor is a device that detects events or changes in the environment and sends that information to other electronic devices

(2) An actuator is a component of machine that is responsible for moving and controlling mechanism.

(3) sensors are connected to the input ports of the system while actuators are connected to the output ports

eg. temperature sensors, image sensors, electric motor, stepper motor.

(b) Micro-controller and Micro-processor: This is the brain of the device, which process the data collected by the sensors and sends commands to the actuators.

(c) connectivity module: This allows the device to connect to the internet or other devices. Example include wifi, bluetooth and cellular modules.

(d) Power supply: The device needs a power source to connect, operate which could be a battery, solar pannel, or other power source.

(e) Software: This includes the firmware that runs on the micro-controller as well as any cloud-based applications or services that the device interacts with.

(f) User interface: This component allow users to interact with the device, which can be through mobile app a web interface such as a button or a screen.

(g) Data storage: The iot device may need to store the data locally before sending it to the cloud or other devices. This can be acheived through flash memory or an SD card.

(h) Example of IOT Device:

- smart thermostat
  - used to control temperature at home or office
  - includes temperature sensor, micro controller, wifi module, software to control thermostat and interact with mobile app or web interface.
  - can be programmed to adjust the temperature based on various factors, such as the time of day. or occupancy of room.
  - can be controlled remotely through App.

Q.2 Explain ... (IOT) with example.
- same answer Q:1

Q.3 Give brief overview of IOT.
- same answer as Q:1

Q.4 What is the vision of iot?
→ (1) The vision of the Iot is to create a world in which physical objects, devices and machines are connected to the internet enabling them to collect and exchange data with each other and with humans.

(2) The vision is based on the idea that by enabling devices to communicate and collaborate with each other, we can create a smarter and more efficient world, with improved processes, better decision-making and enhanced life-style.

(3) The vision of iot includes several key elements including :

(a) connected devices: The proliferation of smart devices, sensors, and other connected objects that can communicate with each other and with humans.

(b) Data-driven decision making: The use of data analytics and machine learning algorithms to analyze the vast amounts of data generated by IOT devices and make more informed decisions.

(c) improved efficiency and productivity: The ability of IOT to automate process and reduce ineffeciencies leading to improved productivity, reduced costs and enhanced competitiveness

(d) Enhanced safety and security: The use of iot devices to monitor and manage safety and security risks such as in the areas of public safety, transportation and critical infrastructure.

(e) personalized Experiences: The ability of IoT deliver personalized experiences based on individual preferences and needs, such as in the areas of health care, retail and entertainment.

Q.5 Explain the 4 pillar of iot and how are they inter-connected to each other.

→ (1) The four pillar of iot refer to the fundamental component that form the basis of the IOT systems.

(2) Pillars are as below:

(a) Device:

- An device is a form of hardware that is capable of transmitting data from one location to another through the internet.
- This data is ususaly recorded by sensor located within the device
- These devices can range from sensors and actuators to everyday objects such as appliances, wearables industrial equipment and vehicles.

(b) Data:

- Data is at the core of iot systems. Iot generates a massive volume of data through sensors, devices and systems.
- This data includes real time measurements, environmental information, use behaviour, and mor

(3) Analytics:

- This pillar is what makes iot applications so powerful and useful in the everyday life of individuals in organizations.
- The data collected is processed, analyzed, and interpreted using various techniques, including machine learning and artificial intelligence to exact valuable insights and support decision making process.

(d) connectivity:
- connectivity enables the three previously mentioned pillars to work in conjunction with each other.
- it is essential that connection is maintained so that the data can be transferred and analyzed correctly.
- connectivity is the fondation of iot enabling devices to communicate and share the data with each other and with the cloud or other networks.
- it involves various communication technologies such as wifi, bluetooth, cellular networks, zigbee etc.

Q.6) Explain different challenges of iot? (S.P.I.S.P.C.D)

→ (1) The iot brings a wide range of benefits, but it also presents several challenges that must be addressed to ensure its successful adoption.
challenges includes

(2) (a) security: iot devices are vulnerable to cyber attacks and breaches, which can result in sensitive data bing stolen or devices being hijacked or used in malicious activities.

(b) privacy: IoT devices are often developed collects large amount of personal data, rising concerns about how this data is used, stored, and protected.

(c) Interpolability: IoT devices are often developed by different manufactures using different standards and protocols, making it difficult for devices to communicate and work together seamlessly.

(d) scalability: As the number of iot devices grows, managing and maintaining them becomes increasingly complex, requiring significant resources and intrastructure.

(e) power consumption: iot devices typically rely on battery power, which can limit their functionality and require frequent replacement or recharging

(f) complexity: iot systems can be complex and difficult to understand, requiring specialized knowledge and experience to design, deploy and manage.

(g) Data management: Iot devices generate massive amounts of data, which can be difficult to store, process and analyze effectively

(2) Addressing this challenges requires holistic approach that involves collaboration between industry, government and academia to develop common standards, best practices and regulations.

Q(7) What are the different components required for Iot device?

→ same as Q:1

Q.8) What is Machine to machine (M2M)?

