IOT

SECTION A (30mks)

QUESTION ONE

a. Discuss the Benefits of wireless sensor networks(4mks)

b. Explain any four ZigBee's M2M/IoT Applications(4mks)

c. Explain how an IOT system works(4mks)

d. Describe the different components of IOT. (4mks)

e. Explain how IoT can influence the development of smart cities(4mks)

QUESTION TWO (20mks)

a. Explain how the 5G cellular networks are likely to impact IoT(5mks)

b. Describe howcan edge computing benefit IoT(5mks)

c.What are some of the biggest security vulnerabilities that come with loT (5mks)

d. What are some use cases for IoT data analytics?(5mks)

QUESTION THREE (20mks)

Using an example of an arduino project, describe how you can implement an IoT project clearly indicating

a. The problem statement(4mks)

b. The materials you require(4mks)

c. How you can connect them to actualize your project.(6mks)

d. Indicate the challenges you are likely to encounter in implementing your project.(6mks)

QUESTION FOUR (20mks)

a. Explain any three liabilities and how they can be mitigated in the implementation of IoT systems

b. Describe how you can test the performance of an IoT system?(6mks)

c. Explain the advantages and disadvantages of Home Area Network (HAN) (6mks)

d. What are the main differences between IoT and M2M?(4mks)

QUESTION FIVE (20mks)

a. Explain any ten ways you can use to protect the privacy of your IOT systems (6mks)

b. What are the top challenges of implementing an IoT system? (6mks)

c. What steps can an organization take to protect IoT systems and devices? (4mks)

d. What are some of the protocols used for IoT communication? (4mks)

SECTION A (30 marks)

QUESTION ONE

a. Benefits of wireless sensor networks (4mks)

1. **Remote Monitoring** – Enables real-time data collection from remote or hazardous environments.
2. **Scalability** – Easily scalable by adding more nodes without much infrastructure.
3. **Cost-effective** – Reduces the need for manual monitoring, lowering labor costs.
4. **Energy Efficiency** – Designed for low-power operation, prolonging battery life.

b. Four ZigBee's M2M/IoT Applications (4mks)

1. **Smart lighting systems** – ZigBee controls lighting remotely and saves energy.
2. **Home automation** – Used in devices like smart thermostats and door locks.

3. **Industrial automation** – For monitoring machinery and environmental conditions.
4. **Smart metering** – Used in energy and water meters for data transmission.

c. How an IoT system works (4mks)

1. **Sensors/Devices** collect data from the environment.
2. **Connectivity** – Data is transmitted via Wi-Fi, Bluetooth, ZigBee, etc.
3. **Data Processing** – Cloud or local servers analyze the data.
4. **Action** – Trigger a response (alert, automation, etc.) based on analysis.

d. Components of IoT (4mks)

1. **Sensors/Actuators** – Gather and react to data.
2. **Connectivity Module** – Enables communication (Wi-Fi, GSM, etc.).
3. **Data Processing** – Cloud or edge computing systems.
4. **User Interface** – Web or mobile apps for monitoring/control.

e. IoT and smart cities (4mks)

1. **Traffic management** – Smart lights and real-time congestion updates.
2. **Waste management** – Sensors in bins optimize collection routes.
3. **Energy efficiency** – Smart grids and street lighting reduce wastage.
4. **Public safety** – Surveillance and emergency response optimization.

f. Uses of Arduino, Raspberry Pi, Actuators and Sensors (5mks)

- **Arduino** – Used for simple control tasks (e.g., reading sensors, blinking LEDs).
- **Raspberry Pi** – Acts as a mini-computer for complex processing (e.g., facial recognition).
- **Sensors** – Gather environmental data (e.g., temperature, motion).
- **Actuators** – Perform actions (e.g., rotate motors, turn lights on/off).

g. Differences between Bluetooth and Bluetooth LE (5mks)

Feature	Bluetooth	Bluetooth Low Energy (LE)
Power Consumption	High	Low
Data Rate	Higher	Lower
Connection Time	Longer	Faster
Application	Audio, file transfer	IoT devices, fitness trackers

Battery Life	Drains faster	Lasts longer

QUESTION TWO (20mks)

a. Impact of 5G on IoT (5mks)

- **Low Latency** – Real-time communication for critical applications.
- **Massive Connectivity** – Supports billions of devices per square km.
- **High Data Speeds** – Ideal for video surveillance, AR/VR, etc.
- **Reliability** – Consistent connectivity even in dense environments.
- **Network Slicing** – Custom virtual networks for different IoT needs.

b. Edge Computing Benefits to IoT (5mks)

