DEPARTMENT OF AI&DS

U20AI702 / INTERNET OF THINGS

PART A – QUESTION BANK

UNIT 1 -FUNDAMENTALS OF IOT

1)What is IoT (Internet of Things)?

Internet of Things (IoT) is a network of physical objects or people called "things" that are embedded with software, electronics, network, and sensors that allows these objects to collect and exchange data. The goal of IoT is to extend to internet connectivity from standard devices like computer, mobile, tablet to relatively dumb devices like a toaster.

2) List the Advantages & Disadvantages of IoT?

Advantages	Disadvantages
Minimizes the human work and effort	Increased privacy concerns
Saves time and effort	Increased unemployment rates
Good for personal safety and security	Highly dependent on the internet
Useful in traffic and other tracking or monitoring systems	Lack of mental and physical activity by humans leading to health issues.
Beneficial for the healthcare industry	Complex system for maintenance
Improved security in homes and offices	Lack of security
Reduced use of many electronic devices as one device does the job of a lot of other devices	Absence of international standards for better communication

3)Difference between Physical and Logical Design of IoT?

Physical Design	Logical Design
Physical design is highly detailed.	Logical design is a high-level design and doesn't provide any detail.
Physical design is more graphical than textual; however, it can comprise both.	Logical design can be textual, graphic, or both.
A physical design focuses on specific solutions explaining how they are assembled or configured.	A logical design focuses on satisfying the design factors, including risks, requirements, constraints, and assumptions.

4)IoT

Communication API?

In **IoT**, there are 2 communication APIs –

- **REST** — based Communication APIs
- **Web Socket** — based Communication APIs

5) DefineREST-Based Communication API?

REpresentational State Transfer (REST) is a set of architectural principles by which you can design web services and web APIs that focus on a system's resources and how resource states are addressed and transferred. REST APIs follow the request-response communication model. The REST architectural constraints apply to the components, connectors, and data elements, within a distributed hypermedia system.

6)Define Web Socket-Based Communication APIs?

Web Socket APIs allow bi-directional, full-duplex communication between clients and servers. It follows the exclusive pair communication model. This Communication API does not require a new connection to be set up for each message to be sent between clients and servers. Once the connection is set up the messages can be sent and received continuously without any interruption.

7)IoT(internet of things) enabling technologies are

1. Wireless Sensor Network
2. Cloud Computing
3. Big Data Analytics
4. Communications Protocols

5. Embedded System

8) Wireless Sensor Network(WSN)?

A **WSN** comprises distributed devices with sensors that are used to monitor environmental and physical conditions. A **wireless sensor network** consists of end nodes, routers, and coordinators. End nodes have several sensors attached to them and the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects WSNs to the internet.

9)Difference between Rest API and Web Socket API?

REST API	WEB SOCKET API
It is a Stateless protocol. It will not store the data.	It is Stateful protocol. It will store the data.
It is Uni-directional. Only either server or client will communicate.	It is Bi-directional. Messages can be received or sent by both server and client.
It is a Request-response model.	It is a Full duplex model.
HTTP request contains headers like head section, and title section.	It is suitable for real-time applications. It does not have any overhead.
A new TCP connection will be set up for each HTTP request.	Only Single TCP connection.
Both horizontal and vertical scaling (we can add many resources and a number of users both horizontally and vertically).	Only vertical scaling (we can add resources only vertically).
It depends upon the HTTP methods to retrieve the data	It depends upon the IP address and port number to retrieve the data
It is slower than the web socket regarding the transmission of messages.	web socket transmits messages very fast than REST API.
It does not need memory or buffers to store the data.	It requires memory and buffers to store the data.

10) Define Cloud Computing?

It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations. With Cloud computing, users can

access any resources from anywhere like databases, web servers, storage, any device, and any software over the internet.

11) Define IaaS ,SaaS and PaaS?

- **IaaS** (**Infrastructure as a service**) Infrastructure as a service provides online services such as physical machines, virtual machines, servers, networking, storage, and data center space on a pay-per-use basis. Major IaaS providers are Google Compute Engine, Amazon Web Services, and Microsoft Azure, etc. Ex: Web Hosting, Virtual Machine, etc.
- **PaaS** (**Platform as a service**) Provides a cloud-based environment with a very thing required to support the complete life cycle of building and delivering West web-based (cloud) applications — without the cost and complexity of buying and managing the underlying hardware, software provisioning, and hosting. Computing platforms such as hardware, operating systems, libraries, etc. Basically, it provides a platform to develop applications. Ex: App Cloud, Google app engine
- **SaaS (Software as a service):** it is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management. SaaS Applications are sometimes called web-based software on-demand software or hosted software. SaaS applications run on a SaaS provider's service and they manage security availability and performance. Ex: Google Docs, Gmail, office, etc.

12) Define Embedded Systems?

It is a combination of hardware and software used to perform special tasks. It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input-output units (display keyword, etc.), and storage devices (flash memory).It collects the data and sends it to the internet

13) List the Components of IOT?

An embedded system has three components. They are:

- Hardware
- Software

- Real Time Operating system (RTOS) that supervises the application software and provide mechanism to let the processor run a process as per schedule by following a plan to control the latencies.

UNIT II - ELEMENTS OF IOT

1) What is M2M?

M2M stands for Machine to Machine communication. 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. Various applications, such as defense, monitoring and tracking, production and facility management, are provided by M2M communications.

2) How M2M works?