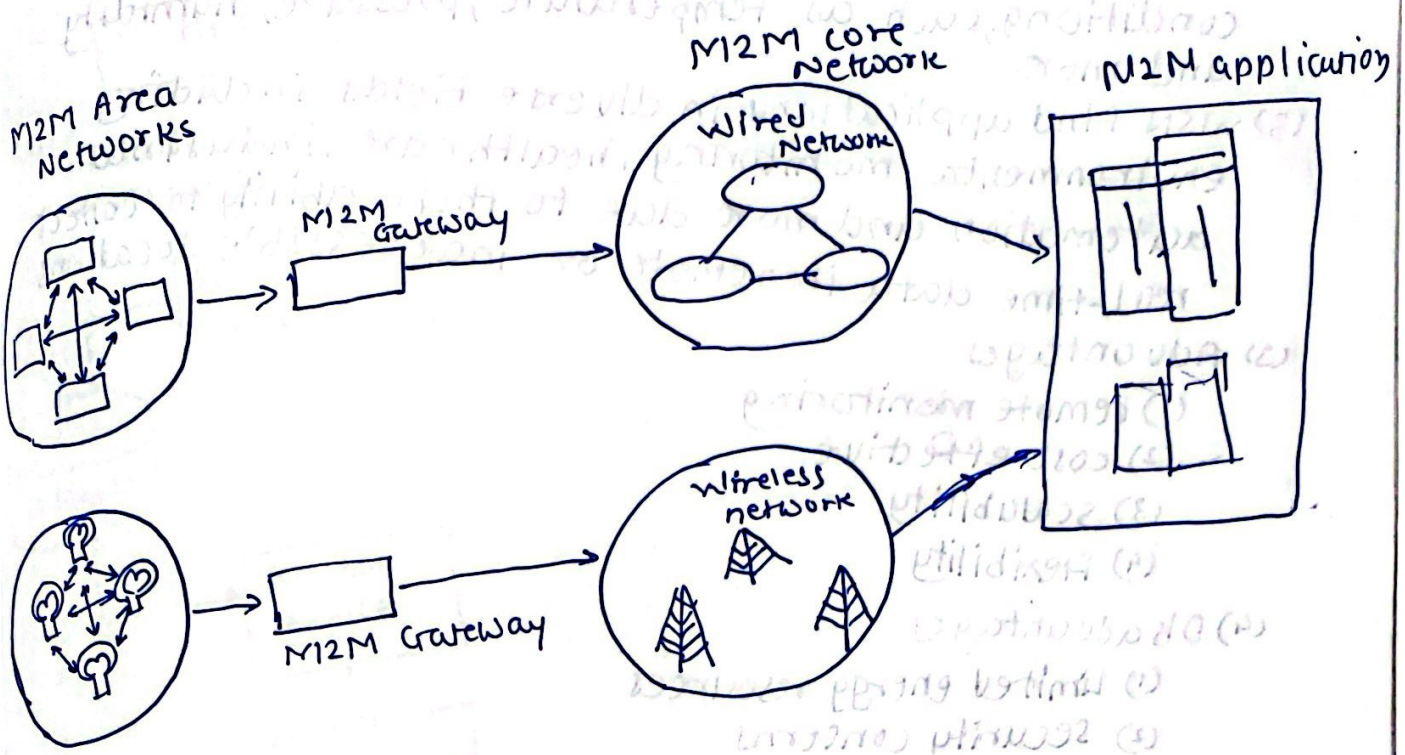
(1) Machine to machine (M2M) communication refers to technologies, standards and protocols that enables the machines to communicate with each other and carry out useful tasks without human intervention

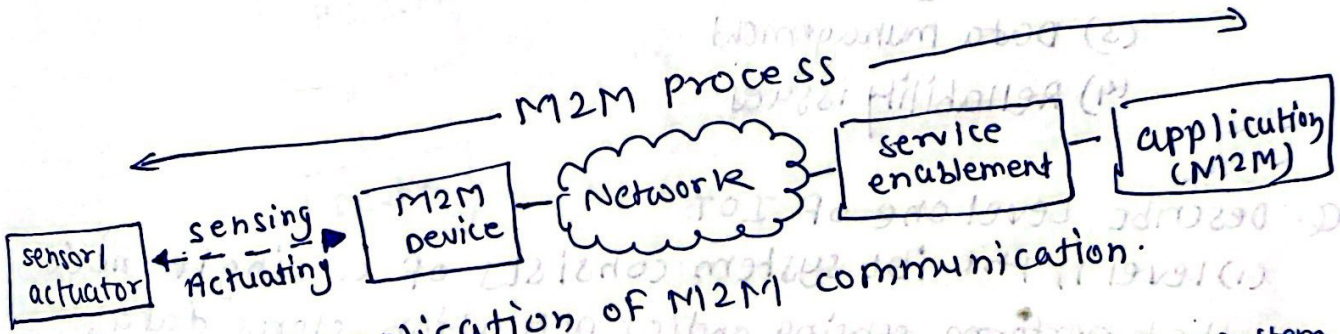
(2) In M2M communication devices are equipped with sensors, actuators, and communication modules that enable them to collect and transmit data to other devices or central system.

(3) This data exchange can occur over various communication channels such as wired connections (ethernet) or wireless networks (cellular, wifi)

(4) The device involved in M2M communication can be anything from simple sensors and actuators to complex machines or systems

(5) M2M (machine to machine) Architecture
(1) M2M Device Domain
(2) M2M Network Domain
(3) M2M application Domain





(6) examples and application of M2M communication:
(1) Fleet Management
- communication between vehicals, GPS, tracking system, and central management systems.
(2) Healthcare
- communication between healthcare devices, wearable sensors, healthcare systems
(3) Industrial Automation:
- communication between machines and systems in factory.

Q. Write a note on wireless sensor network.

→ (1) Wireless sensor network (WSNs) are networks comprised of numerous spatially distributed autonomous sensor nodes that monitor physical or environmental conditions, such as temperature, pressure, humidity and more.

(2) WSN find applications in diverse fields including environmental monitoring, healthcare, industrial automation and more due to their ability to collect real-time data in remote or inaccessible locations.

