INTERNET OF THINGS (IOT)

BRANCH:- OPEN ELECTIVE

SEMESTER – FIFTH

These important questions have been prepared using your previous exam papers (PYQs), verified concepts, and additional reference from trusted online academic sources.
For deeper understanding, please refer to your class notes as well.

1️⃣ HIGH & LONG IMPORTANT QUESTIONS

Unit 1: Introduction to Internet of Things

1. **Define** IoT. Explain the **Physical Design of IoT** (Things, Protocols) and the **Logical Design of IoT** (Functional Blocks, Communication Models) with a neat block diagram illustrating the overall concept.
2. Elaborate on the key **IoT Enabling Technologies**. Discuss the crucial role of **Wireless Sensor Networks (WSN)**, **Cloud Computing**, and **Big Data Analytics** in forming a complete IoT ecosystem.
3. Explain the concept of **IoT Levels and Deployment Templates (Level-1 to Level-6)**. Give a clear example of a domain-specific IoT system (e.g., Home Automation) and map it to an appropriate IoT Level, justifying your choice.

Unit 2: M2M, IoT System Management with NETCONF-YANG

4. Distinguish clearly between **M2M (Machine-to-Machine)** and **IoT** based on architecture, communication, and scope. Discuss the need for a dedicated **IoT Systems Management** solution.
5. Explain the detailed process of **IoT Systems Management using NETCONF-YANG**. Describe the specific roles and advantages of the **NETCONF protocol** and the **YANG data modeling language** in configuring IoT devices.

Unit 3 & 4: Elements of IoT & IoT Application Development

6. Describe the comprehensive **IoT Design Methodology** step-by-step (Purpose, Model, Functional, Operational View, Device/Resource Modeling, Service Specification). Illustrate the steps using a **Smart City** case study example.
7. Discuss the theoretical role of **Hardware Components** (Sensors, Actuators, Smart Objects, RFID) and **Software Components** (Python Packages, Networking Protocols) that form the basic building blocks of an IoT Device.
8. Explain the significance of **Raspberry Pi interfaces** (GPIO, SPI, I2C, UART – focus on theory/functionality, not programming) for connecting various peripherals in an IoT system. Briefly discuss **Data storage on cloud/local server**.

Unit 5 & 6: IoT Security, IIoT and Case Studies

9. Discuss the major **Security, Privacy, and Governance issues** in the context of IoT. Explain the purpose and stages of the **IoT security life cycle** and how it helps mitigate threats.
10. Define **IIoT (Industrial Internet of Things)**. Compare and contrast **IoT and IIoT**, focusing on their differences in terms of security, data volume, and criticality of applications.
11. Select **two** of the following **Domain-specific IoT Case Studies** and explain the system's objective, sensor requirements, and key functionalities in detail:
    - **Health Care** (e.g., Remote Patient Monitoring)
    - **Agriculture** (e.g., Precision Farming)
    - **Urban Cities** (e.g., Smart Parking/Waste Management)

2️⃣ IMPORTANT & SHORT QUESTIONS

1. What is the function of **IoT Communication API's**? Name two common types.
2. Differentiate between the **Request-Response** and **Publish-Subscribe** IoT Communication Models.
3. Explain the concept of **IoT Protocols** and give examples for the Application Layer and Network Layer.
4. Write a short note on the role of **SDN (Software-Defined Networking)** and **NFV (Network Function Virtualization)** for IoT.
5. What are the four main types of **IoT Communication Models**? Explain each briefly.
6. Briefly describe the purpose of **Python Packages of interest for IoT** (e.g., *requests*, *paho-mqtt* – focus on purpose, not code).
7. List the key **Networking Protocols** used in an IoT system.

8. Explain how **Blockchain** technology can be used to enhance **IoT security**.
9. Give a brief overview of the **Security, Privacy, and Trust** challenges in data collected by consumer IoT devices.
10. What are the core differences between a **Sensor** and an **Actuator**? Give one example of each in a home automation system.

---

3 "AA BHI SAKTA HAI"

1. List and briefly explain any three **characteristics** that define an IoT system.
2. Explain the concept of **Smart Objects** and how they enable IoT applications.
3. Why is **Simple Network Management Protocol (SNMP)** often considered unsuitable for constrained IoT devices?
4. What are the key differences between **IoT Level-3** and **IoT Level-4** deployment templates?
5. Briefly explain the application of IoT in the **Environment** monitoring domain (e.g., pollution or weather).
6. What is the main purpose of **Governance** in the context of large-scale IoT deployments?
7. List any three **Popular IoT Platforms** (e.g., AWS IoT, Microsoft Azure IoT, Google Cloud IoT).

