50 IOT questions all chapter

Computer science (Berhampur University)

Certainly! Here are 50 tough multiple-choice questions (MCQs) related to IoT (Internet of Things) along with their answers and explanations. These questions are designed based on the NIELIT O LEVEL syllabus.

1. Which of the following protocols is commonly used for IoT communication?

a) HTTP

b) SMTP

c) UDP

d) MQTT

Answer: d) MQTT

Explanation: MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol designed for efficient communication between IoT devices.

2. Which of the following is an example of a wireless IoT technology?

a) Ethernet

b) Zigbee

c) RS-232

d) CAN

Answer: b) Zigbee

Explanation: Zigbee is a popular wireless IoT technology that operates on low-power, low-data-rate wireless mesh networks.

3. Which of the following is NOT a layer in the IoT protocol stack?

a) Application Layer

b) Sensor Layer

c) Network Layer

d) Data Link Layer

Answer: b) Sensor Layer

Explanation: The IoT protocol stack typically consists of the Application Layer, Network Layer, and Data Link Layer. The Sensor Layer is not a standard layer in the stack.

4. What is the purpose of an IoT gateway?

a) To provide power supply to IoT devices

b) To connect IoT devices to the internet

c) To process and analyze data from IoT devices

d) To secure IoT devices from cyber attacks

Answer: b) To connect IoT devices to the internet

Explanation: An IoT gateway acts as a bridge between IoT devices and the internet, enabling connectivity and communication with remote servers or cloud platforms.

5. Which of the following is a security concern in IoT deployments?

a) Data privacy

b) Network scalability

c) Energy efficiency

d) Device mobility

Answer: a) Data privacy

Explanation: Data privacy is a major security concern in IoT deployments, as the vast amount of collected data requires strong encryption, access controls, and secure storage mechanisms.

6. Which of the following IoT network topologies provides the highest reliability?

a) Star topology

b) Mesh topology

c) Bus topology

d) Ring topology

Answer: b) Mesh topology

Explanation: In a mesh topology, each IoT device is connected to multiple other devices, creating redundant paths for data transmission and ensuring high reliability.

7. Which wireless communication technology is used in NFC (Near Field Communication)?

a) Bluetooth

b) Wi-Fi

c) RFID

d) Z-Wave

Answer: c) RFID

Explanation: NFC utilizes RFID (Radio Frequency Identification) technology for short-range communication between devices, typically within a few centimeters.

8. Which of the following IoT application domains focuses on smart transportation systems?

a) Industrial IoT (IIoT)

b) Healthcare IoT

c) Smart Cities

d) Wearable Devices

Answer: c) Smart Cities

Explanation: Smart Cities involve the integration of various IoT technologies to enhance urban infrastructure, including transportation systems, energy management, and public services.

9. Which IoT security attack involves overwhelming a system with a flood of traffic?

a) Man-in-the-Middle (MitM) attack

b) Denial-of-Service (DoS) attack

c) Spoofing attack

d) Eavesdropping attack

Answer: b) Denial-of-Service (DoS) attack

Explanation: A DoS attack aims to make a system or network unavailable to its intended users by overwhelming it

with excessive traffic, rendering it unresponsive.

10. Which of the following IoT devices has the primary function of tracking and monitoring physical locations?

a) Wearable fitness tracker

b) Smart thermostat

c) Home security camera

d) GPS tracker

Answer: d) GPS tracker

Explanation: GPS trackers are IoT devices specifically designed to track and monitor the physical location of objects or individuals.

11. What is the role of an MQTT broker in an IoT system?

a) It provides power to IoT devices.

b) It analyzes data from IoT devices.

c) It stores and retrieves data from IoT devices.

d) It routes messages between IoT devices.

Answer: d) It routes messages between IoT devices.

Explanation: An MQTT broker is a central server or intermediary that facilitates communication between IoT devices by routing messages between publishers and subscribers.

12. Which IoT communication protocol is based on the REST architectural style?

a) CoAP

b) AMQP

c) LoRaWAN

d) Zigbee

Answer: a) CoAP (Constrained Application Protocol)

Explanation: CoAP is a lightweight application-layer protocol designed for constrained devices and networks, based on the REST architectural style.

13. Which of the following is an example of a fog computing concept in IoT?

a) Storing data on remote servers

b) Performing data analytics on edge devices

c) Routing data through multiple gateways

d) Using blockchain technology for secure transactions

Answer: b) Performing data analytics on edge devices

Explanation: Fog computing refers to performing data processing and analytics at the edge of the network, closer to the IoT devices, rather than relying solely on remote servers.

