Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – WINTER 2021

Subject Code:3171108

Date:23/12/20

21 Subject Name: Internet of things

Time: 10:30 AM TO 01:00 PM **Total Marks: 70**

MARKS

Q.1 **(a)** Define IOT. Also few Applications of IOT. **03**

IoT stands for Internet of Things. It is a network of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to connect and exchange data.

Applications of IoT include:

1. Smart Home: Control lights, temperature, and security remotely using a smartphone app.
2. Industrial IoT: Monitor and control industrial equipment and machinery to improve efficiency and productivity.
3. Connected Cars: Monitor vehicle performance and provide driver assistance.
4. Healthcare: Monitor patients remotely and improve their treatment outcomes.
5. Smart City: Collect and analyze data from various sensors to improve city services and infrastructure.
6. Supply Chain and Logistics: Track inventory and shipments in real-time to improve efficiency and reduce costs.

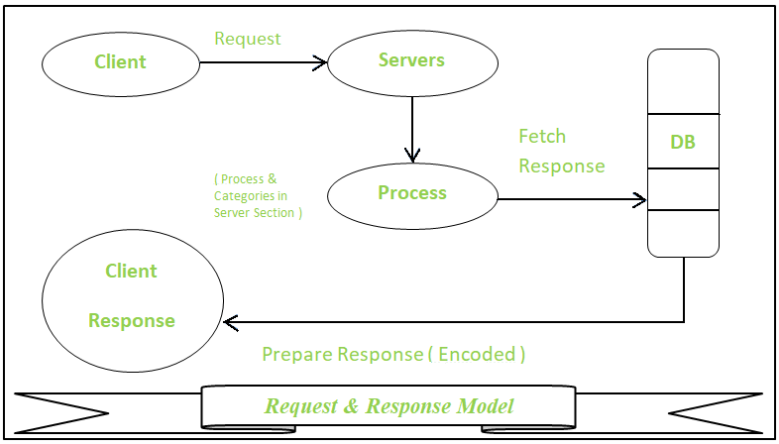
(b) Write Various characteristics of IOT. **04**

1. Connectivity: IoT devices are connected to the internet and can communicate with each other.
2. Sensors: IoT devices are equipped with sensors that collect data and send it to other devices or systems.
3. Intelligence: IoT devices are capable of making decisions and performing actions based on the data they collect.
4. Automation: IoT devices can automate tasks and processes, reducing the need for human intervention.
5. Scalability: IoT can include a large number of devices and can be easily expanded.
6. Remote Access: IoT devices can be accessed and controlled remotely via a smartphone or computer.
7. Real-time data: IoT devices can collect and transmit data in real-time, allowing for immediate action to be taken.
8. Interoperability: IoT devices can connect and communicate with different types of devices and systems.

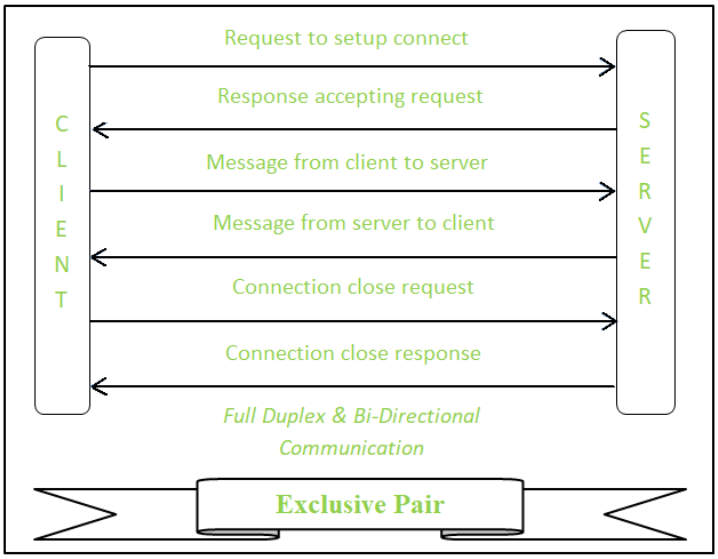
9. Security: IoT devices need to be secure to protect the data they collect and transmit.
10. Adaptability: IoT systems can be adapted to changing requirements and environments.

(c) Write about Request – Response and Exclusive Pair Communication model of IOT. **07**

The Request-Response model is a common communication pattern in IoT, where a device (the client) sends a request to another device (the server) and the server responds with the requested information. This pattern is used in many applications, such as when a smart thermostat requests the temperature from a sensor or when a smartphone app requests the status of a connected light bulb.



Exclusive Pair Communication model is a communication model where two devices are exclusively paired with each other and can only communicate with each other. This model is particularly useful when two devices need to exchange sensitive information and there is a need to ensure that the information is only exchanged between the two devices and no one else can access it. An example of this model is when a smartwatch is paired with a smartphone to exchange sensitive health data.



Both the Request-Response and Exclusive Pair Communication models are widely used in IoT to enable communication between devices and enable the collection, analysis and transmission of data.

Q.2 (a) Describe Bluetooth and BLE. **03**

Bluetooth is a wireless communication technology that enables devices to communicate with each other over short distances. It uses a 2.4 GHz radio frequency to transmit data and can be used to connect devices such as smartphones, laptops, speakers, and headphones. Bluetooth devices can be paired with each other to establish a connection, and once connected, they can exchange data. Bluetooth technology is widely used in IoT applications such as home automation, wearables, and smart home devices.

BLE (Bluetooth Low Energy) is a version of Bluetooth technology that is designed for low-power devices and applications. BLE uses a lower amount of power compared to classic Bluetooth and is ideal for devices that need to run on batteries for long periods of time. BLE is also designed to consume less power when it is in standby mode, making it a good choice for IoT devices that need to be always on and ready to communicate. BLE is commonly used in applications such as fitness trackers, smartwatches, and other wearable devices.

BLE is different from classic Bluetooth in that it has a lower data rate and is optimized for low power consumption. This makes it suitable for IoT devices that need to be always on and ready to communicate, but not necessarily transfer large amounts of data.

(b) What is REST? Write various methods of REST. **04**

REST (Representational State Transfer) is an architectural style for building web services. RESTful web services use HTTP requests to POST (create), PUT (update), GET (read), and DELETE data. A RESTful web service typically defines a URI (Uniform Resource Identifier), which is a service endpoint and a set of HTTP methods that operate on the resource identified by the URI.

The main methods of REST are:

1. GET: Retrieves information about a resource. It is used to retrieve data from the server.
2. POST: Creates a new resource. It is used to send data to the server to create a new resource.
3. PUT: Updates an existing resource. It is used to send data to the server to update an existing resource.
4. DELETE: Deletes a resource. It is used to delete a resource from the server.
5. PATCH: partially updates a resource. It is used to send data to the server to partially update an existing resource.

These methods are also referred to as CRUD (Create, Read, Update and Delete) operations, which are used to perform actions on resources. RESTful web services use these methods to interact with a resource, and the resource is identified by a URI.

(c) Write about IOT Level – 5 and IOT Level – 6. **07**

IoT Level 5 refers to fully autonomous systems, where the IoT devices are able to make decisions and take actions without human intervention. These systems use advanced technologies such as machine learning and artificial intelligence to analyze data and make decisions. Examples of Level 5 IoT systems include self-driving cars, drones, and robots. **07**

IoT Level 6 refers to systems that are integrated into the physical environment and can interact with it in a natural way. These systems use technologies such as augmented reality, virtual reality, and haptic feedback to enhance the user's experience. Examples of Level 6 IoT systems include smart homes, smart cities, and virtual/augmented reality-based applications.

At the highest level, Level 6 IoT systems are able to learn from the environment and adapt to the user's preferences and habits. They allow for the seamless integration of technology into the physical world, creating an immersive and intuitive experience for the user.

It's worth mentioning that these levels are not an official classification and may vary across different sources, and also these levels are not absolute, as many of the IoT systems can have a mix of characteristics of different levels.

OR

What is NFV(Network Function Virtualization)? And write key elements of NFV.

Network Function Virtualization (NFV) is a technology that enables the virtualization of network functions that were previously provided by dedicated hardware. Instead of using physical network devices, NFV allows these functions to be implemented in software and run on commercial off-the-shelf (COTS) servers.

The key elements of NFV include:

1. Virtualized Network Functions (VNFs): These are the software implementations of network functions such as firewalls, routers, and load balancers.
2. Virtualized Infrastructure Manager (VIM): This is the management layer that controls the virtualized resources, such as servers and storage, that are used to run VNFs.
3. NFV Orchestration (NFVO): This is the management and orchestration layer that coordinates the deployment and management of VNFs and other network functions.
4. Virtual Network Functions Management and Orchestration (VNFM/O): This is the management layer that is responsible for the lifecycle management of VNFs.

5. Hardware Abstraction Layer (HAL): This is the layer that abstracts the physical resources, such as servers and storage, from the VNFs.