The primary purpose of M2M technology is to tap into sensor data and transmit it over the network. M2M system often uses cellular or Ethernet and consists of three main components:

1. **Data endpoint (DEP)**: It is the system containing the data to be monitored or transmitted. Data endpoints are microcomputer systems- transmitters that are linked to a receiver. The network consists of many connected devices and data endpoints.
2. **Communication networks**: Cellular networks and wireless or wired internet connections are different types of communication networks transferring data from one machine to another.
3. **Data integration point (DIP)**: It is the machine that receives the information. There can be multiple data endpoints in a network but only one data integration point. The DIP can be a control center for meter readings, a server, or a web crawler.

3) Define Software- Networking (SDN)

Software- Networking (SDN) is a networking architecture that separates the control plane from the data plane and centralizes the network controller. Software-based SDN controllers maintain a united view of the network The underlying infrastructure in SDN uses simple packet forwarding hardware as opposed to specialized hardware in conventional networks

4) Difference between IoT and M2M?

Features	IoT	M2M
Abbreviation	IoT stands for the Internet of Things.	M2M stands for Machine-to-Machine communication.
Intelligence	Devices include objects that are responsible for decision-making processes.	In M2M, there is a limited amount of intelligence observed.
Communication Protocol Used	IoT has used internet protocols like FTP, Telnet, and HTTP.	Communication technology and Traditional protocols are uses in M2M technology.
Connection Type Used	The connection of IoT is through the network and using various types of communication.	M2M uses a point to point connection.
Scope	It has a wide range of devices, yet the scope is large.	It has a limited Scope for devices.
Business Type Used	It has Business to Consumer (B2C) and Business to Business (B2B).	It has Business to Business (B2B) communication.
Data Sharing	In IoT, data sharing depends on the Internet protocol network.	In M2M, devices may be connected through mobile or any other network.
Open API Support	IoT technology supports Open API integrations.	In M2M technology, there is no Open API support.
Example	Big Data, Cloud, Smart wearables, and many more.	Data and Information, sensors, and many more.

5) List the Key elements of SDN?

- **Centralized Network Controller** With decoupled control and data planes and centralized network controller, the network administrators can rapidly configure the network.
- **Programmable Open APIs** SDN architecture supports programmable open APIs for interface between the SDN application and control layers (Northbound interface).
- **Standard Communication Interface(OpenFlow)** SDN architecture uses a standard communication interface between the control and infrastructure layers (Southbound the Open Networking Foundation (ONF) is the broadly accepted SDN protocol for the Southbound interface.

6) Define Network Function Virtualization (NFV)

Network Function Virtualization (NFV) is a technology that leverages virtualization to consolidate the heterogeneous network devices onto industry standard high volume servers, switches and storage. NFV is complementary to SDN as NFV can provide the infrastructure on which SDN can run.

7) List the Key elements of NFV?

NFV Architecture Virtualized Network Function(VNF):

VNF is a software implementation of a network function which is capable of running over the NFV Infrastructure (NFVI).

NFV Infrastructure(NFVI):

NFVI includes compute, network and storage resources that are virtualized.

NFV Management and Orchestration:

NFV Management and Orchestration focuses on all virtualization-specific management tasks and covers the orchestration and life-cycle management of physical and/or software resources that support the infrastructure virtualization, and the life-cycle management of VNFs

8) List the components NETCONF-YANG?

1. Management System
2. Management API
3. Transaction Manager
4. Rollback Manager
5. Data Model Manager
6. Configuration Validator
7. Configuration Database
8. Configuration API
9. Data Provider API

9) What is Software-defined Networking in IoT?

To make networks more adaptable and flexible, Software-defined Networking in IoT is an architecture that easily abstracts many different layers of a network. SDN aims to improve network control by enabling enterprises and service providers to respond quickly to changing business requirements.

10) Different types of software-defined networking

1. **Open SDN:** Open SDN uses open protocols to control the virtual and physical devices responsible for routing the data packets.
2. **API SDN**: API SDN uses programming interfaces, called southbound APIs, to control data flow to and from each device.
3. **Overlay Model SDN**: Overlay Model SDN creates a virtual network above existing hardware, providing tunnels containing channels to data centers. This model then allocates bandwidth in each channel and assigns devices to each channel.
4. **Hybrid Model SDN:** Hybrid Model SDN combines SDN and traditional networking, allowing the optimal protocol to be assigned for each type of traffic. Hybrid SDN is often used as a phase-in approach to SDN.

11) Define Domain Model Specification?

The domain model describes the main concepts, entities and objects in the domain of the IoT system to be designed. Domain model defines the attributes of the objects and relationships between objects. The domain model is independent of any specific technology or platform.Using domain model, system designers can get an understanding of the IoT domain for which the system is to be designed.

12) What is Information Model Specification?

Information model defines the structure of all the information in the IoT system. Does not describe how the information is stored and represented. To define the information model, we first list the virtual entities. Later more details like attributes and relationships are added.

13) What is Functional View Specification?

The functional view defines the functions of the IoT systems grouped into various functional groups. Each functional group provides functionalities for interacting with concepts in the domain model and information related to the concepts.The functional groups in a functional view include: Device, Communication, Services, Management, Security, and Application.

14) List the characteristicsof Sensors?

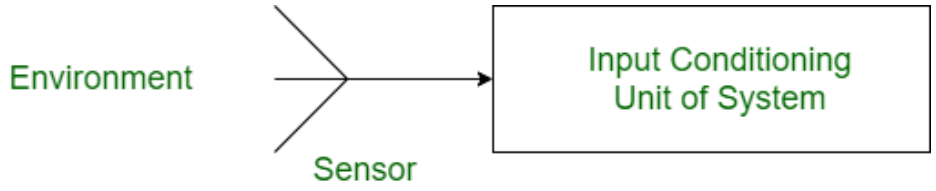
1. Static
2. Dynamic

15) List the Sensor Classification?

