Exam Requirement

The final exam will consist of 15 scenario-based questions, with a total of 90 marks and a duration of 2 hours. There will be no multiple-choice questions. Since these are scenario-based questions, you will need to read each scenario carefully and then provide an answer. Please give concise answers, such as using bullet points, and focus on key terms rather than lengthy explanations.

The exam will cover content taught after the midterm test, and there will be no lab-related questions.

The approximate marks distribution per topic is as following:

- Smart Products　35%
- Introduction to Sensors, Sensing principles & properties　20%
- Privacy and Security in IoT 20%
- Tiny ML 25%

Some examples of the scenario-based questions:

1. A company sells IoT-enabled household devices, such as smart refrigerators and thermostats, to consumers. These devices were rushed to market, and security was not given adequate consideration. 对应Lecture9

   What are the typical security vulnerabilities that arise in IoT devices when manufacturers focus on reducing time-to-market?

   How can consumers protect themselves against these vulnerabilities?

   让我帮你分析这个IoT设备安全问题：

   问题翻译：
   一家公司向消费者销售支持物联网的家用设备，如智能冰箱和恒温器。这些设备仓促上市，没有充分考虑安全性。

   问题1：当制造商专注于缩短上市时间时，物联网设备会出现哪些典型的安全漏洞？
   问题2：消费者如何保护自己免受这些漏洞的影响？

   典型安全漏洞(Typical Security Vulnerabilities)：

   a. 默认凭证问题(Default Credential Issues)：

   - 硬编码密码(Hardcoded passwords)

- 弱默认密码(Weak default passwords)
- 通用访问凭证(Common access credentials)

b. 加密不足(Insufficient Encryption)：

- 数据传输不加密(Unencrypted data transmission)
- 存储数据不加密(Unencrypted stored data)
- 弱加密算法(Weak encryption algorithms)

c. 更新机制问题(Update Mechanism Issues)：

- 缺乏更新机制(Lack of update mechanism)
- 不安全的更新过程(Insecure update process)
- 无安全补丁支持(No security patch support)

d. 认证和授权问题(Authentication and Authorization Issues)：

- 弱认证机制(Weak authentication)
- 缺乏访问控制(Lack of access control)
- 会话管理不当(Poor session management)

消费者保护措施(Consumer Protection Measures)：

a. 基本安全措施(Basic Security Measures)：

- 更改默认密码(Change default passwords)
- 使用强密码(Use strong passwords)
- 定期更新设备(Regular device updates)

b. 网络安全(Network Security)：

- 使用独立网络(Use separate networks)
- 启用防火墙(Enable firewalls)
- 限制设备访问(Restrict device access)

c. 监控和管理(Monitoring and Management)：

- 定期检查设备活动(Regular activity checks)
- 禁用不需要的功能(Disable unnecessary features)
- 监控网络流量(Monitor network traffic)

d. 购买决策(Purchase Decisions)：

- 选择可靠厂商(Choose reliable manufacturers)
- 查看安全评价(Check security reviews)
- 确认更新支持(Verify update support)

1. A machine learning model was developed to classify emails as spam or non-spam. Out of 2000 emails, 500 are spam. The model correctly identifies 400 spam emails and 1400 non-spam emails. It incorrectly flags 100 non-spam emails as spam and fails to detect 100 spam emails. 对应Lecture11

   What are the values of True Positive (TP), False Positive (FP)?

   Calculate the model's accuracy.

问题翻译：
开发了一个机器学习模型来将电子邮件分类为垃圾邮件或非垃圾邮件。在2000封电子邮件中，500封是垃圾邮件。该模型正确识别了400封垃圾邮件和1400封非垃圾邮件。它错误地将100封非垃圾邮件标记为垃圾邮件，并且未能检测到100封垃圾邮件。

关键术语(Key Terms)：

- True Positive (TP) - 真阳性：正确识别为垃圾邮件的数量
- False Positive (FP) - 假阳性：错误识别为垃圾邮件的数量
- Accuracy - 准确率：正确分类的总数/总样本数

解答(Solution)：

a. True Positive (TP) = 400
   - 正确识别的垃圾邮件数(correctly identified spam emails)

b. False Positive (FP) = 100
   - 错误标记为垃圾邮件的非垃圾邮件数(non-spam emails incorrectly flagged as spam)

c. Accuracy = (正确分类的总数)/(总样本数)
   - = (TP + TN)/(总样本数)
   - = (400 + 1400)/2000
   - = 1800/2000
   - = 0.9 或 90%

补充说明：
在这个例子中：

- 总样本数(Total samples) = 2000封邮件
- 实际垃圾邮件(Actual spam) = 500封
- 实际非垃圾邮件(Actual non-spam) = 1500封