NFV enables network operators to be more agile and flexible in deploying and managing network services, as well as reduces costs by using commodity hardware instead of dedicated network devices. It also allows for the dynamic scaling of network resources, making it easier to handle fluctuations in traffic and user demand.

Q.3 (a) Write various Security concerns dealing with IOT. **03**

IoT security is a major concern as it involves a wide range of devices that collect, transmit, and process sensitive information. Some of the security concerns with IoT include:

1. Device security: IoT devices are often vulnerable to hacking and malware attacks, which can compromise the device's security and expose sensitive information.
2. Network security: IoT devices communicate over a network, and if the network is not secure, it can be vulnerable to attacks such as man-in-the-middle (MitM) and eavesdropping.
3. Data security: IoT devices collect and transmit sensitive information, and if this data is not properly secured, it can be intercepted and used for malicious purposes.
4. Privacy: IoT devices can collect and transmit personal information, and if this information is not properly protected, it can be used to track and profile users.
5. Interoperability: IoT devices are often built by different manufacturers and may use different protocols, which can make it difficult to ensure that they are secure.
6. Lack of security standards: There is a lack of security standards for IoT devices, which makes it difficult to ensure that devices are secure.
7. Distributed Denial of Service (DDoS) attacks: IoT devices can be used as part of a botnet to launch DDoS attacks on other systems.

(b) What is M2M? Describe it with few examples. **04**

M2M stands for Machine-to-Machine communication, it refers to the communication between devices and systems without human intervention. These devices can be computers, smartphones, sensors, machines, vehicles, and other equipment that are connected to the internet and can communicate with each other.

Examples of M2M include:

1. Smart grid: Smart meters and other devices in the power grid communicate with each other to manage energy consumption and optimize the distribution of electricity.
2. Remote monitoring: Sensors and cameras can be used to remotely monitor industrial equipment and machinery, allowing for early detection of problems and reducing downtime.

3. Automated inventory management: RFID tags and sensors can be used to track inventory and automatically reorder products when stock is low.
4. Telematics: GPS and other sensors can be used to track vehicles and monitor their performance, which can improve fleet management and reduce costs.
5. Smart cities: Sensors and cameras can be used to collect data on traffic, air quality, and other environmental factors, which can be used to improve city services and infrastructure.

M2M communication enables devices to communicate with each other, share data, and make decisions automatically. This allows for more efficient and effective operations, improved decision making, and the ability to monitor and control devices remotely.

(c) Discuss Difference between IOT and M2M. **07**

IoT (Internet of Things)	M2M (Machine-to-Machine)
IoT refers to the network of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to connect and exchange data.	M2M refers to the communication between devices and systems without human intervention. These devices can be computers, smartphones, sensors, machines, vehicles, and other equipment that are connected to the internet and can communicate with each other.
IoT devices are connected to the internet and can communicate with each other.	M2M devices are connected to each other and can communicate with each other.
IoT includes a wide range of devices, such as smartphones, laptops, home appliances, and industrial equipment.	M2M mainly focuses on industrial and commercial applications, such as manufacturing, transportation, and logistics.
IoT is designed to improve the efficiency and effectiveness of daily life.	M2M is designed to improve the efficiency and effectiveness of industrial and commercial operations.

03

OR

Q.3 **(a)** Write functionality of XMPP.

XMPP (Extensible Messaging and Presence Protocol) is an open-source communication protocol used for real-time messaging and presence information. It is designed for instant messaging, online gaming, and other real-time applications.

The main functionality of XMPP includes:

1. Instant Messaging: XMPP allows users to send and receive instant messages in real-time. It supports one-to-one and multi-user chats, and can also be used for group chats and conference calls.

2. Presence Information: XMPP allows users to share their status (e.g. online, offline, away) and other presence information with their contacts.
3. Roster Management: XMPP allows users to manage their contacts, also known as "roster" in XMPP parlance, and see the presence information of their contacts.
4. Extensibility: XMPP is designed to be extensible, which means that new features and functionality can be added through the use of "XMPP Extensions".
5. Security: XMPP supports encryption and authentication for secure communication.
6. Publish-Subscribe: XMPP allows for publish-subscribe pattern which means that the client can subscribe to certain topics and receive updates on those topics.
7. Interoperability: XMPP allows communication between different clients and servers, regardless of their platform or vendor.
8. Server-to-Server Communication: XMPP allows communication between different servers, this enables users to communicate across different domains.

XMPP is widely used in IoT and M2M communication, it allows devices to communicate with each other, share data and make decisions automatically, this is particularly useful for IoT applications such as home automation, remote monitoring, and smart cities.

(b) Write an arduino code for connecting NodeMCU with temperature and Humidity sensor. And display current temperature and humidity with 5 second delay. **07**

Here is an example of Arduino code for connecting a NodeMCU board to a DHT11 temperature and humidity sensor and displaying the current temperature and humidity with a 5-second delay

```
#include <Adafruit_Sensor.h>

#include <DHT.h>

#include <DHT_U.h>


#define DHTPIN 2     // Pin where DHT sensor is connected

#define DHTTYPE DHT11   // DHT 11


DHT dht(DHTPIN, DHTTYPE);


void setup() {

  Serial.begin(115200);

  dht.begin();
```

```
}

void loop() {
  delay(5000);
  float h = dht.readHumidity();
  float t = dht.readTemperature();

  if (isnan(h) || isnan(t)) {
    Serial.println("Failed to read from DHT sensor!");
    return;
  }

  Serial.print("Humidity: ");
  Serial.print(h);
  Serial.print("%  Temperature: ");
  Serial.print(t);
  Serial.println("°C ");
}
```

In this code, we first include the necessary libraries: Adafruit_Sensor, DHT, and DHT_U. Then, we define the pin and type of the DHT11 sensor. In the setup function, we start the serial communication and initialize the DHT sensor. In the loop function, we use the delay function to wait for 5 seconds, then we use the dht.readHumidity() and dht.readTemperature() functions to read the current humidity and temperature values from the sensor. The humidity and temperature values are stored in variables h and t. We then use the serial.print() function to display the humidity and temperature values on the serial monitor.

Note: Make sure you have the DHT library installed in your Arduino IDE before uploading the code.

Also, ensure that the NodeMCU board is properly connected to the DHT11 sensor and that the correct pin number is used in the code.

(c) Explain SDN(Software Define Networking). **04**

Software-Defined Networking (SDN) is an approach to networking in which the control plane of network devices is separated from the data plane. The control plane is responsible for making decisions about how data is forwarded and the data plane is responsible for forwarding the data.

In traditional networking, the control plane and data plane are tightly coupled and are implemented in the same device. This makes it difficult to make changes to the network and to add new features. With SDN, the control plane is implemented in software and can run on a separate device, such as a server or a virtual machine. This separation allows for more flexibility and easier management of the network.

The key elements of SDN include:

1. The SDN Controller: This is the control plane of the network and is responsible for making decisions about how data is forwarded. The controller can be a physical or virtual device and can run a variety of software.
2. The Network Device: This is the data plane of the network and is responsible for forwarding data. The device can be a switch, router, or other network equipment.
3. The SDN Application: This is the application that runs on the controller and provides network services such as routing, load balancing, and security.
4. The SDN API: This is the interface between the controller and the network devices and allows for the controller to send instructions to the devices.

SDN can be used to improve the scalability, security, and manageability of the network. It allows for the network to be programmed and controlled in a more efficient way, which can lead to faster deployment of new services and reduced operational costs. It also allows for more flexibility in network design and can make it easier

Q.4 **(a)** Write Names of various protocols that are used at Network Layer of IOT. **03**

At the Network Layer of the IoT, a variety of protocols are used to enable communication between devices. Some of the most commonly used protocols at this layer include:

1. Internet Protocol (IP): This is the most widely used protocol at the Network Layer and is responsible for routing data packets between devices. IP can be used in both IPv4 and IPv6 versions.
2. Internet Control Message Protocol (ICMP): This protocol is used to send error messages and operational information about the

network.
3. Address Resolution Protocol (ARP): This protocol is used to map a network address to a physical address.
4. Routing Information Protocol (RIP): This is a distance-vector routing protocol used to distribute routing information within a network.
5. Open Shortest Path First (OSPF): This is a link-state routing protocol used to distribute routing information within a network.
6. Border Gateway Protocol (BGP): This is a path-vector routing protocol used to distribute routing information between different autonomous systems.
7. Multicast: This protocol is used to send data to multiple devices at the same time.
8. 6LoWPAN: This protocol is used to enable communication between IPv6 devices over low-power wireless networks.
9. CoAP: This is a protocol designed specifically for IoT devices and is used for resource-constrained devices and low-power networks.
10. MQTT: This is a publish-subscribe protocol that is designed for machine-to-machine (M2M) and IoT applications.

