IOT

I. Smart Products (35% - 6 Questions)

Scenario: A large logistics company decides to equip its fleet of delivery trucks with a smart sensor system to monitor vehicle conditions and locations in real-time and predict maintenance needs.

Questions:

1. Describe how this type of smart system, through monitoring, control, optimization, and automation functions, can improve the logistics company's operational efficiency.

2.How can this system help the company reduce vehicle maintenance costs?

Scenario: A home appliance company launches a smart washing machine that can automatically detect the weight and material of clothes, adjust washing time and water usage, and includes remote control functions.

Questions:

1.How does this smart washing machine provide users with convenience and energy savings through its optimization and remote control functions?

2.What layers and technologies in IoT architecture should be considered in designing this system?

Scenario: An agricultural tech company develops a sensor-based smart irrigation system that automatically adjusts the water supply based on soil moisture and weather conditions.

Questions:

1.Describe how the smart irrigation system uses sensor data to optimize resource use in agriculture.

2.What advantages do the control and optimization functions of this system provide in an agricultural environment?

Scenario: A medical equipment company introduces a heart rate monitor with remote monitoring functions, allowing doctors to observe patients' heart rate changes in real-time through a cloud platform.

Questions:

1.How does this device improve patient care quality through remote monitoring?

2.How should the system be designed to protect patient privacy?

Scenario: An automotive manufacturer launches a smart onboard system that monitors and adjusts fuel consumption and emissions in real-time to comply with environmental standards.

Questions:

1.How does the smart onboard system reduce emissions and improve vehicle environmental performance through optimization functions?

2.What sensors and data collection methods should be considered in system design?

Scenario: A fitness equipment company launches a smart treadmill that adjusts workout intensity based on the user's heart rate and stride and records workout data on the cloud.

Questions:

1.How does the smart treadmill help users achieve a more personalized workout experience through automatic adjustment and data recording?

2.What data privacy issues need attention for this type of device?

II. Sensors (20% - 3 Questions)

Scenario: An environmental monitoring company plans to install air quality monitoring stations in urban areas to measure PM2.5, temperature, and humidity.

Questions:

1.What key characteristics should be considered when selecting sensors for this environmental monitoring system? Consider precision, durability, etc.

2.How can the stability and reliability of sensors be ensured in different environmental conditions?

Scenario: In an industrial production setting, a factory installs vibration sensors to monitor the operation of critical equipment and prevent equipment failures.

Questions:

1.Describe the working principle of vibration sensors and their role in industrial applications.

2.How can sensor data help engineers predict equipment failures?

Scenario: A high-precision temperature sensor is used in a laboratory to monitor temperature changes during chemical reactions in real-time.

Questions:

1.How is the calibration process for the temperature sensor carried out? How can environmental factors affecting measurement results be reduced?

2.List other performance parameters that should be considered when selecting this sensor.

III. IoT Security (20% - 3 Questions)

Scenario: A smart home company launches a smart door lock that users can remotely control through a mobile app. However, security experts point out that the device is at risk of being hacked.

Questions:

1.What security measures should the manufacturer implement to address potential threats to the smart door lock?

2.What measures can users take to protect their privacy when using such smart devices?

Scenario: A company that produces smart cameras fails to thoroughly test the device firmware for security before launch, leading to easy hacking of the devices.

Questions:

1.Describe the potential security vulnerabilities in this situation and corresponding countermeasures.

2.How can users minimize privacy risks when using this type of device?

Scenario: A company develops an IoT children's toy with remote control and recording functions. However, due to a lack of data encryption, hackers use the toy to collect user voice data.

Questions:

1.List the main security vulnerabilities in this IoT toy and suggest improvements.

2.How can the security of IoT device data be protected to prevent hacking?

IV. Tiny Machine Learning (25% - 4 Questions)

Scenario: A smartwatch manufacturer introduces TinyML technology, enabling the device to locally detect abnormal heart rates and alert users.

Questions:

1.What are the main advantages of TinyML technology in a smartwatch? Describe how data processing and anomaly detection are performed locally.

2.What model optimization methods can be used to address memory and computational limitations?

Scenario: A smart security company develops a low-power camera that uses TinyML technology to detect moving objects and automatically trigger an alarm.

Questions:

1.How does TinyML enable efficient detection while maintaining low power consumption in this security device?

2.How can detection accuracy be improved under low-light conditions? What TinyML model optimization techniques can be used?

Scenario (Calculation Question): A spam detection model is applied to classify emails. Out of 2000 emails, 500 are spam. The model successfully identifies 400 spam emails and 1400 non-spam emails, but incorrectly flags 100 non-spam emails as spam and misses 100 spam emails.