(3) Advantages
- (1) remote monitoring
- (2) cost-effective
- (3) scalability
- (4) flexibility

(4) Disadvantages
- (1) Limited energy resources
- (2) security concerns
- (3) Data management
- (4) Reliability issues

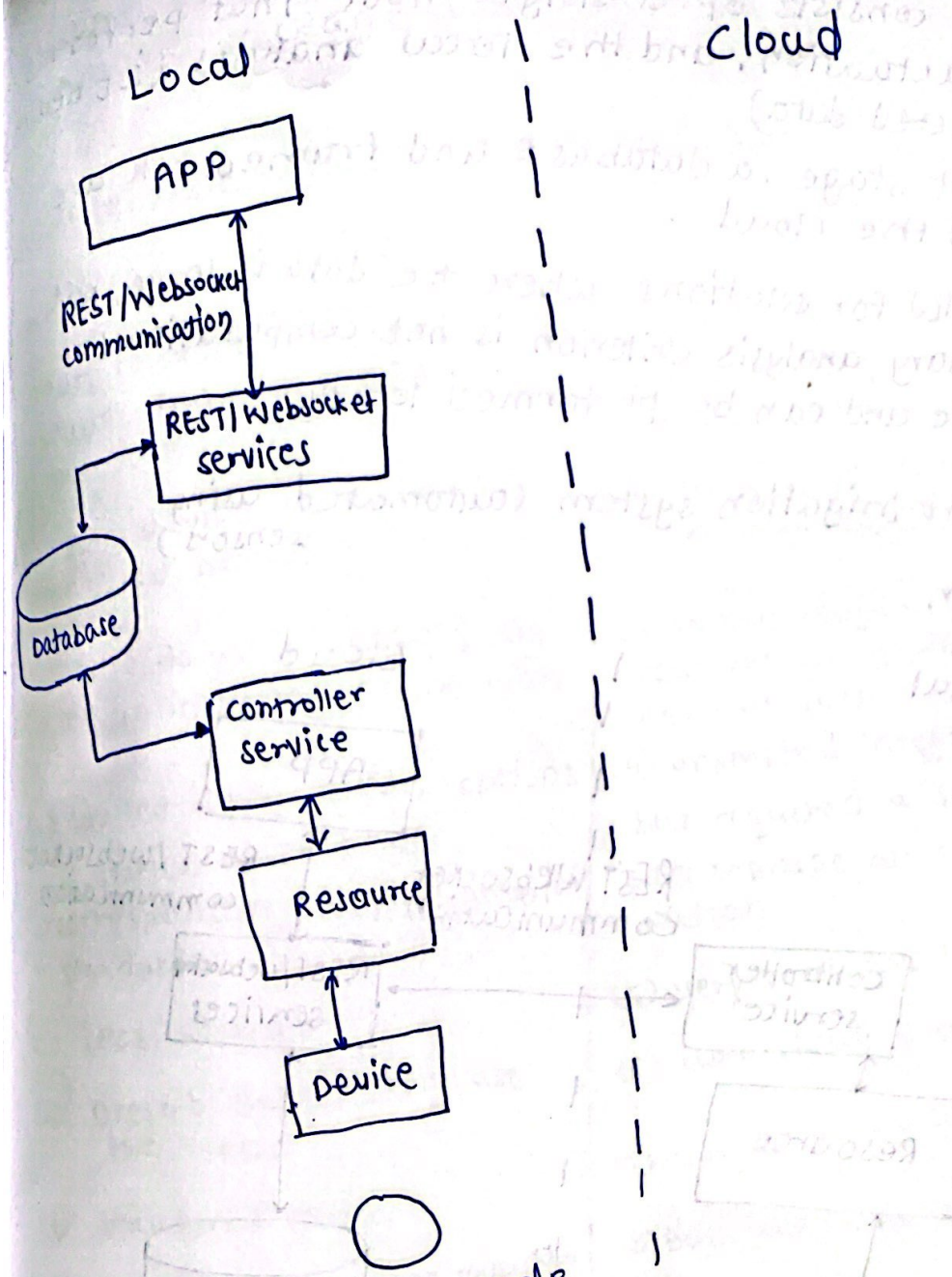
Q. Describe Level one of IOT

(1) level 1, the iot system consists of a single node that perform sensing and/or actuation, stores data, performs analysis and hosts the applications

(2) This level is suitable for the low cost and low-complexity solutions where the data involved is not extensive, and the analysis requirements are not computationally intensive.

(3) Home automation is an example of a level 1 iot system, where a single smart home device controls various appliances and collects data for simple analysis

IOT Level-1



example: smart home APP
(explain in detail if question is of 5-10 marks)