(b) Write Names of Protocols that are used at Link Layer of IOT. **04**

At the Link Layer of the IoT, a variety of protocols are used to enable communication between devices on the same network segment. Some of the most commonly used protocols at this layer include:

1. Media Access Control (MAC) protocol: This protocol is responsible for controlling access to the shared medium, such as a wireless channel or an Ethernet cable, and for addressing devices at the link layer.
2. Bluetooth: This is a wireless technology that is widely used in IoT devices for short-range communications.
3. Zigbee: This is a wireless protocol that is designed for low-power, low-data-rate communications and is often used in IoT applications.
4. Z-Wave: This is another wireless protocol that is designed for low-power, low-data-rate communications and is often used in IoT applications.
5. LoRaWAN: This is a long-range wireless protocol that is designed for low-power, low-data-rate communications and is often used in IoT applications.
6. Wi-Fi: This is a wireless protocol that is widely used in IoT devices for high-speed data communications.
7. Ethernet: This is a wired protocol that is widely used in IoT devices for high-speed data communications.
8. Thread: This is a protocol designed for IoT devices, which is based on IPv6 and 6LoWPAN, it's designed for creating low-power, secure, and reliable networks for connected devices in the home and building automation.
9. Zigbee 3.0: This is a new version of Zigbee protocol which is based on the Zigbee Pro and Smart Energy profile, it's designed for creating low-power, secure, and reliable networks for connected devices.

These protocols are suitable for different types of IoT applications and different types of networks, depending on the requirements of range, power consumption, data rate, and security.

(c) Write various Static Characteristics of Sensors. **07**

Static characteristics of sensors refer to the performance of a sensor when it is not changing or in a steady state. Some of the key static characteristics of sensors include:

1. Sensitivity: This refers to the ratio of the output of the sensor to the input. It is typically measured in units of output per unit of input.
2. Linearity: This refers to the degree to which the output of the sensor is proportional to the input. A sensor with high linearity will have a small deviation from a straight line when plotted on a graph.
3. Hysteresis: This refers to the difference in the output of the sensor when the input is increased or decreased. A sensor with low hysteresis will have a small difference in output when the input is increased or decreased.
4. Repeatability: This refers to the degree to which the sensor produces the same output for the same input. A sensor with high repeatability will produce the same output for the same input multiple times.
5. Accuracy: This refers to the degree to which the sensor's output is close to the true value of the input. A sensor with high accuracy will produce an output that is close to the true value of the input.
6. Resolution: This refers to the smallest change in the input that the sensor can detect. A sensor with high resolution will be able to detect small changes in the input.
7. Drift: This refers to the gradual change in the output of the sensor over time. A sensor with low drift will have a small change in the output over time.
8. Offset: This refers to the output of the sensor when the input is zero. A sensor with low offset will have a small output when the input is zero.
9. Noise: This refers to the unwanted variations in the output of the sensor that are not due to the input. A sensor with low noise will have a small unwanted variations in the output.
10. Range: This refers to the range of input that the sensor can detect. A sensor with a wide range will be able to detect a wide range of input.

OR

Q.4 (a) Define Sensors, Actuators, Transducers. **03**

A sensor is a device that detects changes in the environment and converts them into an electrical signal or other form of output. Sensors can measure a wide range of physical phenomena such as temperature, light, humidity, pressure, motion, and more. They are used in a variety of

applications such as industrial, automotive, and consumer electronics.

An actuator is a device that converts an electrical signal or other form of input into a physical action. Actuators can be used to control a wide range of physical phenomena such as movement, position, temperature, pressure, and more. Examples of actuators include motors, solenoids, and pneumatic and hydraulic cylinders.

A transducer is a device that converts one form of energy into another. Transducers can be used to convert physical phenomena such as temperature, light, sound, pressure, and motion into an electrical signal or other form of output. They can also be used to convert electrical signals into physical phenomena such as movement, position, and sound. Sensors and actuators are types of transducers, they convert physical quantities into electrical signals (sensors) or electrical signals into physical actions (actuators) respectively.

(b) Write about any 4 sensors that you know. And their usages. **04**

1. Temperature Sensor: A temperature sensor is a device that measures the temperature of an object or environment. They are used in a wide range of applications such as HVAC systems, automotive, industrial processes, and consumer electronics. Examples of temperature sensors include thermistors, thermocouples, and RTDs (Resistance Temperature Detectors).
2. Light Sensor: A light sensor is a device that measures the intensity of light. They are used in a wide range of applications such as cameras, smartphones, and industrial automation. Examples of light sensors include photodiodes, phototransistors, and CCD (charge-coupled device) sensors.
3. Proximity Sensor: A proximity sensor is a device that detects the presence of an object without physical contact. They are used in a wide range of applications such as smartphones, industrial automation, and automobiles. Examples of proximity sensors include infrared sensors, ultrasound sensors, and capacitive sensors.
4. Accelerometer: An accelerometer is a device that measures the acceleration and tilt of an object. They are used in a wide range of applications such as smartphones, automobiles, and industrial automation. Examples of accelerometers include MEMS (microelectromechanical systems) accelerometers and piezoelectric accelerometers.

(c) Write an arduino code for connecting NodeMCU with moisture sensor, servo motor and water pipe lines for automatic watering a plant when moisture level is decreasing. **07**

Here is an example of Arduino code for connecting a NodeMCU board to a moisture sensor, a servo motor, and water pipe lines for automatic watering of a plant when the moisture level is decreasing:

```
#include <Servo.h>

int moistureSensor = A0;
int moistureValue = 0;
int thresholdValue = 700;
Servo myservo;

void setup() {
  myservo.attach(D5);
  Serial.begin(115200);
}

void loop() {
  moistureValue = analogRead(moistureSensor);
  Serial.print("Moisture Value: ");
  Serial.println(moistureValue);

  if (moistureValue < thresholdValue) {
    Serial.println("Watering the plant...");
    myservo.write(90);
    delay(1000);
    myservo.write(0);
  }

  delay(1000);
}
```

In this code, we first include the necessary library Servo.h. Then, we define the pin of the moisture sensor, servo motor and the threshold value of moisture level, below which the plant needs to be watered. In the setup function, we attach the servo to pin D5 and start the serial communication. In the loop function, we use the analogRead function to read the moisture level from the sensor, and the value is stored in the variable moistureValue. We then use the serial.print() function to display the moisture level on the serial monitor.

We then use an if-else statement to check whether the moisture level is less than the threshold value. If it is, the servo motor will rotate to open the water

Q.5(a) Write about LoraWan. **03**

LoRaWAN (Long Range Wide Area Network) is a low-power wide area network (LPWAN) protocol that is designed for IoT applications. It operates in the unlicensed ISM (Industrial, Scientific, and Medical) band and uses a chirp spread spectrum modulation technique to achieve long-range communication.

One of the key features of LoRaWAN is its ability to support a large number of devices while maintaining low power consumption. This makes it well-suited for applications such as smart metering, asset tracking, and environmental monitoring.

The architecture of a LoRaWAN network consists of three main components:

1. End devices: These are the devices that are connected to the network and typically have limited power and processing capabilities. Examples of end devices include sensors, actuators, and other IoT devices.
2. Gateways: These are the devices that bridge the end devices to the network and are responsible for forwarding data between the end devices and the network server.
3. Network server: This is the central point of the network that is responsible for managing the communication between the end devices and gateways.

LoRaWAN uses a star-of-stars topology in which gateways forward data to the network server, which then routes the data to the appropriate end device. This allows for a scalable network that can support a large number of devices.

Security is an important aspect of LoRaWAN, it uses AES-128 encryption to secure the communication between devices and the network, also it uses a secure join process to authenticate devices to the network.

(b) Differentiate ESP8266 and ESP32. **04**

ESP8266	ESP32
CPU: 32-bit L106 RISC microprocessor	CPU: 32-bit LX6 microprocessor
Clock Speed: 80 MHz	Clock Speed: up to 240 MHz
Memory: 32-64 kB RAM	Memory: 520 kB SRAM
Communication: WiFi	Communication: WiFi, Bluetooth
Power Consumption: 80mA	Power Consumption: 150mA
Pin Count: 17	Pin Count: 36
ADC Resolution: 10 bit	ADC Resolution: 12 bit
PWM: 2	PWM: 16
UART: 1	UART: 2
I2C: 1	I2C: 2

- The ESP32 has a more powerful processor and more memory than the ESP8266, which makes it better suited for more complex

projects.
- The ESP32 also has built-in Bluetooth support, which the ESP8266 does not have.
- The ESP32 also has a higher power consumption than the ESP8266, so it may require a larger power supply or a battery with a larger capacity.
- The ESP32 has more number of pins, more number of PWM and UART than ESP8266, which can be useful for projects that require more I/O options.

