

Answer Key: JS Questions

Section 1 (5 marks per question)

Q1. Explain the device/cloud collaboration framework and its components.

Keywords:

device/cloud collaboration, scalability, privacy

Main Points:

- Improves scalability and privacy protection.
- Leverages smart mobile devices and cloud resources.
- Protects privacy without affecting application quality.

Detailed Explanation:

The framework leverages smart mobile devices and cloud resources to improve scalability and privacy protection, especially for applications that offer personalized intelligence services.

Examples:

- Google Now provides personalized recommendations based on user context.
- Facebook recognizes users and their relationships from uploaded images.

Q2. Describe the functionalities of the runtime adaptation engine.

Keywords:

runtime adaptation engine, query processing, smart device

Main Points:

- Processes queries on smart devices without cloud transfer.
- Conserves battery life and improves accuracy when needed.
- Supports redundant queries to the cloud when mobile engine results are insufficient.

Detailed Explanation:

The runtime adaptation engine allows for query processing on smart devices, preserving battery life. However, it can also transfer queries to the cloud for improved accuracy or in case of insufficient mobile results.

Examples:

- Lightweight mobile engine answers queries locally.
- Queries may be transferred to the cloud for better accuracy or in case of poor mobile results.

Q3. Discuss the advantages and limitations of the device/cloud collaboration framework.

Keywords:

device/cloud collaboration, advantages, limitations

Main Points:

- Advantages: Increased computing capacity, improved battery efficiency, enhanced privacy.
- Limitations: Network dependency, security concerns, potential latency issues.

Detailed Explanation:

The framework offers increased computing capacity, improved battery efficiency, and enhanced privacy. However, it also introduces network dependency and raises security concerns due to data transfer, and may introduce potential latency issues.

Examples:

- Cloud resources supplement limited device capabilities.
- Network connectivity is crucial for the framework's operation.

Q4. How does the device/cloud collaboration framework enhance privacy protection?

Keywords:

device/cloud collaboration, privacy protection, encryption

Main Points:

- Privacy-preserving data transfer techniques.
- Distributed data storage and processing across devices and cloud.
- Encrypted communication channels to protect sensitive data.

Detailed Explanation:

The framework utilizes privacy-preserving data transfer techniques, distributes data storage and processing, and employs encrypted communication channels to safeguard sensitive data during device-cloud interactions.

Examples:

- Data transfer protocols protect privacy during communication.
- Distributed data processing minimizes data concentration in a single location.

Q5. Analyze the potential applications of the device/cloud collaboration framework in various domains.

Keywords:

device/cloud collaboration, applications, healthcare, transportation, finance

Main Points:

- Healthcare: Remote patient monitoring, personalized treatment plans.
- Transportation: Real-time traffic updates, navigation assistance.
- Finance: Mobile banking, fraud detection.

Detailed Explanation:

The framework finds potential applications in diverse domains due to its ability to combine device capabilities with cloud resources. This allows for personalized services, real-time data analysis, and improved user experiences.

Examples:

- Remote health monitoring allows doctors to access patient data and provide timely interventions.
- Real-time traffic updates help commuters optimize their routes.