Q. Explain IOT level 2

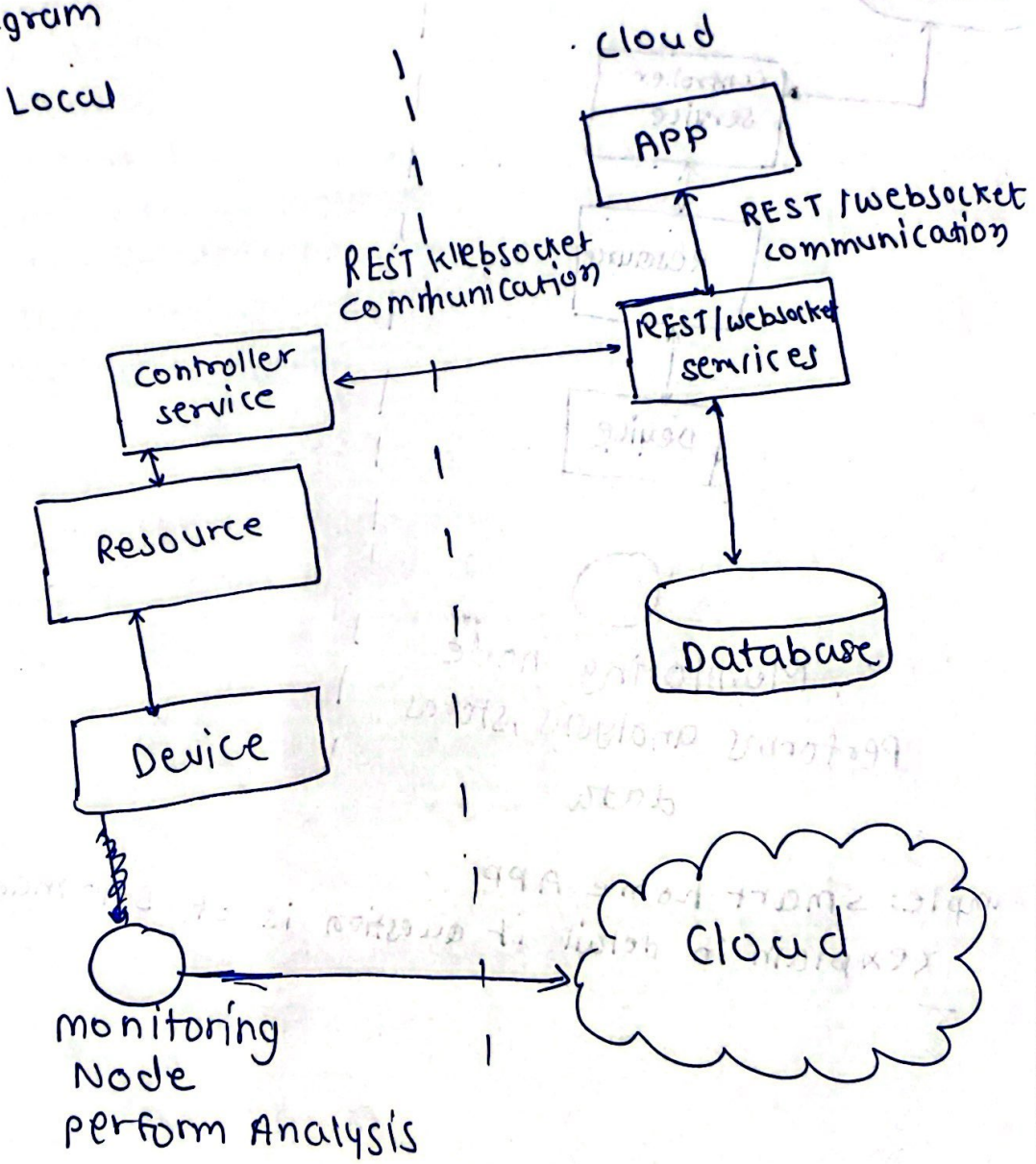
(1) IoT level 2 consists of a single node that performs sensing, actuation, and the local analysis (iot device and collected data)

(2) in this iot stage, a database and framework are setup in the cloud.

(3) it is useful for solutions where the data is large, but the primary analysis criterion is not computationally intensive and can be performed locally

(4) eg. smart irrigation system (automated using sensors)

(5) Diagram



* Explain IoT level 5:
→ same as Level 2
→ example package monitoring system

* Differentiate between M2M AND IOT

→ Machine to Machine	Internet of Things
(1) Point to point communication usually embedded with network	(1) Device communicate using network incorporating with varying protocols.
(2) Many device uses cellular or wired network	(2) Data delivery is relayed through a middle layer hosted in the cloud.
(3) Device do not necessary rely on an internet connection	(3) in the majority cases devices requires an active internet connection
(4) Limited integration options as device must have corresponding communication standards	(4) unlimited integration options but required a solution that can manage all of the communication.
(5) Less scalable	(5) very scalable
(6) Doesn't necessarily use the cloud	(6) uses cloud platforms
(7) Structured data	(7) unstructured data.
(8) often one-way communication	(9) Back and forth communication

Q. What is iot analytics (2 marks)

→ (1) iot analytics refers to the process of collecting, processing, and analyzing data generated by internet of things devices.

(2) Iot devices are embedded with sensors and connectivity capabilities, allowing them to gather data from the surrounding environment and transmit it over the internet.

(3) Iot analytics involves various techniques such as data aggregation, real time processing, and predictive analytics to derive actionable insights from the vast amounts of data generated by Iot devices.

(4) These insights can help businesses and organizations make informed decisions, optimize processes, improve efficiency, enhance customer experience and even develop new products and services

(5) In conclusion, iot analytics enables organizations to harness the power of Iot data to gain valuable insights drive innovation, and create new opportunities for growth and optimization in diverse industries.

Q. What is Zigbee?

(1) Zigbee is wireless communication standard tailored for low power Iot devices, operating in the 2.4 GHz band, (M2M) and iot networks

(2) Zigbee is for low-data rate, low-power applications and is an open standard.

(3) Zigbee is based on the Institute of Electrical and Electronics Engineers (IEEE) standards Association's 802.15 specification.

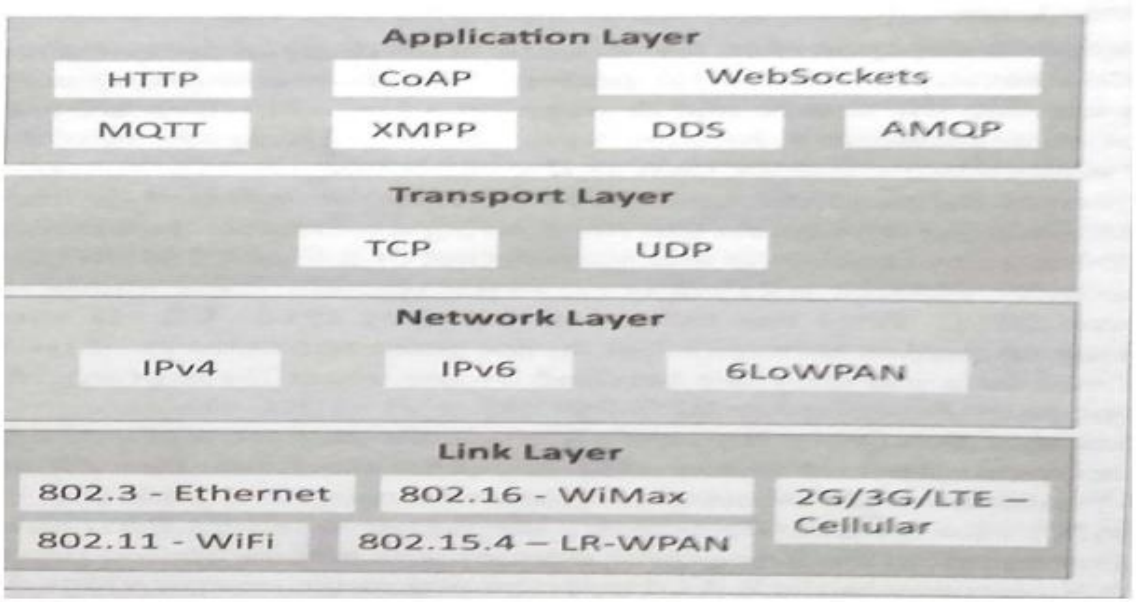
(4) its mesh networking capability enables devices to communicate with each other, extending coverage and reliability.