In summary, the ESP8266 is a good choice for simple projects that only require WiFi connectivity, while the ESP32 is a more powerful option for more complex projects that require WiFi and Bluetooth connectivity, and more number of I/O options.

(c) Write about Encapsulation Protocol 6LowPan. **07**

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) is a communication protocol that enables the transmission of IPv6 packets over low-power wireless networks such as Zigbee, Z-Wave, and other similar technologies. The goal of 6LoWPAN is to enable low-power, low-data-rate devices to communicate using the same Internet Protocol as the rest of the Internet.

The 6LoWPAN protocol encapsulates IPv6 packets into smaller frames that can be transmitted over the low-power wireless network. The 6LoWPAN frames include a header that contains information about the packet, such as the destination address, and a payload that contains the actual IPv6 packet.

The 6LoWPAN protocol also includes several features that are designed to optimize the transmission of IPv6 packets over low-power wireless networks. Some of these features include:

- Header compression: 6LoWPAN uses a header compression mechanism to reduce the size of the IPv6 header, which reduces the amount of data that needs to be transmitted over the wireless network.
- Fragmentation: 6LoWPAN supports fragmentation of IPv6 packets, which allows larger packets to be broken down into smaller fragments that can be transmitted over the wireless network.
- Address management: 6LoWPAN includes mechanisms for managing addresses, such as stateless address autoconfiguration, which allows devices to automatically configure their IPv6 addresses.
- Security: 6LoWPAN includes security mechanisms such as link-layer security and end-to-end security to protect the communication of the devices over the low-power wireless network.

6LoWPAN is widely used in IoT applications and it is supported by many IoT platforms such as Contiki, OpenWSN, and RIOT. It also supports

different link layer technologies such as IEEE 802.15.4, Zigbee, and Z-Wave, which makes it a versatile protocol for different wireless networks.

OR

Q.5 (a) Briefly write about CARP protocol. **03**

CARP (Common Address Redundancy Protocol) is a protocol that is used to implement redundancy in a network. It allows multiple hosts to share a virtual IP address, so that if one host fails, another host can take over the virtual IP address and continue to provide services without interruption.

The CARP protocol works by electing a master host and one or more backup hosts. The master host is responsible for responding to requests for the virtual IP address, while the backup hosts monitor the master host and take over the virtual IP address if the master host fails.

The CARP protocol uses a multicast address to send advertisements that contain the virtual IP address, the host's MAC address, and a priority value. The host with the highest priority value becomes the master host, and the others become backup hosts.

One of the key benefits of CARP is that it allows for automatic failover, which means that the virtual IP address can be quickly and seamlessly transferred to a backup host in the event of a failure. This helps to ensure that services are always available, even in the event of a failure.

CARP is typically used in conjunction with other redundancy protocols such as VRRP (Virtual Router Redundancy Protocol) and HSRP (Hot Standby Router Protocol) to provide redundancy at different layers of the network stack.

(b) Discuss Zigbee. **04**

Zigbee is a communication protocol that is used to connect devices in a low-power, low-data-rate wireless personal area network (WPAN). It is an open standard that is developed and maintained by the Zigbee Alliance, an organization of companies that develop and promote Zigbee technology.

The Zigbee protocol is based on the IEEE 802.15.4 standard, which defines the physical and media access control (MAC) layers of the protocol. Zigbee extends this standard by adding a network layer and application layer that provide additional functionality and services.

One of the key features of Zigbee is its low power consumption, which makes it well-suited for devices that run on batteries or have limited power resources. Zigbee devices can operate for several years on a single

battery, making it a popular choice for IoT applications such as home automation, building automation, and smart metering.

Another important feature of Zigbee is its flexibility, it allows the creation of a mesh network, which means that devices can communicate with each other even if they are not in direct range of a central hub or gateway. This enables devices to communicate over a large area and allows for a scalable network.

Zigbee also provides a wide range of application profiles, which are pre-defined sets of commands and procedures that enable devices to communicate with each other and interact with other devices. Some examples of application profiles include the Zigbee Home Automation profile, the Zigbee Smart Energy profile, and the Zigbee Light Link profile.

In summary, Zigbee is a communication protocol that enables low-power, low-data-rate wireless communication between devices in a personal area network. It is an open standard that is widely used for IoT applications and provides low power consumption, flexibility and a wide range of application profiles.

(c) Discuss MQTT protocol in Detail. **07**

MQTT (Message Queuing Telemetry Transport) is a lightweight publish-subscribe messaging protocol that is designed to be used in low-bandwidth, high-latency, or unreliable networks. It is often used in IoT applications, where devices need to send and receive data in real-time, even in challenging network conditions.

The MQTT protocol is based on a publish-subscribe model, in which clients (devices or applications) connect to a central broker, and publish and subscribe to messages on specific topics. The broker is responsible for routing messages between clients, and for maintaining the state of the network.

One of the key features of MQTT is its low overhead, which makes it well-suited for low-bandwidth, high-latency, or unreliable networks. The protocol uses a binary format for messages, which reduces the amount of data that needs to be transmitted.

MQTT also includes a number of features that are designed to improve reliability and security, such as:

- Quality of Service (QoS) levels: MQTT supports three levels of QoS (0, 1, and 2) which allow clients to control the level of reliability for the messages they send and receive.
- Keep-Alive: MQTT includes a keep-alive mechanism that allows clients to detect when a connection has been lost and re-establish a connection if necessary.
- Clean Session: MQTT supports clean session, which allows clients to start a new session and discard any previous session data.
- Authentication and Encryption: MQTT supports username/password-based authentication, as well as Transport

Layer Security (TLS) encryption to secure the communication between clients and the broker.

MQTT is widely used in IoT applications such as smart home, industrial automation, and transportation. Many IoT platforms such as AWS IoT, Azure IoT, and Google IoT Core, support MQTT as a protocol for communication.

In summary, MQTT is a lightweight publish-subscribe messaging protocol that is designed for low-bandwidth, high-latency, or unreliable networks. It is widely used in IoT applications and provide features such as low overhead, Quality of Service, Keep-Alive, Clean Session, Authentication and Encryption which makes it a reliable and secure protocol for communication.

****

Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – SUMMER 2022

Subject Code:3171108

Date:18/06/20

22 Subject Name: Internet of things

Time: 02:30 PM TO 05:00 PM **Total Marks: 70**

MARKS

Q.1(a) Define Internet of Things and explain it in brief. **03**

The Internet of Things (IoT) refers to the interconnected network of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to collect and exchange data. The IoT allows for the seamless integration and communication between devices, facilitating automation, data collection, and remote control capabilities. This technology is used in a wide range of applications, including smart homes, industrial automation, transportation, and healthcare. The IoT is expected to bring significant improvements in efficiency, accuracy, and cost savings across various industries.

(b) Determine the applications of Internet of Things. **04**

The Internet of Things (IoT) refers to the interconnectedness of physical objects, such as devices and appliances, that are connected to the internet and can communicate with one another. Some common applications of IoT include:

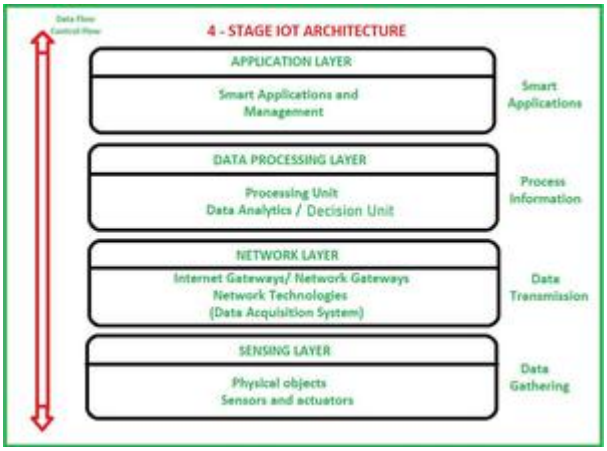
1. Smart home devices, such as thermostats, security systems, and lighting systems, which can be controlled and monitored remotely through a smartphone or computer.
2. Industrial automation, such as in manufacturing and logistics, where IoT devices can be used to optimize processes and improve efficiency.
3. Smart cities, where IoT sensors and devices can be used to monitor and improve various aspects of urban life, such as traffic flow, air quality, and public safety.
4. Health care, where IoT devices and sensors can be used for remote patient monitoring and to improve the efficiency of medical treatments.
5. Agriculture, where IoT-enabled sensors and devices can be used to monitor crop growth and soil conditions, as well as to optimize irrigation and fertilization.
6. Transportation, where IoT devices can be used to optimize traffic flow, improve public transportation and monitor vehicle

maintenance.

7. Retail, where IoT-enabled sensors can be used to track inventory, optimize supply chain, and improve customer experience.
8. Energy management, where IoT-enabled sensors and devices can be used to monitor and optimize energy consumption in buildings and other facilities.

