Q.1) Mention key features of M2M.

➔ Machine-to-Machine (M2M) communication enables automated data exchange between devices, facilitating remote monitoring, control, and efficiency across diverse industries while ensuring security and interoperability.

Q.2) Explain the Proximity Sensor.

➔ A proximity sensor is a device that detects the presence or absence of nearby objects without physical contact. It works by emitting electromagnetic fields, light, or sound waves and then sensing changes in these fields or waves caused by the proximity of an object. Common types include capacitive, inductive, ultrasonic, and infrared sensors

Q.3) Give 2 differences between TCP and UDP.

- TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol.

- TCP uses handshake protocol like SYN, SYN-ACK, ACK while UDP uses no handshake protocols.

- TCP is reliable as it guarantees the delivery of data to the destination router while in UDP The delivery of data to the destination cannot be guaranteed.

Q.4) Define CIA triad.

The CIA triad is a fundamental concept in information security, comprising three core principles:

- Confidentiality (ensuring data is accessible only to authorized individuals),
- Integrity (maintaining the accuracy and trustworthiness of data),
- and Availability (ensuring data is accessible and usable when needed).

Q.5) Explain Predictive and Prescriptive Analytics.

Predictive analytics involves using historical data, statistical algorithms, and machine learning techniques to predict future outcomes or trends. It analyzes patterns and relationships within data to forecast what might happen in the future, often providing probabilities or likelihoods of different outcomes.

Prescriptive analytics, on the other hand, goes beyond predicting future outcomes to provide recommendations on what actions to take to achieve a desired outcome. It considers various possible actions and their potential outcomes, taking into account constraints, objectives, and preferences to offer actionable insights and decision support.

Q.6) Explain IaaS, PaaS and SaaS.

Q.7) Explain IPv4 and IPv6.

IPv4 (Internet Protocol version 4) is the fourth version of the Internet Protocol, which assigns numerical addresses to devices connected to a network. It uses 32-bit addresses, allowing for approximately 4.3 billion unique addresses. However, due to the rapid growth of the internet, IPv4 addresses are running out, leading to the development of IPv6.

IPv6 (Internet Protocol version 6) is the latest version of the Internet Protocol designed to address the limitations of IPv4. It uses 128-bit addresses, providing an exponentially larger address space, capable of accommodating an almost limitless number of devices. IPv6 also offers improved security,

efficiency, and support for emerging technologies like Internet of Things (IoT). However, widespread adoption of IPv6 has been relatively slow compared to IPv4.

Q.8) Mention 4 applications of WSN.

- Environmental Monitoring
- Industrial Automation
- Healthcare and Medical Applications
- Smart Cities

Q.9) Explain IOT Communicational Model.

- Request-Response Model
- Publish-Subscribe Model
- Push – pull Model
- Exclusive Pair

Q.10) Give 2 difference between Sensors and Actuators.

- Sensors take Input from the Environment But the Actuator take input from sensor or micro-controller.

- Sensor converts the Physical characteristics into Electric signals bur the Actuators converts electric signals into physical characteristics.

Ex, Cameras, microphones Ex, LED, Laser, speakers, motor, piston etc

Q.11) Define AAA Framework

The AAA framework, standing for Authentication, Authorization, and Accounting, is a security model used to control access to resources in computer networks.

Authentication: Verifies the identity of users or devices attempting to access the network or specific resources within it.

Authorization: Determines what actions or resources users or devices are permitted to access after successful authentication.

Accounting: Tracks and records the usage of network resources by authenticated users or devices. This includes logging activities such as login attempts, resource access, and data transfers for auditing, billing, and security analysis purposes.

Q.12) IoT Data Analysis

IoT analytics is the process of evaluating data generated and gathered by IoT devices using a particular set of data analytics tools and techniques.

Types of IoT Data Analytics:

- Descriptive Analytics

- Diagnostic Analytics

- Predictive Analytics And Prescriptive Analytics

Q.12) What do you mean by Diagnostic analytics

Diagnostic analytics goes further and concentrates on the “Why?”. In diagnostic analytics, the software focuses on understanding the past and identifying what happened.