Part I：Smart Products 对应内容Lecture 07 35%

1 智能产品 Smart Products的组成成分有哪些？L7 p4

传统产品主要由机械（**mechanical**）和电气（**electrical**）部件构成，较为简单；而Smart Products产品已演变为复杂（**complex**）系统，集成（**integrate**）多种技术（**technologies**）和功能（**functions**）。现代产品的主要组成部分包括：

1. **硬件 (Hardware)**：包括传统的机械和电气部件，如电机（**motors**）、电路板（**circuit boards**），作为物理基础设施（**physical infrastructure**）。
2. **传感器 (Sensors)**：能够检测温度（**temperature**）、湿度（**humidity**）、光线（**light**）和运动（**motion**）等信息。
3. **数据存储 (Data Storage)**：
4. **计算实体 (Computing Entity)**：赋予产品数据处理（**data processing**）和指令执行（**instruction execution**）的能力。
5. **软件 (Software)**：控制硬件和处理数据的核心部分，可能是操作系统（**operating systems**）或应用程序（**applications**）。
6. **连接性 (Connectivity)**：依赖网络连接（**network connections**）如Wi-Fi（**Wi-Fi**）、蓝牙（**Bluetooth**）和云服务（**cloud services**）。

2 智能互联产品的三大核心组件是什么？及其具体内容和作用是什么？P5-22

1. Physical components（物理组件）：

- 基础硬件：mechanical and electrical parts（机械和电气部件）
- 示例：car（汽车）中的 engine block（发动机座），tires（轮胎），batteries（电池）

2. Smart components（智能组件）：

- 核心技术元素：
    - sensors（传感器）
    - microprocessors（微处理器）
    - data storage（数据存储）
    - controls（控制器）
    - software（软件）
    - embedded operating system（嵌入式操作系统）