(c) Describe IoT architecture in detail. **07**

IOT technology has a wide variety of applications and use of Internet of Things is growing so faster. Depending upon different application areas of Internet of Things, it works accordingly as per it has been designed/developed. But it has not a standard defined architecture of working which is strictly followed universally. The architecture of IoT depends upon its functionality and implementation in different sectors. Still, there is a basic process flow based on which IoT is built.
So. here in this article we will discuss basic fundamental architecture of IoT i.e., 4 Stage IoT architecture.



4 Stage IoT architecture

So, from the above image it is clear that there is 4 layers are present that can be divided as follows: Sensing Layer, Network Layer, Data processing Layer, and Application Layer.

These are explained as following below.

1. **Sensing Layer –**
   Sensors, actuators, devices are present in this Sensing layer. These Sensors or Actuators accepts data(physical/environmental parameters), processes data and emits data over network.
2. **Network Layer –**
   Internet/Network gateways, Data Acquisition System (DAS) are present in this layer. DAS performs data aggregation and conversion function (Collecting data and aggregating data then converting analog data of sensors to digital data etc). Advanced gateways which mainly opens up connection between Sensor networks

and Internet also performs many basic gateway functionalities like malware protection, and filtering also some times decision making based on inputted data and data management services, etc.

3. **Data processing Layer –**
   This is processing unit of IoT ecosystem. Here data is analyzed and pre-processed before sending it to data center from where data is accessed by software applications often termed as business applications where data is monitored and managed and further actions are also prepared. So here Edge IT or edge analytics comes into picture.
4. **Application Layer –**
   This is last layer of 4 stages of IoT architecture. Data centers or cloud is management stage of data where data is managed and is used by end-user applications like agriculture, health care, aerospace, farming, defense, etc.

OR

IoT architecture refers to the overall structure and components of an IoT system. The architecture typically includes several layers, each with different functions and components. The main layers of an IoT architecture are:

1. Device Layer: This is the bottom layer of the IoT architecture, and it includes the physical devices and sensors that collect data. These devices may include things like temperature sensors, cameras, and RFID readers.
2. Connectivity Layer: This layer is responsible for connecting the devices to the internet and to other devices. This includes communication protocols such as Zigbee, Z-Wave, and Bluetooth, as well as cellular networks and Wi-Fi.
3. Edge Layer: This layer sits between the device and connectivity layers, and it is responsible for processing the data collected by the devices. The edge layer may include devices such as gateways and edge servers, which are capable of performing tasks such as data filtering, aggregation, and pre-processing.
4. Cloud/Platform Layer: This layer is responsible for managing and storing the data collected by the devices, and for providing access to the data to other systems and applications. This layer may include cloud servers, databases, and analytics tools.
5. Application Layer: This is the top layer of the IoT architecture, and it includes the applications and services that use the data collected by the devices. These applications may include things like dashboards, mobile apps, and automated systems.
6. Security Layer: This layer is responsible for providing security to the IoT systems, which includes the devices, the connectivity, the

data, the platforms, and the applications. This layer includes security protocols, firewalls, intrusion detection, and encryption.

In summary, the IoT architecture is composed of multiple layers that work together to connect devices, collect and process data, and provide access to the data to other systems and applications. Each layer has its own set of functions and components, and the overall architecture is designed to be scalable and flexible to support a wide range of IoT applications.

Q.2(a) Discuss the IoT Sensors. **03**

IoT sensors are devices that collect data from the environment and transmit it to other devices for processing and analysis. They play a crucial role in the Internet of Things (IoT) by enabling the connection of physical objects to the internet. Some common types of IoT sensors include:

1. Temperature sensors: These sensors measure temperature and can be used in applications such as HVAC systems, refrigeration, and weather monitoring.
2. Humidity sensors: These sensors measure the humidity or moisture content in the air and can be used in applications such as agriculture, weather monitoring, and indoor air quality.
3. Light sensors: These sensors measure the intensity and color of light and can be used in applications such as lighting control, security systems, and photography.
4. Pressure sensors: These sensors measure pressure and can be used in applications such as industrial automation, weather monitoring, and medical devices.
5. Accelerometer sensors: These sensors measure acceleration and can be used in applications such as fitness trackers, gaming controllers, and vehicle navigation.
6. Proximity sensors: These sensors detect the presence of objects and can be used in applications such as security systems, touchless controls, and robotics.
7. Ultrasonic sensors: These sensors measure distance and can be used in applications such as obstacle detection, navigation, and industrial automation.
8. Infrared sensors: These sensors detect infrared radiation and can be used in applications such as temperature measurement, motion detection, and night vision.
9. Magnetic sensors: These sensors detect changes in the magnetic field and can be used in applications such as navigation, industrial automation, and security.

IoT sensors can be connected to the internet through various communication protocols such as Zigbee, Z-Wave, Bluetooth, and Wi-Fi, which enables the data they collect to be transmitted to other devices for further processing, storage, and analysis. They are also commonly

connected to an edge device or gateway that can pre-process the data to help reduce the amount of data that needs to be transmitted to the cloud or other remote servers.

(b) Describe the characteristics of IoT. **04**

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 pf a changing context, to best answer a set of requirements.
7. Self-configuration primarily consists of the actions of neighbor and service discovery, network organization, and resource provisioning.

(c) Explain Smart Home Automation in detail. **07**

Smart home automation refers to the use of internet-connected devices and sensors to control and automate various functions in a home. These devices can be controlled remotely through a smartphone or other device, and can be programmed to perform tasks automatically based on certain conditions or schedules.

Some common examples of smart home automation include:

1. Smart thermostats: These devices can be controlled remotely to adjust the temperature in a home, and can also be programmed to automatically adjust the temperature based on factors such as time of day and occupancy.
2. Smart lighting: These devices can be controlled remotely to turn lights on and off, and can also be programmed to automatically turn lights on and off based on factors such as time of day and occupancy.
3. Smart security systems: These systems can include cameras, motion sensors, and door locks that can be controlled remotely and can alert homeowners of any unusual activity.
4. Smart appliances: These devices, such as refrigerators, ovens, and washing machines, can be controlled remotely and can also be programmed to perform certain tasks automatically.
5. Smart entertainment systems: These systems can include smart TVs, speakers, and streaming devices that can be controlled remotely and can also be programmed to automatically play

certain content.

Smart home automation systems can also be integrated with other systems such as voice assistants (such as Amazon Alexa, Google Home) and home hubs (such as Samsung SmartThings, Apple HomeKit) to provide a more seamless and convenient experience for the user.

Smart home automation can provide several benefits to homeowners, such as increased energy efficiency, improved security, and increased convenience. Additionally, it can also offer the ability to monitor, control and troubleshoot problems remotely, saving time and effort. However, it is important to note that with the increasing number of connected devices in the home, the security of these devices and the data they collect is becoming an important concern.

OR

(c) Explain how Smart City and IoT are associated with each other? **07**

Smart cities and the Internet of Things (IoT) are closely associated with each other as they both aim to improve the efficiency, sustainability, and livability of urban environments.

Smart cities use a wide range of technologies, including IoT, to collect and analyze data from various sources such as sensors, cameras, and other devices. This data is then used to optimize and automate various city services and infrastructure, such as transportation, energy management, and public safety.

IoT devices and sensors are a key component of smart city initiatives, as they provide the ability to collect real-time data from the environment. This data can be used to monitor and improve various aspects of urban life, such as traffic flow, air quality, and public safety.

For example, smart traffic management systems can use IoT sensors to monitor traffic flow and adjust traffic signals in real-time to reduce congestion. Smart lighting systems can use IoT sensors to adjust the brightness of streetlights based on the level of ambient light and the presence of pedestrians and vehicles. Smart waste management systems can use IoT sensors to track the level of waste in trash cans and schedule pickups as needed.

IoT devices can also be used to improve public safety by providing real-time monitoring of city streets and public spaces, as well as by providing emergency responders with real-time data and location information during emergency situations.

Moreover, IoT can also be used to improve energy efficiency in smart cities by monitoring and controlling energy consumption in buildings and other infrastructure.

In summary, smart cities and IoT are closely associated with each other as they both aim to improve the efficiency, sustainability, and livability of urban environments. IoT devices and sensors play a crucial role in smart city initiatives by providing the ability to collect real-time data from the environment and use this data to optimize and automate various city services and infrastructure.

Q.3 (a) Write applications of Internet of Things for Medical field. **03**

The Internet of Things (IoT) has the potential to revolutionize the medical field by providing new ways to collect and analyze data, monitor and treat patients, and improve the overall efficiency of healthcare systems. Some common applications of IoT in the medical field include:

1. Remote patient monitoring
2. Medical imaging
3. Medication management
4. Clinical trials
5. Electronic Health Records (EHRs)
6. Telemedicine
7. Medical equipment monitoring and control
8. Assistive devices enhancement
9. Supply Chain Management
10. Remote surgery
11. Patient's Data and Medical Records Management.