14. Which IoT component is responsible for managing device identity and access control?

a) Gateway

b) Cloud platform

c) Sensor

d) Edge device

Answer: b) Cloud platform

Explanation: Cloud platforms typically handle device identity management, authentication, and access control to ensure secure interactions between IoT devices and the cloud infrastructure.

15. Which IoT wireless technology operates in the unlicensed 2.4 GHz frequency band?

a) LoRaWAN

b) Zigbee

c) NB-IoT

d) LTE-M

Answer: b) Zigbee

Explanation: Zigbee operates in the 2.4 GHz frequency band, which is unlicensed and widely used for IoT applications.

16. Which of the following IoT protocols is specifically designed for resource-constrained devices?

a) HTTP

b) MQTT-SN

c) AMQP

d) XMPP

Answer: b) MQTT-SN (MQTT for Sensor Networks)

Explanation: MQTT-SN is a variation of MQTT protocol specifically designed for resource-constrained devices with limited processing power, memory, and bandwidth.

17. What is the purpose of a digital twin in IoT applications?

a) To replicate physical devices in a virtual environment

b) To connect devices to the internet

c) To ensure secure communication between devices

d) To store and analyze data from IoT devices

Answer: a) To replicate physical devices in a virtual environment

Explanation: A digital twin is a virtual representation or replica of a physical device or system, enabling monitoring, analysis, and simulation of its behavior and performance.

18. Which of the following IoT devices is used for monitoring environmental conditions?

a) Smart refrigerator

b) Wearable heart rate monitor

c) Smart water meter

d) Air quality sensor

Answer: d) Air quality sensor

Explanation: Air quality sensors are IoT devices designed to

measure and monitor various parameters of air quality, such as pollutants, humidity, and temperature.

19. Which IoT network topology is characterized by a single central node connected to multiple peripheral nodes?

a) Star topology

b) Mesh topology

c) Bus topology

d) Ring topology

Answer: a) Star topology

Explanation: In a star topology, all peripheral IoT devices are connected to a central node or hub, which facilitates communication between the devices.

20. Which of the following IoT standards defines the communication protocol for IPv6-based devices?

a) 6LoWPAN

b) Zigbee

c) Z-Wave

d) Thread

Answer: a) 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)

Explanation: 6LoWPAN is a standard that enables IPv6 communication over low-power wireless networks, often used in IoT deployments.

21. Which IoT communication protocol is based on publish-subscribe messaging pattern?

a) HTTP

b) MQTT

c) TCP

d) DNS

Answer: b) MQTT (Message Queuing Telemetry Transport)

Explanation: MQTT is based on the publish-subscribe messaging pattern, where publishers send messages to a broker, and subscribers receive messages from the broker based on their subscriptions.

22. Which of the following IoT devices uses an accelerometer to measure acceleration?

a) Smart thermostat

b) Fitness tracker

c) Security camera

d) Smoke detector

Answer: b) Fitness tracker

Explanation: Fitness trackers often incorporate accelerometers to measure acceleration, detect movement, and track physical activities.

23. Which IoT connectivity technology has the longest range?

a) Wi-Fi

b) Bluetooth

c) LoRaWAN

d) Zigbee

Answer: c) LoRaWAN (Long Range Wide Area Network)

Explanation: LoRaWAN is a low-power, long-range wireless communication technology designed for IoT applications, offering extended coverage compared to Wi-Fi or Bluetooth.

24. Which of the following IoT deployment models involves direct communication between nearby devices without relying on a centralized infrastructure?

a) Cloud-based IoT

b) Edge computing IoT

c) Peer-to-peer IoT

d) Hybrid IoT

Answer: c) Peer-to-peer IoT

Explanation: Peer-to-peer IoT enables direct communication and data exchange between nearby devices, eliminating the need for a centralized infrastructure or cloud-based intermediaries.

25. Which of the following IoT platforms provides a cloud-based service for collecting, storing, and analyzing IoT data?

a) Arduino

b) Raspberry Pi

c) IBM Watson IoT

d) Microsoft Azure Sphere

Answer: c) IBM Watson IoT

Explanation: IBM Watson IoT platform is a cloud-based service that offers various tools and capabilities for managing and analyzing IoT data.

26. What is the purpose of an API (Application Programming Interface) in IoT?

a) To connect IoT devices to the internet

b) To enable communication between IoT devices

c) To define the interface for accessing and controlling IoT devices

d) To encrypt and secure IoT data transmissions

Answer: c) To define the interface for accessing and controlling IoT devices

Explanation: APIs in IoT provide a standardized interface that enables developers to interact with IoT devices, access their data, and control their functionalities.