(5) Zigbee ensure interpperability among devices, offers energy-efficient operation for prolonged battery life and incorporate robust security measures

(6) Applications: (1) smart homes
(2) industrial automation
(3) health care
(4) Automated systems etc

2) IoT Protocols:

a) Link Layer : Protocols determine how data is physically sent over the network_s physical layer or medium. Local network connect to which host is attached. Hosts on the same link exchange data packets over the link layer using link layer protocols. Link layer determines how packets are coded and signaled by the h/w device over the medium to which the host is attached.



Protocols:

- 802.3-Ethernet: IEEE802.3 is collection of wired Ethernet standards for the link layer. Eg: 802.3 uses co-axial cable; 802.3i uses copper twisted pair connection; 802.3j uses fiber optic connection; 802.3ae uses Ethernet over fiber.
- 802.11-WiFi: IEEE802.11 is a collection of wireless LAN(WLAN) communication standards including extensive description of link layer. Eg: 802.11a operates in 5GHz band, 802.11b and 802.11g operates in 2.4GHz band, 802.11n operates in 2.4/5GHz band, 802.11ac operates in 5GHz band, 802.11ad operates in 60Ghzband.
- 802.16 - WiMax: IEEE802.16 is a collection of wireless broadband standards including exclusive description of link layer. WiMax provide data rates from 1.5 Mb/s to 1Gb/s.
- 802.15.4-LR-WPAN: IEEE802.15.4 is a collection of standards for low rate wireless personal area network(LR-WPAN). Basis for high level communication protocols such as ZigBee. Provides data rate from 40kb/s to250kb/s.
- 2G/3G/4G-Mobile Communication: Data rates from 9.6kb/s(2G) to up to100Mb/s(4G).

B) **Network/Internet Layer:** Responsible for sending IP datagrams from source n/w to destination n/w. Performs the host addressing and packet routing. Datagrams contains source and destination address.

Protocols:

- **IPv4:** Internet Protocol version4 is used to identify the devices on a n/w using a hierarchical addressing scheme. 32 bit address. Allows total of 2**32addresses.
- **IPv6:** Internet Protocol version6 uses 128 bit address scheme and allows 2**128 addresses.
- **6LOWPAN:**(IPv6overLowpowerWirelessPersonalAreaNetwork)operates in 2.4 GHz frequency range and data transfer 250 kb/s.

C) **Transport Layer:** Provides end-to-end message transfer capability independent of the underlying n/w. Set up on connection with ACK as in TCP and without ACK as in UDP. Provides functions such as error control, segmentation, flow control and congestion control.

Protocols:

- **TCP:** Transmission Control Protocol used by web browsers(along with HTTP and HTTPS), email(along with SMTP, FTP). Connection oriented and stateless protocol. IP Protocol deals with sending packets, TCP ensures reliable transmission of protocols in order. Avoids n/w congestion and congestion collapse.
- **UDP:** User Datagram Protocol is connectionless protocol. Useful in time sensitive applications, very small data units to exchange. Transaction oriented and stateless protocol. Does not provide guaranteed delivery.
-

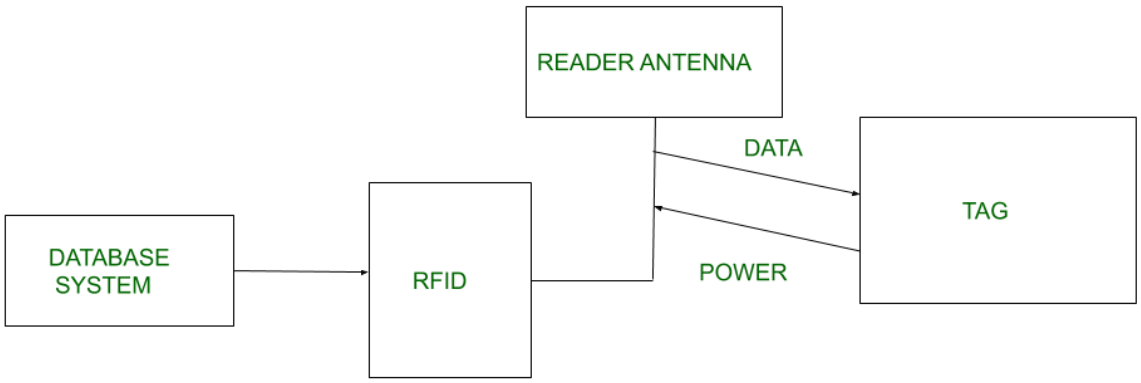
D) **Application Layer:** Defines how the applications interface with lower layer protocols to send data over the n/w. Enables process-to-process communication using ports.