- 特点：software可以替代部分hardware，实现性能灵活调节

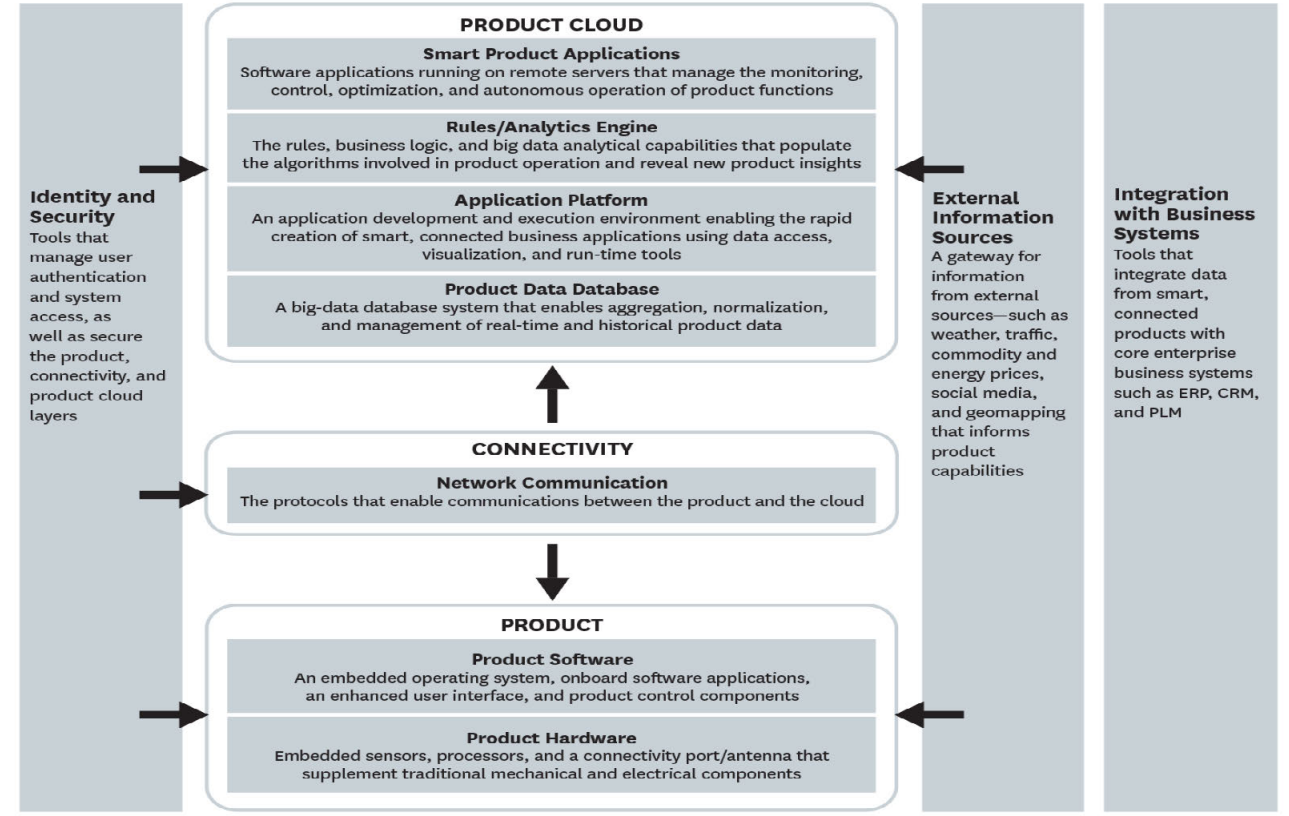
3. Connectivity components（连接组件）：

- 基础设施：
    - ports（端口）
    - antennae（天线）
    - protocols（协议）
- 三种连接模式：!!!!
    - One-to-one：单产品与单一对象连接
    - One-to-many：中央系统与多产品连接
    - Many-to-many：多产品互联及外部数据接入
- 双重功能：
    - Information exchange（信息交换）：产品与环境、制造商、用户间的数据传输
    - Cloud functionality（云功能）：通过product cloud（产品云）扩展产品功能

这三个组件形成递进关系：!!!!

- Smart components增强Physical components的能力
- Connectivity components进一步增强整体功能，并将部分功能延伸到产品物理形态之外。

3 智能产品的完整技术栈架构是什么样的？p30



核心内容可以精炼为以下层次结构（从底层到顶层）：

1. Product Hardware（产品硬件）：

- Embedded System（嵌入式系统）
- Ports（端口）
- Antenna（天线）

2. Product Software（产品软件）：

- Operating System（操作系统）
- Applications（应用程序）
- User Interface（用户界面）

3. Connectivity（连接层）：

- Network Communication（网络通信）
- Protocols（协议）

4. Product Cloud（产品云）：

- Product Data Database（产品数据库）
- Application Platform（应用平台）
- Rules/Analytics Engine（规则/分析引擎）
- Smart Product Applications（智能产品应用）

5. Integration（集成层）：

- Identity and Security（身份与安全）
- External Information Sources（外部信息源）
- Business Systems（业务系统）

这个架构图展示了：

- 智能产品各层次间的关系
- 从硬件到云服务的完整技术链路
- 系统集成的关键环节

4 智能产品的技术架构如何与企业系统集成，以及建设这样的技术架构需要什么？p31-32

1. 系统集成层面：
   所有层都通过以下系统进行访问和集成：

- Identity and security structure（身份和安全结构）
- External data gateway（外部数据网关）
- Business systems（业务系统）集成：
    - ERP (Enterprise resource planning)：
        - 跟踪：cash（现金）, raw material（原材料）, production capacity（产产能）等
    - PLM (Product lifecycle management)：
        - 管理产品从inception（构思）到disposal（处置）的整个生命周期
    - CRM (Customer relationship management)：
        - 管理与customers（客户）的关系和互动

2. 技术架构的价值：

- 支持rapid product application development（快速产品应用开发）
- 实现数据的collection（收集）, analysis（分析）, sharing（共享）

3. 建设要求：
   需要substantial investment（大量投资）和新技能：

- Software development（软件开发）
- Systems engineering（系统工程）
- Data analytics（数据分析）
- Online security（在线安全）

这些内容强调：

1. 技术架构需要与现有企业系统深度集成
2. 建设需要大量新投入和新能力
3. 这种转型对传统制造企业提出了新挑战

5 智能互联产品的四大核心能力是什么?及其具体应用？

1. Monitoring（监控能力）:

- 功能：
    - 监控产品condition（状态）, operation（运行）, environment（环境）
    - 通过sensors（传感器）和external data（外部数据）收集信息
- 应用价值：
    - 产品design（设计）优化
    - market segmentation（市场细分）
    - after-sale service（售后服务）改进
    - warranty compliance（保修合规）监控
- 应用案例：
    - Medtronic's glucose meter（血糖仪）
    - Joy Global's mining equipment（采矿设备）

2. Control（控制能力）:

- 功能：
    - 通过remote commands（远程命令）

        - 通过embedded algorithms（嵌入式算法）
    - 应用案例：
        - Philips Lighting（飞利浦照明）
        - Ring（智能门铃）

