Answer Key: MAQB

Section 1 (6 marks per question)

Q1. Why is security a significant concern in the Internet of Things (IoT)?

Keywords:

security, privacy, data breaches, sensitive information

Main Points:

• IoT involves sharing sensitive data, raising privacy and security concerns.
• Data breaches can expose personal and business information.

Detailed Explanation:

The interconnected nature of IoT devices and the data they collect makes them vulnerable to attacks. Lack of proper security measures can lead to unauthorized access and misuse of sensitive information.

Examples:

• A smart home device being hacked to spy on residents.

Q2. What is the current focus of IoT service providers, and why is this a problem?

Keywords:

availability, interoperability, security, vulnerability, exploits

Main Points:

• IoT service providers prioritize availability and interoperability over security.
• This leaves devices vulnerable to exploits and attacks.

Detailed Explanation:

The emphasis on functionality over security creates a significant risk, as many IoT devices are not adequately protected against cyber threats.

Examples:

• A network of connected medical devices being disrupted by a denial-of-service attack.

Q3. What challenges do the characteristics of IoT devices pose to security implementation?

Keywords:

constrained resources, lightweight security, computational power, memory, energy capacity

Main Points:

- IoT devices have limited capacity and computational power.
- Security measures need to be lightweight and compatible with these limitations.

Detailed Explanation:

Traditional security solutions are often too resource-intensive for IoT devices, necessitating the development of specialized, lightweight security approaches.

Examples:

- A small sensor node being unable to run complex encryption algorithms.

Q4. What are the two proposed approaches for addressing security threats in IoT mentioned in the text?

Keywords:

obfuscation, diversification, operating systems, APIs, communication protocols

Main Points:

- Applying obfuscation and diversification to protect operating systems and APIs.
- Applying obfuscation and diversification to secure communication protocols.

Detailed Explanation:

These techniques aim to make it more difficult for attackers to understand and exploit vulnerabilities in IoT systems and communications.

Examples:

- Varying the communication protocols used by different devices to prevent widespread attacks.

Q5. Why is software compatibility a crucial factor in IoT development?

Keywords:

heterogeneous components, compatibility, resource constraints, low-powered devices, software adaptability

Main Points:

- IoT comprises diverse devices with varying processing power.
- Software must be adaptable to both powerful and resource-constrained devices.

Detailed Explanation:

The wide range of hardware in IoT requires software that can function effectively across different platforms and resource limitations.

Examples:

- An operating system designed to run on both a smartphone and a simple sensor.