Protocols:

- **HTTP:** Hyper Text Transfer Protocol that forms foundation of WWW. Follow request-response model Stateless protocol.
- **CoAP:** Constrained Application Protocol for machine-to-machine (M2M) applications with constrained devices, constrained environment and constrained n/w. Uses client- server architecture.
- **WebSocket:** allows full duplex communication over a single socket connection.
- **MQTT:** Message Queue Telemetry Transport is light weight messaging protocol based on publish-subscribe model. Uses client server architecture. Well suited for constrained environment.
- **XMPP:** Extensible Message and Presence Protocol for real time communication and streaming XML data between network entities. Support client-server and server-server communication.
- **DDS:** Data Distribution Service is data centric middleware standards for device-to-device or machine-to-machine communication. Uses publish-subscribe model.
- **AMQP:** Advanced Message Queuing Protocol is open application layer protocol for business messaging. Supports both point-to-point and publish-subscribe model.

Q. What is RFID? **5 marks**

Radio Frequency Identification (RFID) is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person. It uses radio frequency to search ,identify, track and communicate with items and people. it is a method that is used to track or identify an object by radio transmission uses over the web. Data digitally encoded in an RFID tag which might be read by the reader. This device work as a tag or label during which data read from tags that are stored in the database through the reader as compared to traditional barcodes and QR codes. It is often read outside the road of sight either passive or active RFID.



Kinds of RFID :
There are many kinds of RFID, each with different properties, but perhaps the most fascinating aspect of RFID technology is that most RFID tags have neither an electric plug nor a battery. Instead, all of the energy needed to operate them is supplied in the form of radio waves by RFID readers. This technology is called passive RFID to distinguish it from the (less common) active RFID in which there is a power source on the tag.

UHF RHID (Ultra-High Frequency RFID). It is used on shipping pallets and some driver's licenses. Readers send signals in the 902-928 MHz band. Tags communicate at distances of several meters by changing the way they reflect the reader signals; the reader is able to pick up these reflections. This way of operating is called backscatter.

HF RFID (High-Frequency RFID). It operates at 13.56 MHz and is likely to be in your passport, credit cards, books, and noncontact payment systems. HF RFID has a short-range, typically a meter or less because the physical mechanism is based on induction rather than backscatter.
There are also other forms of RFID using other frequencies, such as LF RFID(Low-Frequency RFID), which was developed before HF RFID and used for animal tracking

There are two types of RFID :

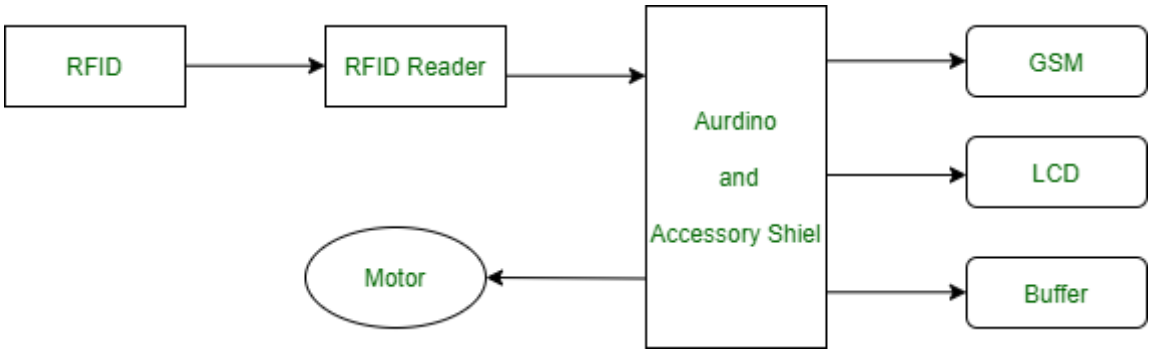
1. **Passive RFID –**
   Passive RFID tags does not have their own power source. It uses power from the reader. In this device, RF tags are not attached by a power supply and passive RF tag stored their power. When it is emitted from active antennas and the RF tag are used specific frequency like 125-134KHZ as low frequency, 13.56MHZ as a high frequency and 856MHZ to 960MHZ as ultra-high frequency.

2. **Active RFID –**
   In this device, RF tags are attached by a power supply that emits a signal and there is an antenna which receives the data. means, active tag uses a power source like battery. It has it's own power source, does not require power from source/reader.

Working Principle of RFID :

RFID, or Radio Frequency Identification, utilizes radio waves for Automatic Identification and Data Capture (AIDC). AIDC technology enables object identification and data collection.

An antenna converts power into radio waves for communication between the RFID reader and tag. The reader retrieves information from the tag, detecting it and reading or writing data. It typically includes a processor, storage, and transmitter/receiver unit.



Working of RFID System :

- RFID systems consist of three components: a scanning antenna, a transceiver, and a transponder.
- The scanning antenna and transceiver together form the RFID reader or interrogator.
- RFID readers come in two types: fixed (permanently attached) and mobile (portable).
- RFID readers use radio waves to transmit signals that activate the tag.
- Once activated, the tag sends a response wave back to the antenna, which translates it into data.
- The transponder, housed in the RFID tag, stores the information to be transmitted.
- Read range varies based on factors such as tag type, reader type, RFID frequency, and environmental interference.
- Tags with a stronger power source generally have a longer read range.

Features of RFID :

- An RFID tag consists of two-part which is an microcircuit and an antenna.
- This tag is covered by protective material which acts as a shield against the outer environment effect.
- This tag may active or passive in which we mainly and widely used passive RFID.

Application of RFID :

- It utilized in tracking shipping containers, trucks and railroad, cars.
- It uses in Asset tracking.
- It utilized in credit-card shaped for access application.
- It uses in Personnel tracking.
- Controlling access to restricted areas.
- It uses ID badging.
- Supply chain management.
- Counterfeit prevention (e.g., in the pharmaceutical industry).

Advantages of RFID :

- It provides data access and real-time information without taking to much time.
- RFID tags follow the instruction and store a large amount of information.
- The RFID system is non-line of sight nature of the technology.
- It improves the Efficiency, traceability of production.
- In RFID hundred of tags read in a short time.