3. Optimization（优化能力）：

- 功能：
    - 提高output（产出）
    - 改善utilization（利用率）
    - 提升efficiency（效率）
- 应用案例：
    - Wind turbines（风力涡轮机）
    - Preventative maintenance（预防性维护）

4. Autonomy（自主能力）：

- 功能：
    - 自主运行
    - 环境学习
    - 自我诊断
    - 适应用户偏好
- 应用案例：
    - iRobot Roomba（扫地机器人）
    - Smart meters（智能电表）
    - Waymo（自动驾驶汽车）

这四种能力的关系：

- 是递进关系
- 从基础的监控到高级的自主运行
- 每个更高级的能力都建立在前面能力的基础上
- 最终目标是实现complete autonomy（完全自主）

应用效果：

- 提高safety（安全性）

- 适应remote locations（远程位置）
- 实现产品间coordination（协调）
- 支持system-level optimization（系统级优化）

Part II: Introduction to Sensors, Sensing principles & properties Lecture 8 20%

1 传感器的定义? 以及传感器的工作过程? p6-7

什么是传感器(Sensor)?

传感器有两个相关但更加细化的定义：

1. 基础定义：传感器是一种检测和响应(detects and responds)物理环境输入(physical environment input)的设备
2. 专业定义：传感器是一种对特定被测量(specified measurand)提供可用输出(usable output)的设备

传感器的工作过程(Process)：

1. 输入(Input)：
    - 可以检测多种物理环境现象(physical phenomena)，如：
        - 光(light)
        - 热(heat)
        - 运动(motion)
        - 湿度(moisture)
        - 压力(pressure)
        - 其他环境现象(other environmental phenomena)
2. 转换过程(Convert)：
    - 获取物理量(physical quantity)并将其转换(convert)为适合处理的信号(signal suitable for processing)
    - 信号可以是多种形式(forms)：
        - 光学(optical)
        - 电气(electrical)
        - 机械(mechanical)
    - 现代传感器主要将物理现象转换为电信号(electrical signal)

3. 输出(Output)：
    - 输出通常是一个信号(signal)
    - 这个信号有两种展现形式：
        - 在传感器位置sensor location直接转换为人类可读的显示(human-readable display)
        - 通过网络电子传输(transmitted electronically over a network)，用于读取或进一步处理(reading or further processing)

这两页内容清晰地展示了传感器的定义(definition)、工作过程(输入-转换-输出 input-convert-output)，以及现代传感器主要以电信号作为输出的特点。这为理解后续更复杂的传感器概念奠定了基础。

2 传感器(Sensor) 传感器元件(Transducer)执行器(Actuator)三个关键概念及其关系？p8-12

三个关键概念及其关系**(Key Concepts and Relationships)**：

1. **Transducer**（传感器元件）：

- 基本定义：将一种能量形式转换为另一种形式的设备(a device which converts one form of energy to another)
- 涉及能量类型(energy domains)：
    - 机械(mechanical)
    - 电气(electrical)
    - 化学(chemical)
    - 磁性(magnetic)
    - 光学(optical)
    - 热能(thermal)
- 特点：只进行转换，不进行量化(converts but does not quantify)
- 示例(examples)：
    - 灯泡：电能→光热能(electrical → light and heat)
    - 电池：化学能→电能(chemical → electrical)

2. **Sensor**（传感器）：

- 包含Transducer的系统

- 工作过程(working process)：
    - 接收信号(receiving signal)
    - 信号响应(responding to signal)
    - 转换为可读输出(converting to readable output)
- 输出类型(output types)：
    - 模拟信号(analog)
    - 数字信号(digital)
- 核心特点：量化测量(quantify measurement)
- 判断标准：物理量输入→电信号输出(physical quantity input → electrical signal output)

3. **Actuator（执行器）：**

- Transducer的另一种应用
- 判断标准：电信号输入→物理量输出(electrical signal input → physical quantity output)
- 作用：对系统施加作用(impose action on system)

关系总结**(Relationship Summary)**：

- Transducer是基础元件(basic element)，负责能量转换(energy conversion)
- Transducer分为两类(classified into)：
    - Sensor：系统监测(system monitoring)
    - Actuator：系统控制(system control)
- 区别(distinction)：能量转换方向(energy conversion direction)和是否量化(quantification)

3 传感器的三大分类体系(Sensor Classification Systems)? 按物理现象 基于工作方式 基于输出信号 p13-18

传感器分类表(Sensor Classification Table)