Q.13) Explain Infrared(IR) Sensor

An Infrared (IR) sensor is a device that detects and measures infrared radiation in its surrounding environment. Infrared radiation is electromagnetic radiation with wavelengths longer than those of visible light, making it invisible to the human eye.

Q.14) Differentiate between IOT and M2M.

Difference between IoT and M2M - GeeksforGeeks

Q.15) What is Protocol Suite

A protocol suite, also known as a protocol stack, is a set of communication protocols that are used together to enable network communication between devices or systems. Each layer of the protocol suite performs specific functions related to the transmission, routing, and delivery of data across a network. The most well-known protocol suite is the TCP/IP (Transmission Control Protocol/Internet Protocol) suite.

Q.16) Mention Big Data analytics tools.

- Hadoop
- Apache Spark
- MongoDB
- Python and R
- TensorFlow (Machine Learnig Framework)

Q.17) Explain Challenges of WSN

- Quality of Service
- Security Issue
- Energy Efficiency
- Network Throughput
- Performance
- Ability to cope with node failure
- Cross layer optimisation
- Scalability to large scale of deployment

Q.18) Mention IoT enabling techniques.

- Wireless Communication Protocols
- Sensors and Actuators
- Embedded Systems
- Cloud Computing

- Security Mechanisms

- Communication Protocols

- Edge Computing

Q.19) Differentiate between Analog and Digital Sensors.

Difference Between Digital And Analog System - GeeksforGeeks

Q.20) Explain Perception Layer of IOT building blocks.

The Perception Layer is one of the building blocks of IoT architecture and refers to the bottom layer where data is collected from the physical world through sensors, actuators, and other devices. It serves as the interface between the physical environment and the digital world, capturing information about various parameters, events, and conditions.

Q.21) What is IOT gateway?

An IoT gateway is a physical or virtual device that serves as an intermediary between IoT devices (sensors, actuators, etc.) and the cloud or data center where data processing, storage, and analysis take place. It plays a crucial role in IoT systems.

Q.22) What is Edge Computing?

Edge computing is a distributed computing paradigm that involves processing data closer to the source of data generation, rather than relying solely on centralized data centers or cloud computing resources. In edge computing, data processing and storage are performed on or near the "edge" of the network, closer to where data is generated, collected, or consumed.

Q.29) What do you mean by RFID

RFID stands for Radio Frequency Identification. It is a technology that uses radio waves to identify and track objects, animals, or people wirelessly. RFID systems consist of three main components:

- RFID Tags

- RFID Readers

- Middleware and Database

Q.31) Differentiate between COAP and HTTP

HTTP use TCP while coap use UDP

HTTP is a general-purpose protocol while CoAP is a specialized protocol

CoAP uses both client-Server & Publish-Subscribe models, while HTTP uses client and server architecture.

CoAP has less overhead and is simpler, while HTTP has more overhead and is more complex.

Q.34) Mention Raspberry pi models name

Raspberry Pi 1 Model A

Raspberry Pi 1 Model A+

Raspberry Pi 1 Model B

Raspberry Pi 1 Model B+

Raspberry Pi 2 Model B

Raspberry Pi 3 Model A

Raspberry Pi 3 Model A+

Raspberry Pi 3 Model B

Raspberry Pi 3 Model B+

Raspberry Pi 4 Model A

Raspberry Pi 4 Model B

Raspberry Pi Zero

Q.35) Define GPIO Component of Raspberry pi

GPIO stands for General Purpose Input/Output, and it refers to the set of pins on a Raspberry Pi (or similar devices) that can be used for digital input or output operations. These pins can be programmed to either read digital signals from external sensors or devices (input) or to send digital signals to control external components such as LEDs, motors, or relays (output).

In short, GPIO pins allow the Raspberry Pi to interact with the physical world by receiving or sending digital signals, making them versatile for a wide range of projects and applications.