Disadvantages of RFID :

- It takes longer to program RFID Devices.
- RFID intercepted easily even it is Encrypted.
- In an RFID system, there are two or three layers of ordinary household foil to dam the radio wave.
- There is privacy concern about RFID devices anybody can access information about anything.
- Active RFID can costlier due to battery.

Q. Explain the issues in IOT security?

Issues in IoT security arise due to the interconnected nature of IoT devices, their proliferation, and the diversity of their implementations. Here are some key issues:

1. **Lack of Standardization**: The absence of uniform security standards across IoT devices and platforms leads to inconsistencies in security measures, making it challenging to implement robust security protocols consistently.

2. **Vulnerabilities in Devices:** Many IoT devices have limited computational resources, making it difficult to implement strong security measures. As a result, they often contain vulnerabilities such as hardcoded passwords, unencrypted communication, and insecure firmware.

3. **Data Privacy Concerns**: IoT devices collect vast amounts of data, often including sensitive information about individuals and organizations. Inadequate data encryption, improper data handling practices, and data breaches can lead to privacy violations and identity theft.

4. **Network Security**: IoT devices communicate over networks, which introduces risks such as eavesdropping, man-in-the-middle attacks, and unauthorized access to network traffic. Insecure network configurations and weak authentication mechanisms exacerbate these risks.

5. **Botnets and DDoS Attacks:** Compromised IoT devices are susceptible to being recruited into botnets, which can launch Distributed Denial of Service (DDoS) attacks. These attacks can disrupt critical services and infrastructure, causing widespread damage and financial losses.

6. **Supply Chain Risks:** The complex supply chain involved in IoT device manufacturing increases the risk of malicious actors inserting backdoors, counterfeit components, or tampered firmware into devices, compromising their security from the outset.

7. **Lifecycle Management**: Managing the security of IoT devices throughout their lifecycle, including deployment, operation, maintenance, and decommissioning, poses challenges. Issues such as unpatched vulnerabilities, end-of-life devices, and insecure device disposal can create security gaps.

8. **Regulatory Compliance**: Compliance with regulations such as GDPR, CCPA, HIPAA, and industry-specific standards adds complexity to IoT security efforts. Failure to comply with these regulations can result in legal repercussions and financial penalties.

9. **User Awareness and Education**: Users may lack awareness of the security risks associated with IoT devices and may not take adequate measures to secure them. Education and awareness programs are essential to promote responsible IoT usage and security best practices.

10**. Resource Constraints**: IoT devices often have limited computational power, memory, and battery life, which constrains the implementation of robust security measures.

Balancing security requirements with resource constraints is a significant challenge in IoT security design.

Addressing these issues requires a holistic approach encompassing device hardening, secure communication protocols, network segmentation, encryption, access control, vulnerability management, security testing, and ongoing monitoring and compliance efforts. Collaboration among stakeholders, including device manufacturers, service providers, regulators, and end-users, is essential to mitigate IoT security risks effectively.

Q. Explain vulnerabilities in IOT. 5 marks

IoT vulnerabilities refer to weaknesses or flaws in IoT devices, networks, and ecosystems that can be exploited by malicious actors to compromise the confidentiality, integrity, or availability of data or systems. Here are some common IoT vulnerabilities:

1. **Weak Authentication and Authorization**: Many IoT devices use default or hardcoded credentials, making them vulnerable to brute-force attacks or unauthorized access. Weak or nonexistent authentication mechanisms allow attackers to gain unauthorized control over devices.

2**. Insecure Communication**: IoT devices often transmit data over unencrypted or insecure channels, exposing sensitive information to interception or manipulation. Lack of transport layer security (TLS) or improper implementation of encryption protocols leaves communication channels vulnerable to eavesdropping and data tampering.

3**. Unpatched Vulnerabilities**: Manufacturers may not release timely security patches or updates for IoT devices, leaving them vulnerable to known exploits. Device owners may also neglect to apply available patches, leaving devices exposed to known vulnerabilities.

4**. Lack of Secure Firmware Updates:** Insecure firmware update mechanisms can be exploited by attackers to deliver malicious firmware or compromise devices during the update process. Lack of cryptographic verification or integrity checks allows attackers to install unauthorized or tampered firmware.

5. Physical Security Weaknesses: Physical access to IoT devices can compromise their security. Devices located in unsecured environments or accessible to unauthorized individuals may be physically tampered with or stolen, allowing attackers to extract sensitive data or install malware.

6. **Insecure APIs and Interfaces:** APIs (Application Programming Interfaces) and web interfaces used for device management may lack proper authentication, input validation, or access control mechanisms, enabling attackers to exploit vulnerabilities such as SQL injection or command injection.

7**. Denial of Service (DoS) Attacks**: IoT devices may be susceptible to DoS attacks, where attackers overwhelm devices or networks with excessive traffic, causing disruption or rendering devices inaccessible. Inadequate resource management or insufficient network bandwidth exacerbates the impact of DoS attacks.

8. **Supply Chain Attacks:** Malicious actors may compromise IoT devices or components during the manufacturing, distribution, or supply chain process. Insertion of backdoors, counterfeit components, or malicious firmware poses significant security risks to end-users.

9. **Insufficient Physical Tamper Protection:** Lack of tamper-resistant hardware or protections against physical attacks allows attackers to manipulate or extract sensitive information from IoT devices by physically accessing them.

10**. Privacy Violations**: IoT devices may collect and transmit sensitive personal data without user consent or adequate privacy safeguards. Unauthorized access to personal information stored on devices or transmitted over networks can lead to privacy violations and identity theft.