分类维度 (CLASSIFICATION DIMENSION)	类别 (CATEGORY)	特点 (CHARACTERISTICS)	典型例子 (EXAMPLES)
基于物理现象(Based on Physical Phenomena)	机械类 (Mechanical)	测量机械物理量(Measure mechanical quantities)	- 应变计(strain gage) - 加速度计 (accelerometer) - 压力计(pressure meter)
	热学类 (Thermal)	测量热物理量(Measure thermal quantities)	- 热电偶(thermo-couple) - 温度计 (thermometer)
	光学类 (Optical)	测量光学特性(Measure optical properties)	- 摄像头(camera) - 红外传感器(infrared sensor)
	电磁类 (Electro-magnetics)	测量电磁特性(Measure EM properties)	- 电压表(voltmeter) - 电流表(ammeter)
	化学类 (Chemical)	测量化学特性(Measure chemical properties)	- 湿度计(moisture meter) - pH计(pH meter)
基于工作方式(Based on Working Principle)	主动式(Active)	发送信号并测量交互(Send and measure signal interaction)	- 雷达(radar) - 声纳 (sonar)
	被动式 (Passive)	记录现有信号(Record existing signals)	- 摄像机(video camera) - PIR传感器 (PIR sensor)
基于输出信号(Based on Output Signal)	模拟式 (Analog)	需要A/D转换(Requires A/D conversion)	- LM35温度传感器 (LM35 temperature sensor)
	数字式 (Digital)	通过通信总线读取(Read via communication bus)	- 通过UART/SPI/I2C 接口的传感器 (Sensors with UART/SPI/I2C interface)

3 传感器规格参数？p19-28

1. 基础精度参数(Basic Accuracy Parameters)：

参数	英文	定义	补充说明
准确度	Accuracy	测量结果与真实值之间的误差(Error between result and true value)	可通过以下方式计算：绝对误差(Absolute Error) = Result – True Value；相对误差(Relative Error) = Absolute Error / True Value
分辨率	Resolution	设备可测量的最小增量(Smallest increment of measure)	与准确度不同，表示能够区分的最小变化量
重复性	Repeatability/Precision	多次测量同一输入时输出的一致性(Consistency of output for same input)	反映传感器的稳定性和可靠性

2. 响应特性参数(Response Characteristics)：

参数	英文	定义	补充说明
灵敏度	Sensitivity	输出变化与输入变化的比率(Ratio of output change to input change)	表现为输入-输出拟合线的斜率(Slope of input-output fit line)
线性度	Linearity	输出与最佳拟合直线的偏差(Deviation from best-fit line)	反映传感器响应的线性程度
动态范围	Dynamic Range	最大可测量值与最小可测量值的比 D.R. = 20 log (Max/Min) dB	表示传感器的测量范围

3. 信号特性参数(Signal Characteristics)：

参数	英文	定义	补充说明
传递函数	Transfer Function	输入信号和输出信号的关系(Relationship between input and output)	可能构成传感器特性的完整描述
带宽	Bandwidth	传感器保持线性响应的频率范围(Frequency range of linear response)	在上下限频率之间保持恒定增益
噪声	Noise	输入的随机波动导致输出的随机波动(Random fluctuations)	影响测量的准确性和可靠性

重要关系：

- 表1 Accuracy vs Resolution：p20
    - Accuracy关注测量值与真实值的接近程度
    - Resolution关注能够检测的最小变化量

- 表2 表3 Linearity vs Transfer Function：
    - Linearity是对理想线性响应的偏离程度
    - Transfer Function描述整个输入输出关系

这些规格参数构成了评估传感器性能的完整体系，帮助我们：

1. 评估测量的准确性(Evaluate measurement accuracy)
2. 了解传感器的响应特性(Understand response characteristics)
3. 选择适合特定应用的传感器(Select sensors for specific applications)

4 MEMS (Microelectromechanical Systems) 技术概述 p29-30

MEMS (Microelectromechanical Systems) 技术概述

1. **定义与国际称谓(Definition & International Names)**：

- MEMS：微机电系统(Microelectromechanical Systems)
- 核心定义(core definition)：制造和组合微型化机械与电子元件的技术实践(the practice of making and combining miniaturized mechanical and electrical components)
- 国际同义词(international synonyms)：
    - 日本：微机器(Micromachines)
    - 欧洲：微系统技术(Microsystems technology)

2. **技术特征(Technical Characteristics)**：

- 尺寸范围(Size Range)：约0.2μm到1mm
- 制造基础(Manufacturing basis)：
    - 基于IC制造技术(IC-based fabrication techniques)
    - 可扩展到非IC技术(extendable to non-IC techniques)
- 生产特点(Production features)：
    - 批量制造(batch fabrication)
    - 单个硅晶片可同时制造数千个设备(thousands of devices on a single silicon wafer)
    - 潜在低成本优势(potential low cost advantage)