1. Passive & Active
2. Analog & digital
3. Scalar & vector

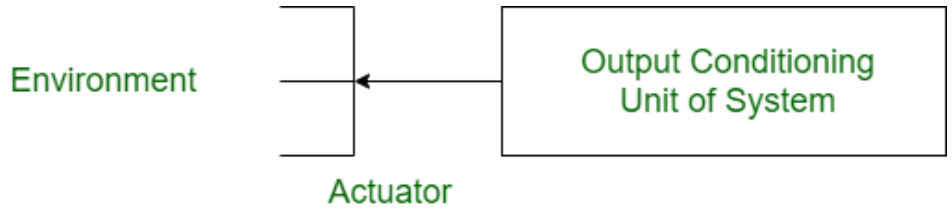
16) What is Sensor?

Sensor is a device used for the conversion of physical events or characteristics into the electrical signals. This is a hardware device that takes the input from environment and gives to the system by converting it.For example, a thermometer takes the temperature as physical characteristic and then converts it into electrical signals for the system.



17) What is Actuator?

Actuator is a device that converts the electrical signals into the physical events or characteristics. It takes the input from the system and gives output to the environment. For example, motors and heaters are some of the commonly used actuators.



18) What is Request & Response Model?

This model follows a client-server architecture.The **client**, when required, requests the information from the server. This request is usually in the encoded format. This model is stateless since the data between the requests is not retained and each request is independently handled. The server Categories the request, and fetches the data from the database and its resource representation. This data is converted to response and is transferred in an encoded format to the client. The client, in turn, receives the response.

19) Difference between Sensor and Actuator?

SENSOR	ACTUATOR
It converts physical characteristics into electrical signals.	It converts electrical signals into physical characteristics.
It takes input from environment.	It takes input from output conditioning unit of system.
It gives output to input conditioning unit of system.	It gives output to environment.
Sensor generated electrical signals.	Actuator generates heat or motion.
It is placed at input port of the system.	It is placed at output port of the system.
It is used to measure the physical quantity.	It is used to measure the continuous and discrete process parameters.
It gives information to the system about environment.	It accepts command to perform a function.
Example: Photo-voltaic cell which converts light energy into electrical energy.	**Example**: Stepper motor where electrical energy drives the motor.

20) What is Publisher-Subscriber Model?

This model comprises three entities: Publishers, Brokers, and Consumers.

- **Publishers** are the source of data. It sends the data to the topic which are managed by the broker. They are not aware of consumers.
- **Consumers** subscribe to the topics which are managed by the broker.
- Hence, **Brokers** responsibility is to accept data from publishers and send it to the appropriate consumers. The broker only has the information regarding the consumer to which a particular topic belongs to which the publisher is unaware of.

21) What is Push-Pull Model?

The push-pull model constitutes data publishers, data consumers, and data queues.

- **Publishers** and **Consumers** are not aware of each other.
- Publishers publish the message/data and push it into the queue. The consumers, present on the other side, pull the data out of the queue. Thus, the queue acts as the buffer for the message when the difference occurs in the rate of push or pull of data on the side of a publisher and consumer.
- **Queues** help in decoupling the messaging between the producer and consumer. Queues also act as a buffer which helps in situations where there is a mismatch between the rate at which the producers push the data and consumers pull the data.

22) What is Exclusive Pair ?

- **Exclusive Pair** is the bi-directional model, including full-duplex communication among client and server. The connection is constant and remains open till the client sends a request to close the connection.
- The **Server** has the record of all the connections which has been opened.
- This is a state-full connection model and the server is aware of all open connections.
- WebSocket based communication API is fully based on this model.

23) What is LoRa?

LoRa technology was developed by a company called Semtech and it is a new wireless protocol designed specifically for long-range, low-power communications. LoRa stands for Long Range Radio and is mainly targeted for M2M and IoT networks. This technology will enable public or multi-tenant networks to connect a number of applications running on the same network.

24) List the advantages of LoRa?

1. Better battery life
2. Long range
3. Cost effective for large deployment

25) Define RFID ?

Radio-frequency identification (RFID) is a technology that **enables communication and data transmission via radio waves.** It automatically identifies and tracks tags attached to the object.

26) How RFID works?

RFID is a wireless system referred to as Automatic Identification and Data Capture (AIDC). The purpose of AIDC is identifying, tracking, recording, storing, and communicating essential data. The system consists of an RFID reader, RFID tags, and an antenna. An RFID tag consists of a transponder, a radio receiver, and a transmitter. Firstly, tags transmit digital data; it emits a unique identification code. Secondly, the primary responsibility of the antenna is to transmit and receive radio waves for communication. Thirdly, the Reader communicates with any tags in its read range. After that, it sends tags' data to an application that can use the data. The data collected from the tag can then be sent either directly to a host computer or stored in a portable reader and uploaded later to the host computer.

UNIT III - IOT PROTOCOLS

1) Define SCADA?