27. Which of the following is an example of an IoT application in the healthcare domain?

a) Smart agriculture

b) Industrial automation

c) Remote patient monitoring

d) Smart home automation

Answer: c) Remote patient monitoring

Explanation: Remote patient monitoring involves using IoT

devices to collect health data from patients in real-time, enabling healthcare providers to remotely monitor their condition and provide timely care.

28. Which of the following IoT technologies is specifically designed for low-power, wide-area networks?

a) NFC

b) Bluetooth

c) NB-IoT

d) Wi-Fi

Answer: c) NB-IoT (Narrowband IoT)

Explanation: NB-IoT is a low-power, wide-area wireless technology designed for long-range communication with IoT devices, consuming minimal power and offering extended battery life.

29. What is the primary purpose of MQTT QoS (Quality of Service) levels in IoT communication?

a) To ensure data privacy

b) To reduce network latency

c) To guarantee message delivery

d) To increase network bandwidth

Answer: c) To guarantee message delivery

Explanation: MQTT QoS levels determine the reliability and guarantee of message delivery between MQTT clients, allowing for various levels of acknowledgement and retries.

30. Which IoT device communication model involves direct communication between devices without relying on cloud or internet connectivity?

a) Device-to-Cloud

b) Device-to-Gateway

c) Device-to-Device

d) Device-to-Server

Answer: c) Device-to-Device

Explanation: Device-to-Device communication involves direct communication between IoT devices without the need for intermediate cloud or internet connectivity.

31. Which of the following is a security vulnerability specific to IoT devices?

a) Buffer overflow

b) Cross-site scripting (XSS)

c) SQL injection

d) Denial-of-Service (DoS)

Answer: a) Buffer overflow

Explanation: Buffer overflow is a security vulnerability where a program writes data beyond the boundaries of allocated memory, potentially leading to unauthorized access or system crashes in IoT devices.

32. Which IoT architecture layer is responsible for collecting data from various sensors and devices?

a) Application layer

b) Network layer

c) Perception layer

d) Data link layer

Answer: c) Perception layer

Explanation: The perception layer in IoT architecture is responsible for collecting data from sensors, devices, and actuators, and performing initial processing or filtering before forwarding it to higher layers.

33. Which of the following IoT wireless technologies is designed for short-range communication with ultra-low power consumption?

a) Bluetooth Low Energy (BLE)

b) Wi-Fi

c) Z-Wave

d) LTE-M

Answer: a) Bluetooth Low Energy (BLE)

Explanation: Bluetooth Low Energy (BLE) is a wireless technology designed for short-range communication with ultra-low power consumption, making it suitable for battery-powered IoT devices.

34. What is the primary purpose of edge computing in IoT deployments?

a) To provide high-speed internet connectivity to IoT devices

b) To store and process IoT data on remote servers

c) To reduce latency and improve real-time processing at the network edge

d) To ensure secure communication between IoT devices

Answer: c) To reduce latency and improve real-time processing at the network edge

Explanation: Edge computing brings computational capabilities closer to IoT devices, reducing latency and enabling real-time data processing and decision-making at the network edge, without relying on remote servers.

35. Which IoT data format is commonly used for representing and exchanging structured data?

a) JSON (JavaScript Object Notation)

b) XML (eXtensible Markup Language)

c) CSV (Comma-Separated Values)

d) YAML (YAML Ain't Markup Language)

Answer: a) JSON (JavaScript Object Notation)

Explanation: JSON is a lightweight data interchange format widely used

in IoT applications for representing and exchanging structured data between different systems and devices.

36. Which IoT security measure involves validating the integrity and authenticity of software and firmware updates?

a) Encryption

b) Access control

c) Code signing

d) Intrusion detection

Answer: c) Code signing

Explanation: Code signing is a security measure that involves digitally signing software or firmware updates with a digital certificate, ensuring their integrity and authenticity during installation or execution on IoT devices.

37. Which of the following IoT technologies is typically used for short-range, point-to-point communication between devices?

a) Zigbee

b) LoRaWAN

c) NB-IoT

d) WiMAX

Answer: a) Zigbee

Explanation: Zigbee is a wireless technology specifically designed for short-range, low-power communication between IoT devices, often used in home automation and industrial applications.

38. What is the purpose of a digital certificate in IoT security?

a) To encrypt IoT data transmissions

b) To authenticate IoT devices or users

c) To detect and prevent network intrusions

d) To route messages between IoT devices

Answer: b) To authenticate IoT devices or users

Explanation: A digital certificate is used in IoT security to authenticate the identity of IoT devices or users, ensuring that only trusted entities can access or communicate with the IoT system.