3. MEMS技术特点：**系统集成能力(System Integration)**：
在芯片尺寸设备上集成多功能(integrating multiple functions on chip-size devices)：

- 传感(sensing)
- 计算(computing)
- 执行(actuating)
- 控制(control)
- 通信(communication)
- 供电(power)

4. **核心优势(Key Advantages)**：

优势类别	具体表现
制造优势(Manufacturing)	• 极高精度(very high precision) • 批量生产(batch production)
性能优势(Performance)	• 高空间功能性(high spatial functionality) • 快速响应速度(fast response speed)
微型化优势(Miniaturization)	• 改善响应速度(improved response) • 降低功耗(reduced power consumption)

5. **应用特点(Application Features)**：

- 集成度高(High Integration)：
    - 所有功能集成在芯片级别(all functions integrated at chip level)
    - 实现系统级微型化(system-level miniaturization)
- 性能优化(Performance Optimization)：
    - 通过微型化提升响应速度(improved response through miniaturization)
    - 通过集成降低功耗(reduced power consumption through integration)

5 常见传感器类型及特征总览

1. **应变计(Strain Gauge)** [第35页]

- 基本功能(Basic Functions)：
    - 形变测量(deflection measurement)
    - 应力测量(stress measurement)
    - 压力测量(pressure measurement)

- 工作原理(Working Principle)：
    - 电阻应变(resistance changes with strain)
    - 使用惠斯通电桥测量(Wheatstone bridge measurement)

2. **加速度计(Accelerometer)** [第38,42,43页]

- 测量能力(Measurement Capability)：
    - 一个或多个轴向加速度(acceleration along axes)
    - 对正交方向不敏感(insensitive to orthogonal directions)
- 主要类型(Main Types)：
    - 地震质量型(Seismic mass)：弹簧-阻尼-质量系统
    - 压电型(Piezoelectric)：晶体应力产生电压
    - 电容型(Capacitive)：微结构电容变化
    - 压阻型(Piezoresistive)：电阻变化
- 应用领域(Applications)：
    - 汽车：倾斜、防滑、碰撞监测(tilt, skid, impact monitoring)
    - 航空：导航、无人驾驶(navigation, unmanned vehicles)
    - 消费电子：手机、游戏(phones, games)
    - 工业：机械监测(machinery monitoring)

3. **温度传感器(Temperature Sensor)** [第47-50页]

- 应用特点(Application Features)：
    - 应用范围：医疗、工业、农业、汽车(medical, industrial, agricultural, automotive)
    - 精度范围：0.01°C - 10°C
- 主要类型(Major Types)：
    - 电阻温度计(resistance thermometer)
    - 热敏电阻(thermistors)
    - 热电偶(thermocouples)
    - 辐射温度计(radiation thermometers)

4. **压电传感器(Piezoelectric Sensors)** [第39-41页]

- 基本原理(Basic Principle)：
    - 压电效应(piezoelectric effect)

        - 材料：石英(quartz)、钛酸钡(barium titanate)
    - 工作模式(Working Modes)：
        - 直接效应：力→电(force to electricity)
        - 逆效应：电→力(electricity to force)
    - 优势(Advantages)：
        - 直接转换(direct conversion)
        - 智能材料(smart materials)
        - 简化设计(simplified design)

5. **电化学传感器(Electrochemical Sensors)** [第44-46页]

- 传感器类型(Sensor Types)：
    - 电导式(conductimetric)：测电阻
    - 电位式(potentiometric)：测电压
    - 电流式(amperometric)：测电流
- 测量参数(Measurement Parameters)：
    - 化学量：气体、pH值、湿度(gases, pH, humidity)
    - 生物量：葡萄糖、胆固醇、酶(glucose, cholesterol, enzymes)
- 应用领域(Application Areas)：
    - 生物医学(biomedical)
    - 环境监测(environmental monitoring)
    - 工业过程(industrial processes)

这些传感器展现了不同的物理原理(physical principles)在测量技术(measurement technology)中的应用，构成了现代传感系统(modern sensing systems)的基础。

6 传感器选择考虑因素？

传感器选择考虑因素对比表(Sensor Selection Factor Comparison)

考虑类别(CATEGORY)	具体因素(SPECIFIC FACTORS)	关注重点(KEY CONCERNS)
环境因素(Environmental Factors)	• 温度适应性(Temperature) • 湿度耐受(Humidity) • 抗干扰性(Interference) • 功耗要求(Power) • 保护特性(Protection)	• 工作环境适应能力 • 可靠运行保证 • 能源使用效率