Discuss in brief

1. Remote patient monitoring: IoT devices such as wearables and sensors can be used to collect data from patients, such as their vital signs, and transmit this data to healthcare providers in real-time, allowing for remote monitoring of patients' health.
2. Medical imaging: IoT devices can be used to collect and transmit medical images, such as X-rays and MRI scans, to healthcare providers for remote analysis.
3. Medication management: IoT devices can be used to track and manage patients' medication schedules, ensuring they take their medication on time and in the correct dosage.
4. Clinical trials: IoT devices can be used to collect data from patients participating in clinical trials, allowing for more accurate and efficient tracking of their health.
5. Electronic Health Records (EHRs): IoT devices can be used to collect and transmit patient data to EHR systems, allowing for more accurate and efficient tracking of patients' health.
6. Telemedicine: IoT devices can be used to connect patients with healthcare providers remotely, allowing for remote consultations, diagnosis, and treatment.
7. Medical equipment: IoT devices can be used to monitor and control medical equipment, such as ventilators and infusion pumps, allowing for remote monitoring and control of the equipment.
8. Assistive devices: IoT devices can be used to enhance the capabilities of assistive devices, such as prosthetic limbs, allowing

for more natural and intuitive control of the devices.
9. Supply Chain Management: IoT devices can be used to track medical equipment and supplies, allowing for more efficient and accurate tracking of inventory levels.

Overall, IoT has the potential to greatly improve the efficiency, effectiveness and accessibility of healthcare, allowing for better patient outcomes and reduced costs.

(b) Discuss vulnerabilities of Internet of Things. **04**

The Internet of Things (IoT) refers to the interconnectedness of physical objects, such as devices and appliances, that are connected to the internet and can communicate with one another. While IoT has many benefits, it also poses several vulnerabilities. Some common vulnerabilities of IoT include:

1. Insecure devices: Many IoT devices are not designed with security in mind, and may have weak or easily guessable passwords, lack of encryption, or other vulnerabilities that make them easy to hack.
2. Lack of software updates: Many IoT devices may not receive regular software updates, leaving them vulnerable to known security vulnerabilities that have not been patched.
3. Insufficient network security: IoT devices may be connected to networks that are not properly secured, leaving them vulnerable to cyberattacks.
4. Lack of device management: Many IoT devices may not have proper management systems in place, making it difficult to detect or respond to security incidents.
5. Lack of user education: Many users may not be aware of the security risks associated with IoT devices, and may not take proper steps to secure them.
6. Interconnectedness: As IoT devices are connected to each other, a vulnerability in one device can spread to others, creating a chain reaction of vulnerabilities.
7. Weak Authentication: many IoT devices rely on weak or default credentials, making it easy for attackers to gain unauthorized access.
8. Unsecured communication: IoT devices often communicate using unencrypted protocols, making it easy for attackers to intercept and manipulate the communication.
9. Insecure Cloud Interface: Many IoT devices rely on cloud-based services, which can be vulnerable to attacks if the cloud infrastructure is not properly secured.
10. Lack of regulation: IoT security is still a relatively new field, and there are currently few regulations in place to ensure that IoT devices are secure.

It's important to note that these vulnerabilities can lead to serious consequences, such as data breaches, loss of personal information, unauthorized access to devices and even physical harm. Therefore, it is crucial for IoT device manufacturers, network providers, and users to be aware of these vulnerabilities and take steps to mitigate them.

(c) Describe Internet of Things protocols in detail. **07**

The Internet of Things (IoT) relies on a variety of communication protocols to connect devices and transmit data. These protocols are used to govern the communication between IoT devices, and between IoT devices and other systems. Here are some common IoT protocols:

1. Transmission Control Protocol (TCP): This is a core protocol of the internet, and it is used to establish a reliable connection between devices and ensure that data is transmitted correctly.
2. User Datagram Protocol (UDP): This is a simpler protocol than TCP, and it is used for faster, low-latency communication between devices.
3. MQTT (Message Queuing Telemetry Transport): This is a lightweight protocol designed for low-power devices and networks with limited bandwidth. It is commonly used in IoT applications such as remote monitoring and control.
4. CoAP (Constrained Application Protocol): This is a web transfer protocol designed specifically for use with constrained devices and networks. It is similar to HTTP, but it is designed to be more lightweight and efficient.
5. Zigbee: This is a low-power, low-data-rate wireless protocol that is commonly used in IoT applications such as home automation and industrial control.
6. Z-Wave: This is another low-power, low-data-rate wireless protocol that is commonly used in home automation and other IoT applications.
7. Bluetooth: This is a wireless protocol that is commonly used in IoT applications such as wearables and smart home devices.
8. LoRa (Long Range): This is a low-power, wide-area network protocol that is designed for long-range communication and is commonly used in IoT applications such as remote monitoring and control.
9. 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks): This protocol is used to enable IPv6 communications over low-power wireless networks, such as Zigbee and Z-Wave.
10. Sigfox: This is a low-power, wide-area network protocol that is designed for low-bandwidth communication and is commonly used in IoT applications such as remote monitoring and control.

OR

Q.3(a) Write applications of Internet of Things for Smart Parking in Smart City. **03**

Smart parking is an application of the Internet of Things (IoT) that utilizes various technologies to optimize the use of parking spaces in a smart city. Here are some common applications of IoT for smart parking:

1. Real-time parking availability
2. Dynamic pricing
3. Smart parking meters
4. License plate recognition
5. Parking guidance systems
6. Reservation systems
7. Smart parking management
8. Predictive parking analytics
9. Smart parking enforcement
10. Electric Vehicle Charging Management
11. Occupancy-based Lighting Control
12. Integrated Transportation Systems.

Discuss in brief

1. Real-time parking availability: IoT sensors can be installed in parking garages and on-street parking spaces to detect the presence of vehicles, and transmit this information to a central system in real-time. This allows drivers to easily find available parking spaces and avoid wasting time searching for a spot.
2. Dynamic pricing: IoT sensors can be used to track the occupancy of parking spaces, and to adjust pricing in real-time based on demand. This can help to ensure that parking spaces are always available, and can also generate additional revenue for the city.
3. Smart parking meters: IoT-enabled parking meters can be used to accept payments from a variety of sources, such as credit cards and mobile payments, and can also be used to track occupancy and adjust pricing in real-time.
4. License plate recognition: IoT-enabled cameras can be used to automatically detect and recognize license plates, and to track the arrival and departure of vehicles in parking garages and on-street parking spaces.
5. Parking guidance systems: IoT-enabled parking guidance systems can be used to guide drivers to available parking spaces, and to provide real-time information about parking availability.
6. Reservation systems: IoT-enabled systems can be used to allow drivers to reserve parking spaces in advance, and to pay for parking online, reducing the need to carry cash or credit cards.

(b) Describe Constrained application protocol. **04**

Constrained Application Protocol (CoAP) is a web transfer protocol designed specifically for use with constrained devices and networks in the Internet of Things (IoT). It is similar to HTTP, but it is designed to be

more lightweight and efficient, making it well suited for use with devices that have limited resources such as memory, processing power, and bandwidth.

CoAP uses a request/response model, similar to HTTP, but it uses a smaller message format and a simpler message header. This allows it to be used with devices that have limited resources or low-power networks. CoAP also supports multicast communication and can be used to discover resources in a local network.

CoAP uses the User Datagram Protocol (UDP) as its transport protocol, which provides a simpler and less overhead compared to Transmission Control Protocol (TCP) that HTTP uses. This makes it more suitable for use in low-power, lossy networks where the overhead of TCP may be too high.

CoAP also supports a variety of security mechanisms, such as DTLS (Datagram Transport Layer Security) which is similar to SSL and TLS, which is used to encrypt and authenticate messages.

CoAP is widely used in IoT applications such as building automation, smart cities, industrial control, and home automation. It is also supported by many IoT platforms and can be easily integrated with other protocols such as MQTT and HTTP

(c) Explain access control and message integrity of Internet of Things in detail. **07**

Access control and message integrity are important security features of the Internet of Things (IoT) that are used to protect devices and data from unauthorized access and tampering.

Access control refers to the mechanisms that are used to control who or what is allowed to access a device or system. This can include authentication methods such as passwords, PINs, and biometrics, as well as authorization methods such as access control lists (ACLs) that define which users or systems are allowed to access specific resources.

One of the most common access control mechanisms in IoT is the use of digital certificates and public key infrastructure (PKI) which is based on the use of a pair of public and private keys. The public key is used to encrypt the data and the private key is used to decrypt the data, this way only the devices that have the private key can decrypt the data sent by the device that has the public key.

Message integrity, on the other hand, refers to the mechanisms that are used to ensure that the data transmitted between devices and systems has not been tampered with. This can include the use of digital signatures, message authentication codes (MACs), and hash functions.