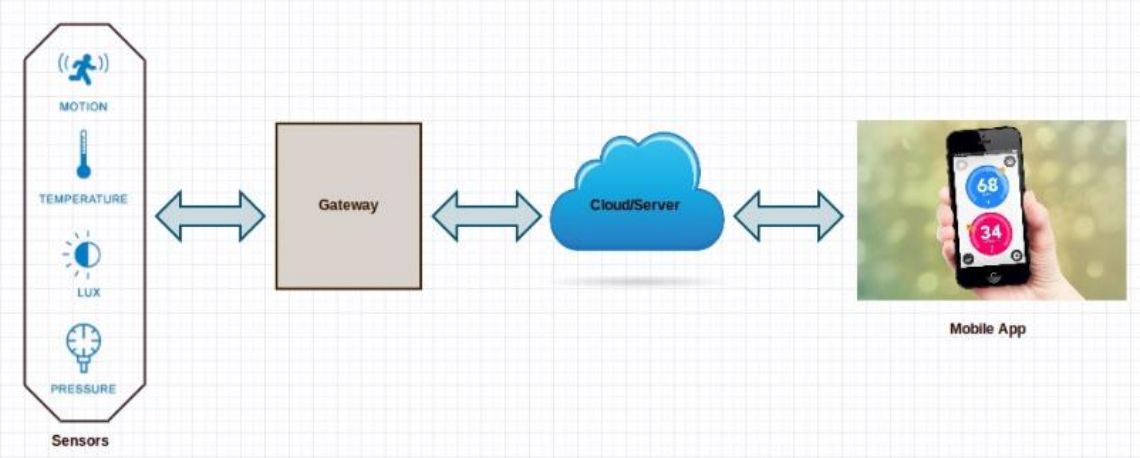
SCADA (Supervisory Control and Data Acquisition) and RFID (Radio Frequency Identification) protocols are two critical technologies that have transformed various industries. SCADA systems allow for remote monitoring and control of industrial processes in the oil and gas, energy, and manufacturing industries. These systems collect data from sensors and deliver it in real-time to human operators, allowing them to monitor and adjust the process as needed.

2) What is SCADA?

SCADA stands for **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition.

SCADA is a category of software applications for controlling industrial processes, which is the gathering of data in real time from remote locations in order to control equipment and conditions. SCADA provides organizations with the tools needed to make and deploy data-driven decisions regarding their industrial processes.

3) How does The SCADA work:



4) Define BACNet Protocol?

• Communications protocol for **B**uilding **A**utomation and Control (BAC) **N**etworks

• Provides mechanisms for computerized building automation devices to exchange information

• Designed to allow communication of building automation & control system for application like

- Heating, Ventilating and Air-conditioning Control (HVAC)
- Lighting Control, Access Control
- Fire Detection Systems and their Associated Equipment

5) What is BACnet Protocol Architecture?

The BACnet protocol architecture is predominately restricted to lighting controls, HVAC & gateways. This protocol highlights lightweight and efficient communication which is optimized for short messages, small networks, and inter-networks.

6) What is MODBUS?

Modbus is a **serial communications protocol** originally published by Modicon (now Schneider Electric),Used to establish **master-slave/client-server** communication between intelligent devices,Openly published and royalty-free,Modbus**enables communication between many (approximately 247) devices** connected to the same network

7) List and define the Types of Modbus Communication Protocol?

Modbus serial protocol (the original version) is a master/slave protocol, e.g. one master that controls the Modbus data transactions with multiple slaves that respond to the master's requests to read from or write data to the slaves.

Modbus TCP, also known as Modbus TCP/IP, uses a client/server architecture. Network architectures are shown in Figures below.

8) Difference between BACnet Protocol and Modbus?

BACnet Protocol	Modbus
It was developed by ASHRAE.	It was developed by Modicon Inc.
Bacnet is used for communication across devices.	Modbus is used for communication between devices.
Its transmission modes are; IP, Ethernet, Zigbee & MS/TP.	Its transmission modes are; ASCII, RTU, and TCP/IP.
Its standards are; ANSI/ASHRAE Standard 185; ISO-16484-5; ISO-16484-6.	Its standards are; IEC 61158.
It is used in different markets like Industrial, Energy Management, Transportation, Building Automation, Regulatory, health & security.	It is used in different markets like Lighting, Life Safety, Access Controls, HVAC, transportation & maintenance.
Network Interfaces: Existing LANs &LANs infrastructure.	Network Interfaces: Traditional serial & Ethernet protocols.
Examples: Measurements of Tank Level. Boiler Control.	Examples: Tasks like fan schedule, sending a status alarm, and requesting temperature reading.

9) Define ZigBeeCoordinator (ZC)?

The Coordinator forms the root of the ZigBee network tree and might act as a bridge between networks.There is a single ZigBeeCoordinator in each network, which originally initiates the network.It stores information about the network under it and outside it.It acts as a Trust Center& repository for security keys.

10) Define ZigBeeRouter (ZR)?

It is Capable of running applications, as well as relaying information between nodes connected to it.

11) Define ZigBeeEnd Device (ZED)?

- It contains just enough functionality to talk to the parent node, and it cannot relay data from other devices.
- This allows the node to be asleep a significant amount of the time thereby enhancing battery life.
- Memory requirements and cost of ZEDs are quite low, as compared to ZR or ZC.

12) List some of the application of Zigbee?

1. Building automation
2. Remote control (RF4CE or RF for consumer electronics)
3. Smart energy for home energy monitoring
4. Health care for medical and fitness monitoring
5. Home automation for control of smart homes
6. Light Link for control of LED lighting
7. Telecom services

13) Define APS Layer?

• Application Support Sublayer (APS)

• Provides services necessary for application objects (endpoints) and the ZigBee device object (ZDO)

• Some of services provided by the APS to the application objects for data transfer are

• Request

- Confirm
- Response

14) What is ZigBee Device Object (ZDO)

It is used to Control and management of application objects ,it also Performs overall device management tasks:

- Determines the type of device in a network (for example, end device, router, or coordinator)
- Initializes the APS, network layer, and security service provider
- Performs device and service discovery
- Initializes coordinator for establishing a network

15) Define 6LoWPAN?

The IPv6 Low Power Wireless Personal Area Network (6LoWPAN) standard allows IPv6 to be used over 802.15.4 wireless networks. 6LoWPAN is often used for wireless sensor networks, and the Thread protocol for home automation devices also runs over 6LoWPAN.

6LoWPAN is an IPv6 protocol, and It's extended from is IPv6 over Low Power Personal Area Network. As the name itself explains the meaning of this protocol is that this protocol works on Wireless Personal Area Network i.e., WPAN.

