1. Which of the following is NOT a commonly used IoT platform?
a) Arduino
b) Raspberry Pi
c) TensorFlow
d) Amazon Web Services (AWS)

Answer: c) TensorFlow

Explanation: TensorFlow is primarily a machine learning framework developed by Google, whereas Arduino and Raspberry Pi are popular hardware platforms used in IoT projects. Amazon Web Services (AWS) offers cloud services that can be utilized in IoT applications.

2. Which IoT platform is known for its simplicity and ease of use, often used for prototyping and educational purposes?
a) Raspberry Pi
b) Arduino
c) ESP8266
d) BeagleBone

Answer: b) Arduino

Explanation: Arduino is well-known for its simplicity and user-friendly environment, making it a popular choice for beginners and educational purposes in IoT projects.

3. What type of storage model is commonly used in IoT applications to store large volumes of data generated by sensors and devices?
a) Relational Database
b) NoSQL Database

c) Object Storage
d) Block Storage

Answer: b) NoSQL Database

Explanation: NoSQL databases are commonly used in IoT applications due to their ability to handle large volumes of unstructured data generated by sensors and devices more efficiently compared to traditional relational databases.

4. Which communication API is commonly used for real-time data exchange in IoT applications?
a) HTTP
b) FTP
c) MQTT
d) SMTP

Answer: c) MQTT

Explanation: MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol commonly used in IoT applications for real-time data exchange between devices and servers due to its low bandwidth and power consumption requirements.

5. What is a common attack vector in IoT systems where attackers overwhelm the target device with a flood of traffic, rendering it unavailable?
a) DDoS (Distributed Denial of Service)
b) SQL Injection
c) Cross-Site Scripting (XSS)
d) Man-in-the-Middle (MitM) Attack

Answer: a) DDoS (Distributed Denial of Service)

Explanation: DDoS attacks involve overwhelming a target device or network with a flood of traffic from multiple sources, causing it to become unavailable to legitimate users.

6. Which vulnerability analysis technique involves analyzing the source code, hardware, and software configurations of IoT devices for security flaws?
a) Penetration Testing
b) Static Analysis
c) Dynamic Analysis
d) Fuzz Testing

Answer: b) Static Analysis

Explanation: Static analysis involves examining the source code, hardware design, and software configurations of IoT devices without executing the code, to identify potential security vulnerabilities.

7. Which IoT case study involves the integration of various smart devices within a household to enhance convenience, security, and energy efficiency?
a) Smart Farming
b) Industrial Automation
c) Smart Home
d) Healthcare Monitoring

Answer: c) Smart Home

Explanation: Smart Home systems involve the integration of various IoT devices such as

smart thermostats, lighting, security cameras, and appliances to enhance convenience, security, and energy efficiency within a household.

8. Which cloud service model is commonly used for IoT applications, providing on-demand access to computing resources over the internet?
a) Infrastructure as a Service (IaaS)
b) Platform as a Service (PaaS)
c) Software as a Service (SaaS)
d) Function as a Service (FaaS)

Answer: a) Infrastructure as a Service (IaaS)

Explanation: IaaS provides on-demand access to virtualized computing resources such as servers, storage, and networking over the internet, which is commonly used in IoT applications for scalable and flexible infrastructure deployment.

9. What IoT platform is known for its low-power consumption and is commonly used in battery-operated devices?
a) Arduino
b) Raspberry Pi
c) ESP8266
d) BeagleBone

Answer: c) ESP8266

Explanation: ESP8266 is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capability, known for its low-power consumption, making it suitable for battery-operated IoT devices.

10. Which data analytics technique involves analyzing historical IoT data to identify patterns and make predictions about future events?
a) Descriptive Analytics
b) Diagnostic Analytics
c) Predictive Analytics
d) Prescriptive Analytics

Answer: c) Predictive Analytics

Explanation: Predictive analytics involves analyzing historical IoT data using statistical algorithms and machine learning techniques to identify patterns and trends, enabling predictions about future events or outcomes.

Related posts:

1. Introduction to Information Security
2. Introduction to Information Security MCQ
3. Introduction to Information Security MCQ
4. Symmetric Key Cryptography MCQ
5. Asymmetric Key Cryptography MCQ
6. Authentication & Integrity MCQ
7. E-mail, IP and Web Security MCQ