In addition, it's possible to use encryption mechanisms such as Advanced

Encryption Standard (AES) to encrypt the data before it's transmitted, this way even if the data is intercepted by an attacker, it will not be able to read the data.

Both access control and message integrity are important for ensuring the security of IoT devices and systems, as they help to prevent unauthorized access and tampering of data. It's essential to implement these security measures at the device and network level to ensure the integrity and confidentiality of the data transmitted between devices.

Q.4(a) Discuss IoT Levels in details. **03**

IoT (Internet of Things) can be broadly classified into six levels, these levels are:

1. Device Level: This is the most basic level of IoT, where individual devices or "things" are connected to the internet. These devices are equipped with sensors and/or actuators that allow them to collect and transmit data, and respond to commands. Examples of device-level IoT devices include smart thermostats, smart light bulbs, and wearable fitness trackers.
2. Network Level: This level of IoT involves connecting multiple devices together and allowing them to communicate and share data with one another. This can be done using various communication protocols such as Zigbee, Z-Wave, and Bluetooth Low Energy (BLE). In addition to device-to-device communication, this level also involves communication between devices and gateways or hubs that allow them to connect to the internet.
3. Cloud/Application Level: This is the highest level of IoT and involves connecting devices to the cloud, where data is analyzed and stored, and applications are built on top of this data. This level also includes the development of software platforms and APIs that allow different devices and systems to interact with one another. This level enables remote monitoring, control, and automation of devices and systems.
4. Data Management Level: This level of IoT refers to the collection, storage, and management of data generated by IoT devices. This includes the use of data management platforms and databases to store and analyze data, as well as the development of data pipelines to process and transmit data.
5. Analytics Level: This level of IoT involves the use of advanced analytics techniques to extract insights and knowledge from IoT data. This includes the use of machine learning, statistical analysis, and data visualization to gain a deeper understanding of IoT data and to make informed decisions.
6. User Interface Level: This level of IoT refers to the development of user interfaces and applications that allow users to interact with and control IoT devices. This includes the use of mobile apps, web interfaces, and voice-controlled assistants to control and monitor IoT devices.

It is worth noting that these levels are not mutually exclusive and often overlap with each other. Many IoT systems involve multiple levels working together to provide a seamless and integrated experience for users.

(b) Describe Transport layer protocol. **04**

The Transport layer is the fourth layer of the OSI model, and its main function is to provide end-to-end communication between devices on a network. The Transport layer is responsible for providing reliable data transfer and error checking. It is responsible for breaking large data packets into smaller segments, and reassembling them at the receiving end.

One of the most widely used transport layer protocols is the Transmission Control Protocol (TCP). TCP is a connection-oriented protocol, which means that it establishes a reliable connection between two devices before data is transferred. This is done using a three-way handshake, where the devices first exchange messages to establish a connection, and then exchange messages to confirm the connection before data transfer begins.

TCP is responsible for ensuring that data is delivered in the correct order, and retransmitting any data that is lost or corrupted during transmission. It also provides flow control, which means it regulates the amount of data that is sent at one time, to prevent the sender from overwhelming the receiver.

Another transport layer protocol is the User Datagram Protocol (UDP), which is connectionless and does not establish a connection before data is transferred. It is typically used for real-time applications such as streaming media and online games where low latency is more important than reliability.

In summary, the Transport layer protocol is responsible for providing a reliable and efficient means of data transfer between devices on a network, and it plays a crucial role in ensuring that data is delivered accurately and in the correct order.

(c) Describe Gas Sensors in brief. **07**

Gas sensors are devices that detect and measure the concentration of gases in the air. They work by using a chemical reaction to detect the presence of a specific gas, and then outputting an electrical signal that corresponds to the concentration of that gas. Gas sensors can be used in a variety of applications, such as industrial monitoring, environmental monitoring, and safety systems.

There are different types of gas sensors available, each of which is

designed to detect a specific gas or group of gases. Some common types of gas sensors include:

- Electrochemical sensors: These sensors use an electrochemical reaction to detect gases, and are commonly used to detect gases such as carbon monoxide and hydrogen.
- Metal oxide semiconductor (MOS) sensors: These sensors use a metal oxide film to detect gases, and are commonly used to detect gases such as carbon monoxide, methane, and propane.
- Infrared (IR) sensors: These sensors use infrared absorption to detect gases, and are commonly used to detect gases such as carbon dioxide and methane.
- Catalytic sensors: These sensors use a catalytic reaction to detect gases, and are commonly used to detect gases such as propane and methane.

Gas sensors are highly sensitive and precise, and are designed to detect gases even at very low concentrations. They are also relatively small, making them easy to integrate into a wide range of systems and applications.

In summary, Gas sensors are devices that can detect and measure the concentration of gases in the air, they are widely used in various applications such as industrial monitoring, environmental monitoring and safety systems, There are different types of gas sensors available, each of which is designed to detect a specific gas or group of gases.

OR

Q.4(a) Write short note on Network layer protocols. **03**

The Network layer is the third layer of the OSI model, and its main function is to provide logical addressing and routing of data packets between devices on a network. Two of the most widely used network layer protocols are the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP).

The Internet Protocol (IP) is a connectionless protocol that provides logical addressing and routing of data packets. It assigns a unique IP address to each device on a network, which is used to identify the source and destination of each packet. IP also provides routing functionality, which means it determines the best path for data packets to travel from the source to the destination.

The Internet Control Message Protocol (ICMP) is a connectionless protocol that is used to send error messages and operational information about network conditions. ICMP message can be generated by network devices, such as routers, to indicate error conditions, such as network congestion or a broken link. ICMP also includes Echo Request and Echo Reply (ping) messages, which are used to test the reachability

of a device on a network.

(b) Describe IoT Gateway in brief. **04**

An IoT gateway is a device that acts as an intermediary between IoT devices and the cloud or a local network. It is responsible for collecting, analyzing, and forwarding data from IoT devices, as well as for providing local control and management of these devices.

IoT gateways typically have a variety of communication interfaces, such as Wi-Fi, Bluetooth, Zigbee, and Z-Wave, which allow them to connect to a wide range of IoT devices. They also have processors, storage, and memory to perform data processing, storage and forwarding.

The main functions of an IoT gateway include:

- Data collection: IoT gateways collect data from IoT devices, and process it before forwarding it to the cloud or a local network.
- Data analysis: IoT gateways can perform local data analysis to extract insights, or to perform tasks such as data compression, encryption and filtering
- Device management: IoT gateways can be used to remotely configure, control, and manage IoT devices.
- Security: IoT gateways can provide security features such as encryption, authentication, and access control to protect against unauthorized access to IoT devices and data.

IoT gateways can be used in a wide range of applications, such as industrial automation, smart homes, and smart cities. They are particularly useful in situations where a direct connection to the cloud is not possible or practical, such as in remote or low-power environments.

In summary, IoT Gateway is a device that acts as an intermediary between IoT devices and the cloud or a local network, it is responsible for collecting, analyzing, and forwarding data from IoT devices, as well as for providing local control and management of these devices. IoT gateways typically have a variety of communication interfaces, and can be used in a wide range of applications, such as industrial automation, smart homes, and smart cities. They provide important functions such as data collection, data analysis, device management and security.

Describe how does a sensor data travel from one device to the Cloud?
Sensor data travels from one device to the cloud through a series of steps that involve the device, the network, and the cloud.

1. The sensor data is generated by the device, which may include various types of sensors such as temperature, humidity, or motion sensors.
2. The device then uses a communication protocol, such as Zigbee, Z-Wave, or Bluetooth Low Energy (BLE), to transmit the data to a

local gateway or hub.
3. The local gateway or hub is responsible for connecting the device to the internet and acts as an intermediary between the device and the cloud. It may perform tasks such as data filtering, compression, encryption and analysis

(c) Describe how does a sensor data travel from one device to the Cloud? **07**

Sensor data travels from one device to the cloud through a series of steps that involve the device, the network, and the cloud.

1. The sensor data is generated by the device, which may include various types of sensors such as temperature, humidity, or motion sensors.
2. The device then uses a communication protocol, such as Zigbee, Z-Wave, or Bluetooth Low Energy (BLE), to transmit the data to a local gateway or hub.
3. The local gateway or hub is responsible for connecting the device to the internet and acts as an intermediary between the device and the cloud. It may perform tasks such as data filtering, compression, encryption and analysis.
4. The gateway then sends the sensor data to the cloud using a communication protocol such as MQTT, HTTP, or CoAP.
5. Once the data reaches the cloud, it is stored in a cloud-based database or data lake. This data can then be analyzed and processed by various cloud-based services, such as machine learning and big data analytics platforms.
6. The processed data can be then exposed to end-users or other applications through an API (Application Programming Interface)
7. The end-users or other applications can use the data for various purposes, such as monitoring, control, and automation.