16) List the Features of 6LoWPAN?

- It is used with IEEE 802.15,.4 in the 2.4 GHz band.
- Outdoor range: ~200 m (maximum)
- Data rate: 200kbps (maximum)
- Maximum number of nodes: ~100

17) List the Advantages of 6LoWPAN?

1. 6LoWPAN is a mesh network that is robust, scalable, and can heal on its own.
2. It delivers low-cost and secure communication in IoT devices.
3. It uses IPv6 protocol and so it can be directly routed to cloud platforms.
4. It offers one-to-many and many-to-one routing.

5. In the network, leaf nodes can be in sleep mode for a longer duration of time.

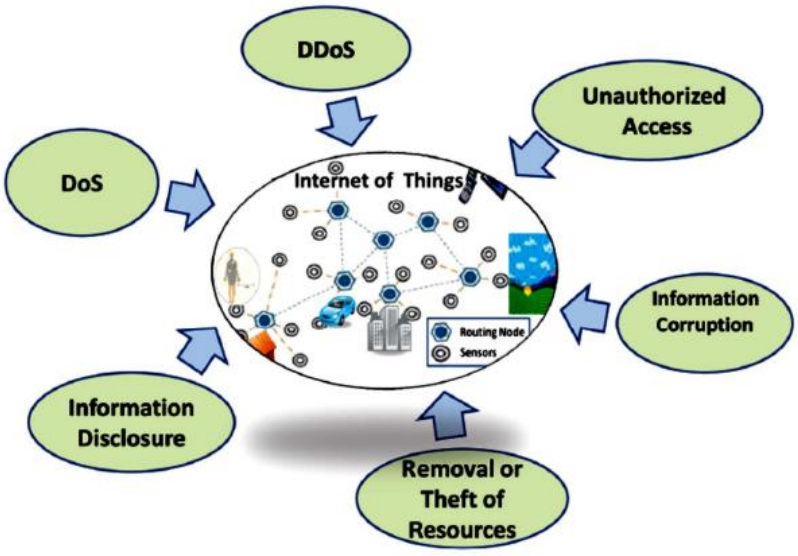
18) List the Disadvantages of 6LoWPAN?

1. It is comparatively less secure than Zigbee.
2. It has lesser immunity to interference than that Wi-Fi and Bluetooth.
3. Without the mesh topology, it supports a short range.

19) Define CoAP?

CoAP (Constrained Application Protocol) is a session layer protocol that provides the RESTful (HTTP) interface between HTTP client and server. It is designed by IETF Constrained RESTful Environment (CoRE) working group. It is designed to use devices on the same constrained network between devices and general nodes on the Internet. CoAP enables low-power sensors to use RESTful services while meeting their low power constraints. This protocol is specially built for IoT systems primarily based on HTTP protocols.

20) Draw the diagram for Different Vulnerabilities of IoT?



21) List the Key Elements of Security?

- Authentication
- Access Control
- Data and Message Security

• Prevention from denial of taking part in a transaction

UNIT IV - BUILDING IoT WITH CLOUD AND DATA ANALYTICS

1) Define IoT platforms?

As in IoT, all the IoT devices are connected to other IoT devices and application to transmit and receive information using protocols. There is a gap between the IoT device and IoT application. An IoT Platform fills the gap between the devices (sensors) and application (network). Thus we can say that an IoT platform is an integrated service that fulfills the gap between the IoT device and application and offers you to bring physical object online.

2) What is Amazon Web Services (AWS) IoT platform?

Amazon Web Service IoT platform offers a set of services that connect to several devices and maintain the security as well. This platform collects data from connected devices and performs real-time actions.

3) What is Microsoft Azure IoT platform?

Microsoft Azure IoT platform offers strong security mechanism, scalability and easy integration with systems. It uses standard protocols that support bi-directional communication between connected devices and platform. Azure IoT platform has an Azure Stream Analytics that processes a large amount of information in real-time generated by sensors. Some common features provided by this platform are:

- Information monitoring
- A rules engine
- Device shadowing
- Identity registry

4) What is Arduino in IoT?

Arduino acts as the brain of the system and processes the data from the sensor. Arduino is an open source hardware platform that is readily available for hobbyists & enthusiasts across the globe to build projects. It comes with an ATMEGA microcontroller that processes the data and facilitates the proper working of the IoT system. And the beauty is that the Arduino can be programmed 'n' number of times making it possible for you to build various types of IoT projects just by changing a simple code.

5) What is a Raspberry Pi?

It is a cheap, credit-card-sized device that uses a daily keyboard and mouse and joins to a TV or computer monitor. It is a thin weighable computer that let every person of all ages to discover programming and gain how to program in variant languages like Python and Scratch. From exploring the internet and watching high-definition video, word-processing, to creating spreadsheets, and it can do every possible thing we'd expect a desktop computer to do and playing sports.

6) What is Cloud IoT?

Cloud IoT is a technology architecture that connects IoT devices to servers housed in cloud data centers. This enables real-time data analytics, allowing better, information-driven decision making, optimization, and risk mitigation. Cloud IoT also simplifies management of connected devices at-scale.

7) How Does Cloud IoT Work?

Cloud IoT connects IoT devices – ***which collect and transmit data*** – to cloud-based servers via communication protocols such as MQTT and HTTP and over wired and wireless networks. These IoT devices can be managed and controlled remotely and integrated with other cloud services.IoT data is sourced from anywhere and everywhere, including sensors, actuators, operating systems, mobile devices, standalone applications, and analytic systems. By involving the cloud, vast amounts of IoT data can be stored and processed in a central location.

8) What are the Cloud Services for IoT?