Questions:

1.Calculate the True Positive (TP) and False Positive (FP) values of the model.

2.Using these values, calculate the accuracy of the model.

Scenario: A medical company uses TinyML to develop a portable ECG monitoring device that processes and analyzes ECG data locally to detect arrhythmias.

Questions:

1.Describe the advantages of TinyML in medical devices, including considerations for latency and data privacy.

2.How can efficient model inference be achieved given memory limitations? Which model compression techniques can be used?

万金油格式：回答情景题的通用步骤

背景介绍：

简要描述情境中的产品或系统，包括其功能和主要应用场景。
如果涉及到特定的技术（例如智能产品、TinyML、IoT 安全、传感器等），可以简单阐述其技术特点或核心作用。

示例：

“某公司推出了一款智能家居设备，能够通过物联网技术进行远程控制和监测，旨在提高用户的居住便利性和安全性。”

问题分析：

识别情景中的关键问题或挑战。
根据题目要求，详细列出可能遇到的技术问题（如安全漏洞、资源限制、环境干扰等）或用户需求（如个性化、数据隐私等）。

示例：

“在此情境下，该智能设备可能面临的主要问题包括：弱安全性（如默认密码未修改、缺乏数据加密）、远程控制的隐私泄露风险，以及设备固件更新不及时导致的漏洞。”

解决方案：

针对问题分析，提出具体、合理的解决方法。
对技术问题，结合所学知识提出具体技术手段或措施（例如加密、身份认证、模型压缩技术等）。
对用户需求，提出满足用户需求的优化方法（如个性化服务、优化用户体验等）。

示例：

“为了解决安全性问题，公司可以采取以下措施：① 强制用户更改默认密码；② 实施双因素认证；③ 使用端到端加密保障数据安全。此外，可定期进行固件更新，修补已知漏洞。”

总结与拓展：

总结解决方案的优势，并简要提到其可能带来的进一步好处。
如果适用，可以提及该技术或系统未来的优化方向（如提升用户体验或扩展功能等）。

示例：

“通过上述措施，该智能家居设备可以显著提升安全性和用户信任度，同时在未来还可以拓展为更多场景提供安全、便捷的智能服务。”

1. Lecture 07: Smart Products and Their Impact on Industry

Definition of Smart Products: Smart products integrate hardware, sensors, data storage, computing units, software, and connectivity. This integration enhances the product's capabilities and creates new applications that go beyond traditional product boundaries.

Transformation of Value Chains: The introduction of smart products disrupts traditional value chains by forcing companies to reevaluate and adjust internal processes, such as procurement, production, distribution, and service. Value chains for smart products rely heavily on data collection, analysis, and sharing capabilities, making data a critical resource.

Strategic Implications of Smart Products: Companies face strategic decisions regarding data management, relationships with traditional partners, and the expansion of industry boundaries. For example, businesses may need to determine how to use data to optimize customer relationships, provide personalized experiences, and create new revenue streams.

Technology Stack (Tech Stack): The tech stack supporting smart products includes hardware, embedded OS, network communications, a cloud platform for data storage, analytics platforms, and security frameworks. This stack also integrates with systems like ERP (Enterprise Resource Planning), PLM (Product Lifecycle Management), and CRM (Customer Relationship Management), providing a robust infrastructure for product operation and data flow.

Capabilities of Smart Products:

Monitoring: Real-time tracking of product status, performance, and environmental conditions.

Control: Remote commands or built-in algorithms allow automated device control.

Optimization: Data-driven optimizations enhance product efficiency and functionality.

Autonomy: Enables products to make decisions and take actions independently, as seen in applications like autonomous vehicles.

2. Lecture 08: Sensors and Transducers

Definition of a Sensor: A sensor detects and responds to physical inputs (such as light, heat, motion, moisture, and pressure) by producing an output signal. This signal is often converted to an electrical signal, which can then be processed for further analysis.

Role of Transducers: A transducer converts one form of energy into another without quantifying it. For instance, a light bulb converts electrical energy to light energy. Sensors, a specific type of transducer, are used to quantify inputs and measure them accurately.

Types of Sensors:

Analog vs. Digital Sensors: Analog sensors produce a continuous signal, whereas digital sensors output discrete data, usually in binary form.

Active vs. Passive Sensors: Active sensors emit signals to interact with the environment, like radar; passive sensors, such as infrared cameras, detect natural signals.

Sensor Specifications:

Accuracy: The difference between the measured value and the true value.

Resolution: The smallest detectable change in measurement.

Sensitivity: The ratio of output signal change to input physical signal change.

Dynamic Range: The ratio between the maximum and minimum values a sensor can measure.