Addressing IoT vulnerabilities requires a comprehensive approach involving secure design practices, robust authentication mechanisms, encryption of data in transit and at rest, timely patching and updates, secure firmware management, physical security measures, and ongoing monitoring and risk assessment. Collaboration among manufacturers, developers, regulators, and end-users is essential to mitigate IoT vulnerabilities effectively and ensure the security and privacy of IoT ecosystems.

Q. Explain SCADA.

SCADA stands for Supervisory Control and Data Acquisition. It's a system used for monitoring and controlling processes in industries such as energy, telecommunications, water and waste control, transportation, and manufacturing. SCADA systems gather real-time data from sensors and equipment located at remote sites and then transmit that data to a central location for monitoring and analysis.

The key components of a SCADA system include:

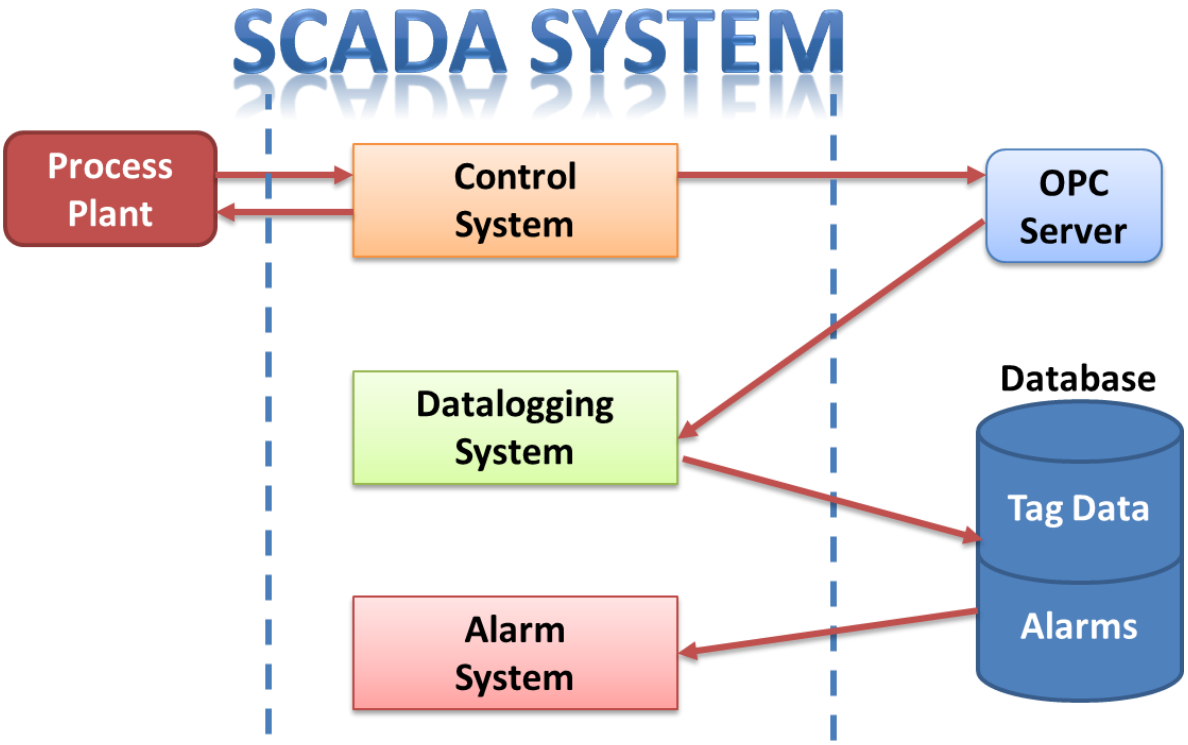
1. **Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs**): These are devices installed at remote sites to monitor and control equipment and processes. They collect data from sensors and can send control signals to actuators.

2. **Human Machine Interface (HMI):** This is the interface through which operators interact with the SCADA system. It typically includes graphical displays showing real-time data, alarms, and controls.

3. **Communication Infrastructure**: SCADA systems use various communication technologies such as radio, satellite, wired or wireless networks to transmit data between remote sites and the central control location.

4. **Supervisory System**: This is the central control system where data from remote sites is collected, analyzed, and presented to operators. It often includes software for data storage, trending, reporting, and alarm management.

SCADA systems are crucial for industries because they allow operators to monitor processes in real-time, identify issues, and take corrective actions promptly. They also enable remote control of equipment, reducing the need for on-site personnel and improving operational efficiency and safety.


SCADA SYSTEM
Process Plant
Control System
OPC Server
Datalogging System
Database
Tag Data
Alarms
Alarm System

2.8 M2M value chains

- M2M value chains are internal to one company and cover one solution.
- Reasons for using M2M vary from project to project and company to company.
- It can include things such as cost reductions through streamlined business processes,

product quality improvements, and increased health and safety protection for employees.

- Input and output of the value chains as follows:

1.Inputs: Inputs are the base raw ingredients that are turned into a product. Examples could be cocoa beans for the manufacture of chocolate or data from an M2M device that will be turned into a piece of information.

2.Production/Manufacture: Production/Manufacture refers to the process that the raw inputs are put through to become part of a value chain. For example, cocoa beans may be dried and separated before being transported to overseas markets. Data from an M2M solution, meanwhile, needs to be verified and tagged for provenance.

3.Processing: Processing refers to the process whereby a product is prepared for sale. For example, cocoa beans may now be made into cocoa powder, ready for use in chocolate bars. For an M2M solution, this refers to the aggregation of multiple data sources to create an information Component.

4.Packaging: Packaging refers to the process whereby a product can bebranded as would be recognizable to end-user consumers. For example, a chocolate bar would now be ready to eat and have a red wrapper with the words "KitKatt" on it. For M2M solutions, the data will have to be combined with other information from internal corporate databases.

5.Distribution/Marketing: This process refers to the channels to market for products. For example, a chocolate bar may be sold at a supermarket or even online. An M2M solution, however, will have produced an Information Product that can be used to create new knowledge within a corporate environment.