Cloud platforms deliver a collection of capabilities that allow Internet of Things (IoT) devices to interact with cloud services, other applications, and even other IoT devices. These cloud

platforms let users centrally onboard, manage, monitor, and control IoT devices.In addition, the cloud supports services such as scalable storage, device connectivity, analytics and reporting, and identity and access management (IAM) in IoT.

9) Define Identity and Access Management (IAM)?

Security for the data generated by IoT devices can be protected in the cloud using Identity and Access Management (IAM), which is an authentication and authorization service. IAM enables organizations to grant or deny access to services and resources in the cloud for large numbers of users with different access needs.With so much IoT data being sent to the cloud, the granularity of IAM controls allows organizations to comply with security and regulations that are relevant for storing and accessing sensitive information.

10) How does cloud connectivity works?

Cloud connectivity is sometimes referred to as cloud networking. Users of a cloud network are granted access to networking resources that are provided by a centralized third-party provider that operates various connected servers. To make use of cloud connectivity, users obviously need to utilize a connectivity protocol, such as WAN, to send data quickly and securely

11) What are the advantages of IoT or M2M Cloud Connectivity?

1. Data Integration
2. Low Entry Barrier
3. Cloud+5G = new use cases
4. Security and Privacy
5. Higher Reliability
6. Facilitating Inter-device Communication
7. Better cloud connectivity through edge computing
8. The future of cloud connectivity and IoT

12) Define IoT Device SDK?

IoT Device SDK is used to help us quickly connect hardware devices to the IoT platform. We can download the IoT Device SDK from the corresponding cloud platform,

e.g. AWS IoT Device SDK.

13) Difference between DTU and industrial gateway?

DTU is a wireless terminal device used to convert serial data into IP data or IP data into serial data and transmit it through a wireless communication network. It has fast and flexible networking, a short construction period and low cost. The industrial gateway has the functions of collecting data from field devices through serial port or network port. Data collection, protocol analysis, data standardization and uploading to the IoT platform through edge computing functions. Which is more flexible, powerful and customizable than DTU, but it is more expensive and needs more resources to maintain.

14) How is big data used in IoT?

Big data analytics help to make sense of the data and information that is gathered by IoT devices. These solutions take the vast, unstructured data that's been collected, and identify ways to organize it into smaller data sets that can give companies insights into how their processes are working, as well as improve decision-making.

15) Define Data Visualization?

In order to present data understandably, data scientists utilize data visualization techniques. However, with vast amounts of real-time data of different formats and kinds, both structured and unstructured, visualization becomes more difficult to perform. Especially with the growing need for real-time data, taking too much time to efficiently visualize defeats the purpose. The future of data will require new visualization capabilities that will help people achieve their business goals

16) What are the Challenges in IoT data visualization?

Effective analysis of IoT data poses its own set of challenges. The data generated by sensors and sensor-enabled devices is different from the transactional data at the core of many organizations. It is usually less structured and requires a new set of tools to run an effective analysis.

17) List and define the Data visualization tools for IoT

- **Grafana tool** – It is an open-source visualization tool that is built to consume time-series metric data. It offers a visual dashboard that covers multiple functionalities. It also supports various data sources seamlessly like MySQL, PostgreSQL, Elasticsearch, and Prometheus, etc.

- **Kibana tool** – It is an open-source visualization tool that can be used to analyze large volumes of log data. It also contains interactive dashboards that can be easily converted into reports for future reference.
- **PowerBI tool** – It is a popular business intelligence tool from Microsoft for real-time data visualization. Like many of its predecessors, PowerBI can provide detailed analysis reports for large enterprises.
- **Tableau** – It is one of the most popular interactive data visualization tools. It offers an extremely intuitive interface, delivers powerful analytics, is easy to learn, allows integration with multiple data sources, and can manage large data volumes. All these and more such features make it a popular choice for world-leading companies like Bank of America, Amazon, Burger King, and EY.

UNIT V - CHALLENGES IN IOT AND CASE STUDIES

1. List the Security challenges in IoT?

- Lack of encryption
- Insufficient testing and updating
- Brute forcing and the risk of default passwords
- IoT Malware and ransomware
- IoT botnet aiming at crypto currency
- Inadequate device security
- Lack of standardization
- Vulnerability to network attacks
- Privacy concerns
- Unsecured data transmission
- Software vulnerabilities
- Insider threats

2. List the IoT security issues?

- Lack of visibility
- Limited security integration
- Open-source code vulnerabilities
- Overwhelming data volume
- Poor testing
- Weak passwords
- Vulnerable APIs
- Unpatched vulnerabilities

3.Explain the term 'smart city' in IoT.

IoT technology has been a driving force behind the development of smart cities since their inception. IoT technology will continue to grow as more countries adopt next-generation

connectivity, and it will have a greater impact on our lives. Connected sensors, lights, and meters are some of the IoT devices in smart cities that collect and analyze data. As a result, cities use this data to improve infrastructure, utilities, and other city services.