Sensor Attributes: Additional attributes include dynamic range, linearity, transfer function, bandwidth, and noise. These factors determine a sensor's response characteristics and suitability for specific environments.

3. Lecture 09 (Part 2): IoT Security

Common IoT Vulnerabilities:

Weak or Default Passwords: Devices often ship with simple or default passwords that are easily exploitable.

Lack of Encryption: Insufficient encryption of data transmission can lead to sensitive information leaks.

Open Ports: Many IoT devices have open ports that run unnecessary or vulnerable services.

Insufficient Firmware Updates: Many manufacturers do not provide regular updates, leaving devices vulnerable to emerging threats.

Notable IoT Security Incidents:

Mirai Malware Attack: Exploited default credentials to infect IoT devices, leading to large-scale Distributed Denial of Service (DDoS) attacks.

Smart Toy Privacy Issues: Toys like CloudPets were found to lack security, allowing unauthorized users to connect via Bluetooth and potentially record audio, posing significant privacy risks.

IoT Security Objectives:

Confidentiality: Ensures that resources are protected from unauthorized access, usually through encryption and access control.

Integrity: Guarantees that data and settings are not modified maliciously.

Availability: Ensures continuous access to resources and prevents denial-of-service attacks.

Accountability: Establishes a traceable record of actions, allowing responsibility to be assigned in the event of unauthorized actions.

Security Countermeasures:

Access and Authentication Controls: Includes firewalls, secure authentication protocols, and biometric models.

Software Assurance: Ensures that software is free from vulnerabilities and operates as intended.

Security Protocols: Protect data transmission with encryption and authentication measures.

4. Lecture 10 (Part 1): Impact of Smart Products on Industry Structure

Five Forces Model: The five forces shaping competition in an industry are buyer bargaining power, supplier bargaining power, the threat of new entrants, the threat of substitutes, and competitive rivalry. Smart products alter these forces by providing enhanced features and data insights, thereby reshaping the competitive landscape.

Buyer and Supplier Bargaining Power: Smart products enable manufacturers to gather data, allowing them to optimize customer segmentation, customize products, and increase value-added services, thus enhancing their bargaining power. However, buyers also gain leverage as product usage data helps them make informed decisions, sometimes reducing reliance on manufacturers.

Barriers to Entry: High fixed costs for developing complex product designs and IT infrastructure (e.g., embedded systems) raise the barrier to entry for new competitors.

Substitution Threat: Smart products can replace traditional devices by offering superior features, such as health monitoring in fitness devices. Additionally, product-as-a-service models reduce the need for ownership, as seen in services like car-sharing and equipment rental.

5. Lecture 10 (Part 2): Tiny Machine Learning (TinyML)

Definition of TinyML: TinyML is an emerging field of machine learning designed for resource-constrained devices, such as microcontrollers, that can perform data analysis at extremely low power levels. This enables battery-operated devices to continuously run machine learning models.

Basic Concepts of Machine Learning:

Supervised Learning: Uses labeled data to train models for tasks like classification and regression.

Unsupervised Learning: Finds patterns in unlabeled data, often used for clustering and dimensionality reduction.

Reinforcement Learning: An agent interacts with its environment, receiving rewards or penalties to learn optimal actions.

Model Compression Techniques:

Pruning: Reduces the number of parameters by removing neurons or weights with minimal impact on performance.

Quantization: Lowers computational requirements by reducing the precision of weights and activations.

Knowledge Distillation: Transfers knowledge from a large, accurate model to a smaller, more efficient model, maintaining performance while reducing resource demands.

Model Evaluation Metrics: Common evaluation metrics include accuracy, precision, recall, F1 score, and the confusion matrix, which help assess the model's performance in tasks like classification.

6. Lecture 11: Ethical AI and Tiny Machine Learning

Ethics in AI: Ethical AI emphasizes trustworthiness, transparency, privacy protection, fairness, and accountability. AI systems should align with legal and ethical standards while minimizing risks to society.

Trustworthy AI: Trustworthy AI must be lawful, ethical, and robust. It should be designed to respect social values, fairness, and inclusivity while allowing human oversight. Approaches like “human-in-the-loop” ensure that AI decisions are overseen or influenced by humans.

Challenges in TinyML: TinyML faces unique challenges, such as resource limitations, model size constraints, and energy efficiency requirements. These limitations are critical when deploying AI on small devices, especially when privacy concerns demand that data processing occurs locally rather than in the cloud.

AI Evaluation Terminology: Terms like TP (True Positive), TN (True Negative), FP (False Positive), and FN (False Negative) are essential in evaluating model accuracy, error rates, and precision. Metrics like accuracy and error rate help quantify the reliability and performance of AI models.