QUICK REVISE

Unit 1: Introduction to IoT

Concept	Short Note
IoT Definition	A network of **physical "things"** embedded with sensors, software, and other technologies, connected over the internet to exchange data. Key characteristic: **Ubiquitous connectivity**.
Physical Design	Focuses on the "Things" (devices/sensors) and how they communicate. Includes **IoT Devices** (e.g., microcontrollers) and **IoT Protocols** (e.g., HTTP, MQTT, CoAP).
Logical Design	Focuses on the abstract components and software implementation. Includes **IoT Functional Blocks**

Concept	Short Note
	(Sensing, Actuating, Data Processing, Application) and **Communication Models**.
Communication Models	**1. Request-Response** (Client requests, Server responds), **2. Publish-Subscribe** (Broker manages messages between Publishers/Subscribers), **3. Push/Pull**.
IoT Enabling Tech.	**WSN** (Wireless Sensor Networks), **Cloud Computing** (for data storage/processing), **Big Data Analytics** (for insights), **Embedded Systems**.
IoT Levels/Templates	**Level 1** (Single device, local analysis), **Level 6** (Complex system, multiple devices, centralized control/cloud processing). Describes complexity/deployment type.

Unit 2: M2M & IoT System Management

Concept	Short Note
M2M	**Machine-to-Machine.** Focuses on point-to-point communication between two machines, often siloed, for specific tasks (e.g., utility meter reading).
IoT vs. M2M	**IoT** is broader (network of networks), uses standard IP protocols, and focuses on **data and applications**. **M2M** is specific, often uses proprietary/cellular tech, and focuses on **remote monitoring**.
SDN & NFV for IoT	**SDN (Software-Defined Networking)** separates control and data planes. **NFV (Network Function Virtualization)** virtualizes network services. Both enhance flexibility, scalability, and resource management for large IoT networks.
NETCONF	**Network Configuration Protocol.** A protocol used to install, manipulate, and delete the configuration of network devices. Key for centralized IoT system management.
YANG	**Yet Another Next Generation.** A data modeling language used with NETCONF to describe the structure and syntax of configuration and state data for IoT devices.

Unit 3 & 4: Elements & Design

Concept	Short Note
Basic Building Blocks	**Device** (e.g., Raspberry Pi/Arduino), **Gateway** (aggregates data), **Cloud/Data Centre**, and **User Interface/Application**.
Sensors/Actuators	**Sensors** measure physical quantities (e.g., temp, pressure) and convert them to electrical signals. **Actuators** convert electrical signals into physical action (e.g., opening a valve, switching a light).
Smart Objects/RFID	**Smart Objects** are small devices with processing/communication capabilities. **RFID** (Radio-Frequency Identification) uses electromagnetic fields to automatically identify and track tags attached to objects.
IoT Design Methodology	A systematic, multi-step process: 1. Purpose & Requirements, 2. Process Specification, 3. Domain Model, 4. Information Model, 5. Service Specification, 6. Operational View, 7. Device and Resource Modeling.
Data Storage	IoT data can be stored locally on the **device/gateway** (for fast action) or on **Cloud Servers** (for long-term storage, analytics, and global access).

Unit 5: Privacy, Security, and Governance

Concept	Short Note
Security Issues	Threats include **Device Hijacking**, **Data Eavesdropping**, **Physical Tampering**, and **DDoS attacks** via botnets of compromised IoT devices.
Privacy Issues	IoT devices collect large volumes of sensitive **Personally Identifiable Information (PII)**. Key risk is **data misuse** and **lack of consent** in data collection/sharing.
Governance	The establishment of **policies, standards, and regulatory frameworks** to manage the operational risks, legal compliance, and ethical use of IoT devices and data.
Security Life Cycle	**1. Secure Initialization** (Secure boot), **2. Secure Operation** (Authentication, Encryption), **3. Secure Updates**

Concept	Short Note
	(Patching), and **4. Secure Decommissioning** (Secure data wiping).
Blockchain in IoT	Used for creating **decentralized, tamper-proof ledgers** for device identity management, secure data sharing, and automated peer-to-peer transactions, enhancing trust.

Unit 6: IIoT and Case Studies

Concept	Short Note
IIoT Definition	**Industrial Internet of Things.** IoT applied to industrial sectors like manufacturing, oil & gas, and energy. Focuses on mission-critical operations and performance.
IoT vs. IIoT	**IIoT** demands higher reliability, lower latency, extreme security, and ruggedized hardware, focusing on **machine health and safety**. **IoT** focuses on consumer convenience.
Home Automation	**Objective:** Remote control/monitoring of home appliances (lights, security, HVAC). **Components:** Smart Plugs, Cameras, Voice Assistants.
Health Care	**Objective:** Remote Patient Monitoring (RPM), tracking vital signs. **Components:** Wearable sensors, medical-grade IoT devices.
Urban Cities	**Objective:** Optimizing public services (e.g., Smart Traffic, Smart Parking, Waste Management). **Components:** Road sensors, smart meters, environment sensors.
Agriculture	**Objective:** Precision Farming. Monitoring soil health, weather, and crop conditions. **Components:** Soil moisture sensors, weather stations, drones.