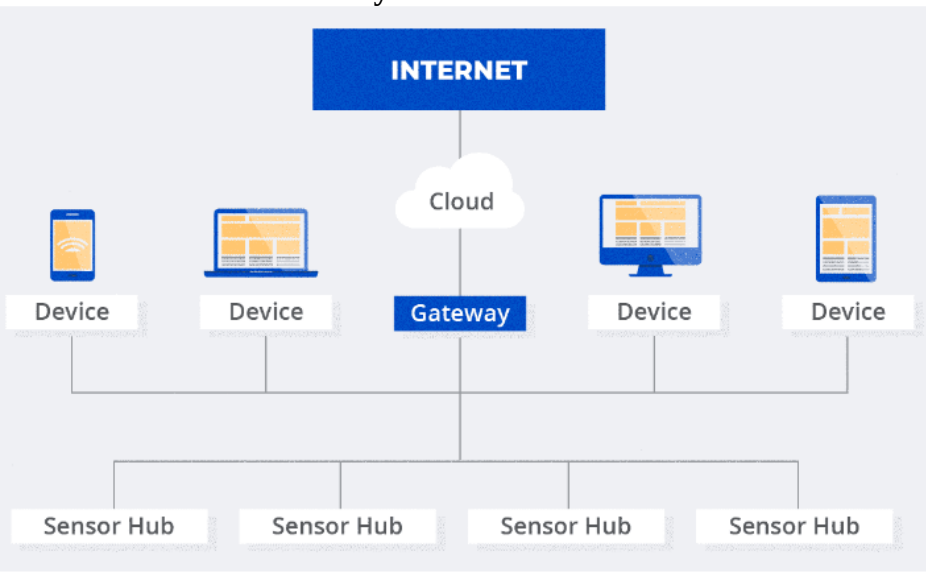
It is possible to create clever energy grids, automated waste management systems, smart homes, advanced security systems, traffic management mechanisms, water conservation mechanisms, smart lighting, and more with the help of the IoT. IoT has added a new layer of artificial intelligence and innovation to public utilities and urban planning, allowing them to be highly intuitive. These innovations have led to the emergence of smart homes and cities

4. What do you mean by PWM (Pulse Width Modulation)?

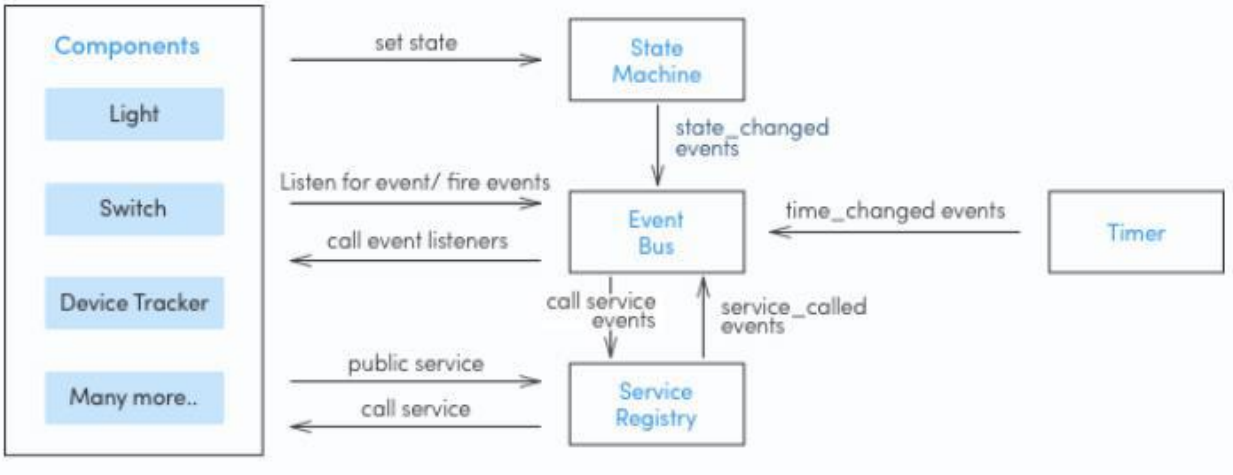
Have trouble adjusting the brightness of the LEDs in your project? Changing the voltage of the power supply directly in the circuit isn't easy. In that case, you can use Pulse Width Modulation (PWM).

Pulse Width Modulation (PWM), also referred to as PDM (Pulse Duration Modulation) refers to changing the amount of power that is delivered to a device. PWM is a technique for generating an analog signal from a digital source and is an efficient way to control the amount of energy delivered to a load without wasting any energy. PWM regulates voltage and is therefore used to control brightness in Smart Lighting Systems and also to control motor speed

5. How Does an IoT-Based Automation System Work?



6. Draw the core architecture of Home Assistant?



7. What is IoT-Enabled Smart Lighting?

Smart lighting uses IoT-enabled sensors, bulbs, or adapters to allow users to manage their home or office lighting with their smartphone or smart home management platform. Smart lighting solutions can be controlled through an external device like a smartphone or smart assistant, set to operate on a schedule, or triggered by sound or motion.

8. Key Benefits of IoT-Enabled Smart Lighting

- Save money by switching to more energy-efficient LED bulbs.
- Set schedules to ensure that lights are off when they aren't needed – or control lighting schedules remotely as a security measure when you're away from home or out of town.
- Adjust the color or dimness of lights in different rooms or individual bulbs.

9. Smart traffic management

This offers an array of routes to manage unruly traffic. In cases of a road incident, it promptly arranges for aid via real-time updates. Of course, these systems are closely in contact with the traffic police. A smart vehicle system has been crafted for accident prevention and accident location detection. Within this system, the shock sensor, ultrasonic sensor and temperature sensor function as an input along with GPS and GSM for real-time analysis. In case of a mishap, the processing unit takes the necessary action.

10. Working of Smart water management?

There is a wealth of real-time data about water systems and water bodies. IoT can make this wealth available to you. As a result, water resources can be managed smoothly with minimal wastage.

11. What the use of Smart waste management?

Sensors to the rescue again! These can identify full garbage bins and inform the public authorities accordingly. What's more, when relevant data is collected and stored, the cost of operations can go down.

These are a few of the ways in which IoT is likely to play a compelling role in enhancing city life. All in all, considering their myriad advantages, smart homes and smart cities are gifts of the futuristic technology of IoT

12. What issues you would come into while parking vehicles?

Parking lot is saturated– The most severe issue is the increasing number of vehicles with no increase in the parking space, hence, resulting in the jam.