- **Reduced Latency** – Processes data near the source.
- **Lower Bandwidth Usage** – Only sends necessary data to the cloud.
- **Improved Security** – Data remains local, reducing exposure.
- **Faster Decision Making** – Real-time analytics.
- **Reliability** – Works even during internet outages.

c. Biggest Security Vulnerabilities (5mks)

1. Weak passwords and credentials.
2. Unpatched firmware or software.
3. Lack of data encryption.
4. Physical tampering.
5. Poor network security.

d. Use Cases for IoT Data Analytics (5mks)

1. **Predictive maintenance** – Detect equipment failure early.
2. **Smart agriculture** – Optimize irrigation and fertilizer usage.
3. **Fleet management** – Monitor vehicle performance and routes.
4. **Healthcare monitoring** – Track patient vitals in real-time.
5. **Energy optimization** – Analyze consumption patterns.

QUESTION THREE (20mks)

Using an example of an arduino project, describe how you can implement an IoT project clearly indicating

Example Project: Smart Temperature Monitoring System

a. Problem Statement (4mks)

Need for real-time temperature monitoring in remote greenhouses to ensure optimal plant growth.

b. Materials Required (4mks)

- Arduino Uno
- DHT11 temperature sensor
- Wi-Fi module (ESP8266)
- LCD Display
- Breadboard and jumper wires
- Power supply

c. Connection & Implementation (6mks)

- Connect DHT11 sensor to Arduino to collect temperature.
- Use ESP8266 to send data to a cloud server.
- Display readings on LCD.
- Monitor and set alerts for temperature thresholds via web dashboard.

d. Challenges (6mks)

- Internet connectivity in remote areas.
- Sensor calibration issues.
- Power reliability.
- Data accuracy and delays.
- Integration with cloud services.
- Handling multiple sensor inputs.

QUESTION FOUR (20mks)

a. Three liabilities and mitigation (6mks)

1. **Data Breach** – Use encryption and secure authentication.
2. **Device Malfunction** – Regular maintenance and fail-safes.
3. **Unauthorized Access** – Implement firewalls and access control.

b. Testing IoT Performance (6mks)

- Stress testing for load handling.
- Latency checks.
- Power consumption monitoring.
- Network performance analysis.
- Functional and integration testing.
- Real-world scenario simulations.

c. Home Area Network (HAN) Pros/Cons (4mks)
Advantages:

- Centralized control of home devices.
- Improved energy efficiency.

Disadvantages:

- Vulnerable to hacking.
- High setup cost.

d. IoT vs M2M (4mks)

Feature	IoT	M2M
Scope	Broad, cloud-connected	Point-to-point
Connectivity	Internet-based	Wired/Wireless
Scalability	High	Limited
Intelligence	Smart & analytical	Simple communication

QUESTION FIVE (20mks)

a. Ten ways to protect IoT privacy (6mks)

1. Use Strong Authentication and Authorization: Require secure login credentials (e.g., strong passwords, two-factor authentication) to prevent unauthorized access to IoT devices and systems.

2. Encrypt Data Transmission: Use encryption protocols like **TLS/SSL** to protect data being transmitted between IoT devices and the cloud/server from eavesdropping.

3. Regular Software and Firmware Updates: Keep devices updated with the latest security patches to fix vulnerabilities that could be exploited by attackers.

4. Disable Unused Services and Ports: Turn off unnecessary features or communication ports to reduce attack surfaces.

5. Use Firewalls and Network Segmentation: Place IoT devices on separate networks (VLANs) and use firewalls to restrict traffic to and from these devices.

6. Secure Device Storage: Encrypt stored data on the device and ensure local memory is protected, especially if the device stores sensitive information.

7. Anonymize and Minimize Data Collection: Collect only essential data and remove personally identifiable information (PII) where possible to reduce privacy risks.

8. Monitor and Log Device Activity: Continuously monitor IoT devices for unusual behavior and keep logs for audits and incident response.

9. Physical Security: Secure physical access to IoT devices to prevent tampering, especially in public or industrial environments.

10. User Awareness and Training: Educate users and staff on IoT privacy best practices, including safe device configuration and recognizing threats like phishing.

b. Challenges of implementing IoT (6mks)

1. Security risks.
2. Integration complexity.
3. High initial cost.
4. Interoperability issues.
5. Data management.
6. Power constraints.

c. Organization protection steps (4mks)

- Enforce strong access control.
- Use intrusion detection systems.

- Regularly audit devices.
- Employ device lifecycle management.

d. IoT Protocols (4mks)

1. **MQTT** – Lightweight messaging protocol.
2. **CoAP** – REST-based protocol for constrained devices.
3. **HTTP** – Web communication.
4. **IPv6** – Expands address space for devices.