考虑类别(CATEGORY)	具体因素(SPECIFIC FACTORS)	关注重点(KEY CONCERNS)
经济因素(Economic Factors)	• 成本(Cost) • 可用性(Availability) • 使用寿命(Lifetime) • 尺寸要求(Size)	• 总体拥有成本 • 供应链保障 • 投资回报率
性能特征(Performance)	• 灵敏度(Sensitivity) • 测量范围(Range) • 分辨率(Resolution) • 重复性(Repeatability) • 响应时间(Response Time)	• 测量准确性 • 性能稳定性 • 响应特性
系统集成(System Integration)	• 数据处理(Data Processing) • 系统兼容(Compatibility) • 环境适应(Environment)	• 数据采集通信 • 系统匹配度 • 集成便利性

选择原则(Selection Principles):

- 应用需求优先(Application Priority)
- 性价比最优(Cost-effectiveness)
- 可靠性保证(Reliability Assurance)
- 系统兼容性(System Compatibility)

Part III Privacy and Security in IoT 20% 对应内容：Lecture 9

1 导致物联网设备潜在安全漏洞的关键因素 p7

ENGLISH	中文
Profit driven businesses	利润驱动的商业模式
Time-to-market constraint	产品上市时间的限制/市场投放时间的压力
Absence of related legislation	缺乏相关法律法规
Manufacturers overlook security considerations that result in potentially vulnerable IoT devices.	制造商忽视安全考虑，导致物联网设备潜在的安全漏洞。

2 基于物联网的已知安全漏洞有哪些案例？

案例1：Mirai：

目标设备：主要针对运行Linux系统的网络设备，如摄像头、路由器、智能家居设备等。

攻击原理：

用户名和密码列表：Mirai使用一个包含超过60个常见工厂默认用户名和密码的表格来识别可被攻击的设备。这些默认凭据default credentials通常未被改变remain unchanged，使得设备容易受到攻击。

后果和影响：

- **拒绝服务攻击 Denial of Service （DoS）**：2016年10月，Mirai通过控制大量被感染的设备对美国主要的DNS提供商 provider : Dyn发起了大规模的拒绝服务攻击。这导致Dyn的服务中断，影响了多个知名网站的正常访问。
- **后续影响**：自从Mirai的源代码发布以来，许多其他恶意软件项目受其启发，采用了相似的技术，进一步扩大了网络安全威胁的范围。

案例2：CloudPet泰迪熊案例

CloudPets玩具在与手机app通信时没有使用任何标准的蓝牙安全功能 standard Bluetooth security features：

- 没有配对加密 No pairing encryption
- 任何在范围内的人都可以连接玩具
- 可以上传消息到玩具
- 可以静默触发玩具的录音功能
- 可以下载玩具录制的音频

案例3：密歇根大学研究人员交通信号灯被黑客入侵

- 密歇根大学研究人员（经当地道路管理部门许可）成功入侵了近100个无线网络连接的交通信号灯
- 发现了三个主要安全弱点：
    - 未加密的无线连接 Unencrypted wireless connections
    - 使用可在网上找到的默认用户名和密码
    - 容易受到攻击的调试端口 Vulnerable debugging ports

案例4：现代智能汽车的安全漏洞问题

攻击方式：

- 称为"放大器攻击"(amplifier attack)
- 使用便宜且容易构建的无线电放大器
- 通过改变无线电频率来欺骗无钥匙传感器技术 Deceives keyless sensor technology by altering radio frequencies

- 让车辆误以为车主和钥匙在附近

3 IoT安全技术难点 p11-12

1. 难点1：设备限制 (Device Limitations)：

- 计算能力 (Computational Capabilities)
- 存储容量 (Storage)
- 电源供应 (Power)
- 更新机制 (Update mechanism)

2. 难点2：解决方案开发障碍 (Solution Development Barriers)：

- 缺乏经验数据 (Lack of empirical data)
- 缺少攻击特征 (Lack of attack signatures)
- 协议差异性 (Protocol differences)

4 IoT漏洞有哪些？p13-18

IoT设备在不同层面的安全漏洞：

1. 设备层/物理层漏洞 (Physical Layer Vulnerabilities)：

- 物理安全不足 (Deficient physical security)
    - 可被未授权物理访问
- 能量收集不足 (Insufficient energy harvesting)
    - 能量可被攻击者耗尽 (一些IoT设备通过收集环境能量维持运行（如太阳能等），能量可被攻击者耗尽，导致设备无法执行关键功能)

2. 网络层漏洞 (Network Layer Vulnerabilities)：

- 认证不足 (Inadequate authentication)
- 加密不当 (Improper Encryption)
- 不必要的开放端口 (Unnecessary open ports)