Overpay– Sometimes,drivers or customer don't know how long they will stay at a specific place. Therefore, they overpay the parking fees sometimes.

Environment impact– The parking lot accumulated amounts of contaminant that are unable to be absorbed, which are flushed into the water body when raining.

On-street or Off-street parking– There're not enough space on the parking lot of the shopping malls or reservation areas, in this case, severe traffic jam will appear.

Improper use of existent parking lot– People are always in a hurry and get impatient to parking properly, which result in insufficient parking space for other vehicles.

13. How can you install a smart parking sensor using IoT?

Different kinds of sensors are installed in different ways. For Example, camera is tricky, so it needs to be installed in a certain distance and angle to avoid blind spot. Laser radar sensor usually be installed in a pillar with 30~80 centimeters and be located repeatedly in a certain range, but it makes sense only when conducting massive processing.

The in-ground vehicle IoT sensors are the most easiest to be installed, which usually be installed on the ground of every parking lot to detect the vehicle parked above. Such IoT sensors can be simply glued on the surface or fixed with screws. Additionally, such IoT sensors are easy to be transformed without any unique installation practice and most of them don't need any maintenance. The smart parking system using iot can communicate with gateway through parking site and transfer the data to the internet.

14. What components involved in the smart parking system using IoT?

- A sensor that can detect the presence of the vehicle.
- A micro control that can help you processing the data.
- A cloud platform will restore the data.
- A mobile application enables you to control the smart parking process.

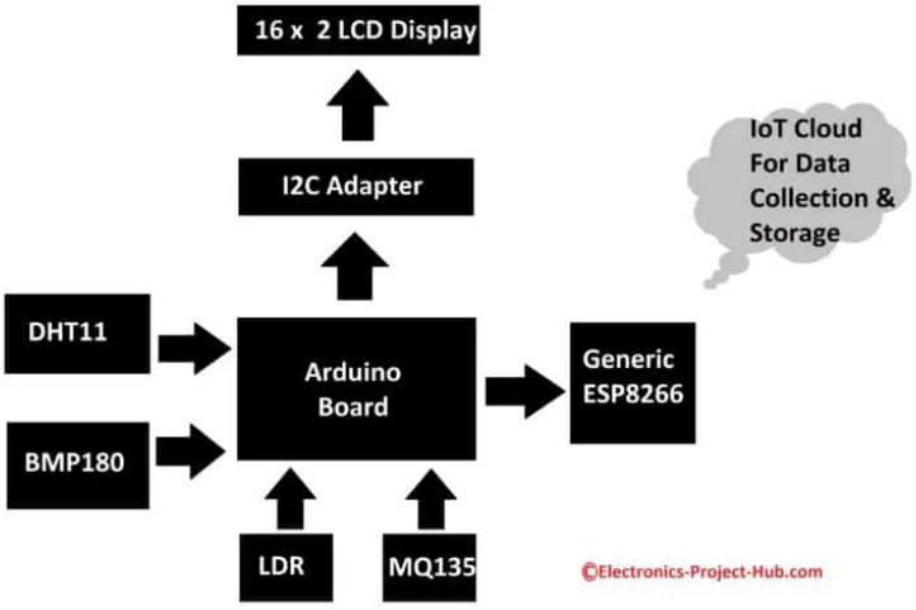
15. What is an IoT based weather monitoring system?

It is a system that involves in acquiring weather and environment data using advanced electronic sensors and sending them to a web server via internet for real time weather monitoring and storage of data for future analysis and study.

16. Why we need an IoT based weather monitoring system?

1. Ease of monitoring your local weather conditions in real time from anywhere in the world.
2. For storing weather and environment data for short and long term for studying weather pattern changes and to understand how human induced climate change affected your local weather.
3. Easy deployment of the setup for monitoring local atmospheric conditions and microclimates for weather forecasting and prediction

17. Draw Block diagram of IoT based weather monitoring system?



Block diagram – IoT based weather monitoring system

PART B QUESTIONS

UNIT - 1

1. Explain architecture of IOT with neat Sketch
2. Elaborate the Different IOT Levels in detail
3. Explain in detail about Various IOT communication models with neat Sketch
4. Elaborate the IOT communication API in detail
5. Elaborate the various enabling technologies is detail.
6. Write short notes on embedded system.
7. Explain wireless sensor network with examples.

UNIT – 2

1. Explain NETCONF-YANG with neat diagram
2. Write Short notes on LoRa,
3. Write Short notes on RFID
4. Write Short notes on WI-FI.
5. Elaborate the difference between IoT and M2M.
6. Explain IOT Design Methodology?
7. Explain SDN Architecture with neat diagram
8. Elaborate the Network Function Virtualization in detail.
9. Explain in detail about sensors and actuators.

UNIT- 3

1. Explain SCADA and RFID Protocols with neat diagram.
2. Discuss about on M2M and WSN protocol.
3. Write Short notes on Modbus?
4. Write Short notes on Zigbee Architecture.
5. Discuss about on BACNet protocol with suitable diagram.
6. Write short notes on 6LoWPAN.
7. Explain briefly on COAP architecture with neat diagram?

8. Elaborate briefly on various IOT securities.

UNIT – 4

1. Explain architecture of Arduino with neat Sketch.
2. Write briefly about Raspberry Pi in detail with neat diagram.
3. Elaborate the Big Data analytics in detail.
4. Elaborate the Cloud Computing in IoT in detail.
5. Explain about data visualization in detail.

UNIT – 5

1. Explain about Real time applications of IoT.
2. Write short notes on Home automation using IoT.
3. Write short notes on Automatic lighting and Home intrusion detection using IoT.
4. Explain about Smart parking Weather monitoring system using IoT.
5. Elaborate how IoT used in Agriculture and Irrigation.