It is worth noting that this process can vary depending on the specific implementation and the type of sensor data being transmitted. For example, in some cases, the data may be sent directly from the device to the cloud without going through a local gateway. Additionally, some systems may include additional layers of security to ensure that the data is protected as it travels from the device to the cloud.

Q.5(a) Write short note on Message Queue Telemetry Transport protocol. **03**

Message Queue Telemetry Transport (MQTT) is a publish-subscribe based messaging protocol that is designed for use in IoT and machine-to-machine (M2M) communication. It is a lightweight protocol that uses a small code footprint and low network bandwidth, making it well suited for use in resource-constrained environments such as IoT devices.

MQTT uses a publish-subscribe model, where devices can publish data to a specific topic, and other devices can subscribe to that topic to receive

the data. This allows for efficient communication between devices, as each device only receives the data that it is interested in.

MQTT also includes features such as Quality of Service (QoS) levels, which allow for different levels of reliability and guarantee of delivery of messages. Additionally, it includes a keep-alive mechanism that allows clients to detect when a connection has been lost, and to automatically reconnect if necessary.

MQTT is widely used in IoT systems and is supported by many IoT platforms, such as AWS IoT and Azure IoT. It is also supported by many programming languages and libraries, making it easy to implement in a wide range of devices and systems.

(b) Determine the challenges in IoT Security. **04**

IoT security is a complex and multifaceted issue that encompasses a wide range of challenges. Some of the main challenges in IoT security include:

1. Device Security: IoT devices are often resource-constrained and have limited processing power and memory, making it difficult to secure them against attacks. Additionally, many IoT devices use proprietary operating systems and protocols, which can make it difficult to apply standard security measures.
2. Network Security: IoT devices often rely on wireless communication, which can be vulnerable to a variety of attacks such as man-in-the-middle attacks, and denial-of-service attacks.
3. Data Security: IoT devices generate large amounts of data, which can be vulnerable to breaches and attacks if it is not properly protected. This data can include sensitive information such as personal information, financial data, and medical records.
4. Cloud Security: IoT devices often rely on cloud-based services to store and process data, making them vulnerable to attacks on the cloud infrastructure. Additionally, cloud-based services can also be vulnerable to data breaches and data loss.
5. Interoperability: IoT devices and systems often use different communication protocols and standards, making it difficult to ensure security across different devices and systems.
6. Update and patch management: Many IoT devices are not easily updated or patched, making it difficult to address security vulnerabilities and apply software updates.
7. Insufficient regulations and standards: There are currently few regulations and standards for IoT security, which makes it difficult to ensure that devices are secure.
8. Human factor: IoT systems often rely on user interactions and decisions, which can introduce security risks if users are not properly educated about security best practices.

(c) Describe recent developments and future aspects of IoT in brief. **07**

Recent developments in IoT include the following:

1. Edge Computing: With the increasing amount of data generated by IoT devices, edge computing has emerged as a way to process and analyze data closer to the source. Edge computing involves the use of small, low-power devices that can perform data processing and analysis at the edge of the network, rather than in a centralized data center.
2. 5G: The deployment of 5G networks is expected to greatly increase the capabilities of IoT devices, by providing faster speeds, lower latency and more reliable connections. 5G networks will support a large number of connected devices, and will enable new IoT applications such as autonomous vehicles and industrial automation.
3. Artificial Intelligence: Artificial intelligence (AI) is being increasingly used in IoT to extract insights and knowledge from the large amount of data generated by IoT devices. AI is being used for tasks such as predictive maintenance, anomaly detection, and pattern recognition.
4. Smart Cities: IoT is playing an increasing role in the development of smart cities, which use IoT and other technologies to improve the quality of life for citizens, by providing services such as smart lighting, traffic management, and waste management.
5. Blockchain: Blockchain is being used in IoT to provide secure, decentralized systems for data storage and management. This can provide a high level of security and transparency in IoT systems and applications.

In the future, IoT is expected to become more integrated into our daily lives, and to have a significant impact on a wide range of industries. IoT is expected to play a key role in the development of autonomous vehicles, smart cities, and Industry 4.0. Additionally, IoT is also expected to be a key enabler for the development of new business models, such as the Internet of Services, which will provide new ways for organizations to create value for customers.

OR

Q.5(a) Describe Security components in IoT Security. **03**

IoT security is a complex issue that involves a wide range of security components, each of which plays a critical role in protecting IoT systems and devices from attacks. Some of the main security components in IoT security include:

1. Device Authentication: This component is used to ensure that only authorized devices are able to connect to a network or a cloud service. This can be achieved through the use of authentication methods such as password-based authentication, digital

certificates, and biometric authentication.
2. Data Encryption: This component is used to protect data as it is transmitted between devices and the cloud, or between devices on a local network. Encryption can be used to protect data from eavesdropping, tampering, and other types of attacks.
3. Access Control: This component is used to ensure that only authorized users and devices are able to access specific resources and perform specific actions. This can be achieved through the use of mechanisms such as role-based access control, and attribute-based access control.
4. Firewall: This component is used to protect IoT devices and networks from unauthorized access and attacks. Firewalls can be used to filter incoming and outgoing network traffic, and to block malicious traffic.
5. Intrusion Detection and Prevention: This component is used to detect and prevent unauthorized access to IoT devices and networks. Intrusion detection and prevention systems can be used to detect and prevent a wide range of attacks, including denial-of-service attacks, man-in-the-middle attacks, and malware infections.
6. Software updates and patch management: This component is used to ensure that IoT devices and systems are up to date with the latest security patches and updates. This can be achieved through the use of automated software update mechanisms, and through the use of security best practices such as vulnerability management.
7. Incident response and management: This component is used to detect, respond and mitigate security incidents in the IoT systems. This can be achieved through the use of incident response plans, incident response teams and incident response toolkits.

(b) Define the roles of IoT in Health Care Monitoring. **04**

IoT in healthcare monitoring plays a significant role in improving patient care and outcomes, by providing real-time monitoring of patients' vital signs, managing chronic diseases, and enabling remote care. Here are some examples of the roles of IoT in healthcare monitoring:

1. Remote monitoring: IoT devices such as wearables and smart devices can collect and transmit real-time data on patients' vital signs, such as heart rate, blood pressure, and oxygen levels, to healthcare providers. This allows for remote monitoring of patients' health conditions, and enables healthcare providers to intervene quickly if there are any signs of deterioration.
2. Managing chronic diseases: IoT devices can be used to monitor and manage chronic diseases such as diabetes, heart disease, and respiratory conditions. Wearable devices can track glucose levels, blood pressure, and other vital signs, and send alerts to healthcare providers if there are any signs of a problem.
3. Medication management: IoT devices can be used to remind patients to take their medication and to track their adherence to

their medication regimen. This can help to improve patient outcomes and reduce the risk of complications.

4. Telemedicine: IoT technology can enable remote consultations between patients and healthcare providers, through video conferencing and other forms of telecommunication. This can make healthcare more accessible, especially for patients in remote or underserved areas.
5. Medical devices integration: IoT technology can be used to integrate medical devices, such as diagnostic equipment, into healthcare systems. This can improve the efficiency and accuracy of diagnostic procedures, and enable healthcare providers to make more informed decisions.
6. Predictive analytics: IoT devices can be used to gather large amounts of data on patients' health conditions, which can then be analyzed to identify patterns.

(c) Explain Commercial IoT with an example. **07**

Commercial IoT refers to the use of IoT technology in commercial settings, such as businesses, organizations, and industries. The commercial IoT can be used to improve the efficiency and effectiveness of business operations, and to create new revenue streams.

One example of commercial IoT is the use of IoT sensors and devices in the manufacturing industry. These sensors can be used to monitor the performance of equipment, and to collect data on production processes. The data can then be analyzed to identify inefficiencies and to optimize production processes, leading to increased productivity and reduced costs.

For example, a manufacturing company that produces automotive parts, can use IoT sensors to track the condition of their machines, the temperature of the manufacturing environment, and the status of their inventory. By monitoring these factors in real-time, they can make adjustments to their production line to improve efficiency and reduce downtime. Additionally, they can predict when equipment is likely to need maintenance, and schedule it accordingly, reducing the risk of unexpected downtime.

Another example of commercial IoT is the use of IoT technology in retail industry. Smart shelves equipped with IoT sensors can detect when products are running low, and automatically reorder them. This can help retailers to maintain optimal inventory levels and reduce the risk of stockouts. Additionally, IoT technology can be used to track customers in-store, allowing retailers to gain insights into consumer behavior, and optimize the store layout accordingly.

In summary, Commercial IoT is the use of IoT technology in commercial settings, such as businesses, organizations, and industries. It can be used to improve the efficiency and effectiveness of business operations and to create new revenue streams. Examples include the use of IoT sensors and

devices in the manufacturing industry to optimize production processes and reduce costs, and the use of IoT technology in retail industry to optimize inventory and gain insights into consumer behavior.

****