39. Which of the following IoT technologies is commonly used for tracking and managing inventory in supply chain operations?

a) RFID (Radio Frequency Identification)

b) NFC (Near Field Communication)

c) Bluetooth

d) Wi-Fi

Answer: a) RFID (Radio Frequency Identification)

Explanation: RFID technology is widely used in supply chain operations to track and manage inventory, enabling real-time visibility and automated identification of items using radio frequency signals.

40. Which of the following IoT deployment models involves deploying IoT infrastructure within a restricted geographical area?

a) Wide-Area IoT

b) Global IoT

c) Local-Area IoT

d) Hybrid IoT

Answer: c) Local-Area IoT

Explanation: Local-Area IoT deployments focus on deploying IoT infrastructure within a restricted geographical area, such as a building, campus, or city district.

41. Which IoT communication protocol is commonly used for real-time streaming of sensor data?

a) CoAP

b) MQTT

c) HTTP

d) UDP

Answer: d) UDP (User Datagram Protocol)

Explanation: UDP is commonly used for real-time streaming of sensor data in IoT applications, as it provides low-latency communication without the overhead of reliability mechanisms.

42. What is the primary purpose of an IoT data analytics platform?

a) To ensure secure communication between IoT devices

b) To provide real-time visualization of IoT data

c) To store and manage IoT data in a distributed manner

d) To derive insights and patterns from IoT data for decision-making

Answer: d) To derive insights and patterns from IoT data for decision-making

Explanation: IoT data analytics platforms enable organizations to analyze large volumes of IoT data, derive meaningful insights, detect patterns, and make data-driven decisions.

43. Which of the following is an example of an IoT application in the agriculture domain?

a) Smart lighting systems

b) Industrial robotics

c) Precision irrigation systems

d) Virtual reality gaming

Answer: c) Precision irrigation systems

Explanation: Precision irrigation systems utilize IoT technologies to monitor soil moisture, weather conditions, and crop requirements, enabling efficient and targeted water management in agriculture.

44. What is the purpose of a digital watermark in IoT data?

a) To provide real

-time visualization of IoT data

b) To ensure data privacy and confidentiality

c) To authenticate the integrity and origin of IoT data

d) To optimize data transmission and storage efficiency

Answer: c) To authenticate the integrity and origin of IoT data

Explanation: Digital watermarks are used in IoT data to provide an embedded identifier or signature that authenticates the integrity and origin of the data, ensuring its trustworthiness and preventing tampering.

45. Which IoT connectivity technology operates in the licensed cellular spectrum and provides wide coverage?

a) Wi-Fi

b) Zigbee

c) LoRaWAN

d) NB-IoT

Answer: d) NB-IoT (Narrowband IoT)

Explanation: NB-IoT operates in the licensed cellular spectrum and provides wide coverage, making it suitable for IoT deployments requiring long-range communication and extended battery life.

46. What is the primary purpose of IoT data anonymization?

a) To ensure secure communication between IoT devices

b) To reduce the size of IoT data for efficient storage

c) To protect the privacy of individuals in IoT data

d) To optimize data transmission and network bandwidth

Answer: c) To protect the privacy of individuals in IoT data

Explanation: IoT data anonymization techniques are used to remove or obfuscate personally identifiable information from IoT data, ensuring the privacy and confidentiality of individuals involved.

47. Which IoT security measure involves regularly applying software updates and patches to IoT devices?

a) Encryption

b) Access control

c) Intrusion detection

d) Firmware updates

Answer: d) Firmware updates

Explanation: Regularly applying software updates and patches, including firmware updates, is an essential security measure to address vulnerabilities and ensure the latest security enhancements on IoT devices.

48. Which of the following IoT communication protocols is commonly used for device discovery and service announcement?

a) HTTP

b) SSDP (Simple Service Discovery Protocol)

c) CoAP

d) MQTT

Answer: b) SSDP (Simple Service Discovery Protocol)

Explanation: SSDP is commonly used for device discovery and service announcement in IoT applications, allowing devices to advertise their presence and available services on the network.

49. What is the purpose of a digital signature in IoT security?

a) To ensure data privacy during transmission

b) To authenticate the integrity and origin of data

c) To encrypt IoT data transmissions

d) To prevent unauthorized access to IoT devices

Answer: b) To authenticate the integrity and origin of data

Explanation: A digital signature is used in IoT security to provide a cryptographic mechanism for authenticating the integrity and origin of data, ensuring its trustworthiness and preventing tampering.

50. Which of the following IoT connectivity technologies is designed for low-power, short-range communication between devices?

a) LoRaWAN

b) Wi-Fi

c) Zigbee

d) LTE-M

Answer: c) Zigbee

Explanation: Zigbee is a low-power, short-range wireless communication technology designed for IoT applications, particularly in home automation and industrial settings, where power efficiency and reliability are crucial.