3. 软件层漏洞 (Software Layer Vulnerabilities)：

- 访问控制不足 (Insufficient Access control)

        - 密码复杂度要求低
        - 默认凭证未强制更改
- 补丁管理不当 (Improper patch management)
        - 缺乏定期维护
        - 更新机制缺乏完整性保证
- 编程实践薄弱 (Weak programming practices)
        - 固件存在已知漏洞
- 审计机制不足 (Insufficient audit mechanisms)
        - 日志记录不完善

归纳为架构层面的漏洞分类表 (Architectural Layer Vulnerabilities)：

层级 (LAYER)	漏洞 (VULNERABILITIES)
设备层 (Device-based)	物理安全缺陷，能量收集不足
网络层 (Network-based)	认证不足，加密不当，开放端口
软件层 (Software-based)	访问控制不足，补丁管理不当，编程实践薄弱，审计不足

总结：
IoT设备存在多层次的安全漏洞（Multi-layer security vulnerabilities），从物理层到网络层再到软件层都面临不同的安全挑战。这些漏洞主要源于设计缺陷（Design flaws）、资源限制（Resource limitations）和管理不当（Poor management），需要在设备整个生命周期中采取综合性的安全措施。

5 IoT安全目标涵盖哪些维度？p19-22

IoT Security Objectives（IoT安全目标），包含四个核心安全目标：

1. Confidentiality（保密性）

- 防止未授权访问 (Unauthorized access)
- 通过访问控制 (Access control)
- 依靠认证程序 (Authentication)
- 实施加密措施 (Encryption)

2. Integrity（完整性）

- 检测未授权修改 (Unauthorized modifications)
- 使用哈希算法 (Hashing)

- 加密原语 (Cryptographic primitives)
- 接口限制 (Interface restrictions)

3. Availability（可用性）

- 确保资源及时访问 (Timely access)
- 包括数据 (Data)
- 应用程序 (Applications)
- 网络基础设施 (Network infrastructure)

4. Accountability（责任性）

- 追踪行为事件 (Tracing actions)
- 建立责任制 (Establish responsibility)
- 维护日志记录 (Logging)

核心表述：
IoT安全目标涵盖CIAA四个维度(Dimensions)，旨在保护数据机密性、确保系统完整性、维持服务可用性、建立行为追责机制(Protection mechanisms)。

6 IoT安全策略框架有哪些？

IoT Security Strategy Framework（IoT安全策略框架）

1. Protection Mechanisms（防护机制）

- Access Control（访问控制）
    - Authentication schemes（认证方案）
    - Firewalls（防火墙）
    - Biometrics（生物识别）
    - Context-aware（上下文感知）
- Software Security（软件安全）
    - Vulnerability checks（漏洞检查）
    - Function verification（功能验证）
    - Integrity assurance（完整性保证）
- Security Protocols（安全协议）
    - Lightweight designs（轻量级设计）

- Remediation plans（补救方案）

2. Awareness Systems（感知系统）

- Security Assessment（安全评估）
    - Vulnerability scanning（漏洞扫描）
    - Risk analysis（风险分析）
- Active Defense（主动防御）
    - Honeypot traps（蜜罐陷阱）
    - Attack monitoring（攻击监控）
    - Threat blocking（威胁阻断）
- Intrusion Monitoring（入侵监控）
    - Real-time detection（实时检测）
    - Behavior analysis（行为分析）

Key Features（核心特征）：

- Proactive（主动性）
- Real-time（实时性）
- Lightweight（轻量级）
- Multi-layered（多层次）

7 按攻击目标分类，IoT有哪些攻击类型？IoT Attack Types？

"IoT Attack Types"（IoT攻击类型）按攻击目标分类总结：

1. Attacks Against Confidentiality & Authentication（针对保密性和认证的攻击）

- Dictionary attacks（字典攻击）
- Brute force（暴力破解）
- Eavesdropping（窃听）
- Identity spoofing（身份欺骗）

2. Attacks Against Data Integrity（针对数据完整性的攻击）

- False Data Injection/FDI（虚假数据注入）
    - Sensor data manipulation（传感器数据操纵）
    - Economic impact（经济影响）

        - Safety risks（安全风险）
- Firmware modification（固件修改）
        - Functional disruption（功能破坏）

3. Attacks Against Availability（针对可用性的攻击）

- Denial of Service/DoS（拒绝服务）
        - Network isolation（网络隔离）
        - Resource exhaustion（资源耗尽）
- Device capture（设备捕获）
        - Physical access（物理访问）
        - Key extraction（密钥提取）
- Battery draining（电池耗尽）
        - Message flooding（消息泛洪）

核心表述：
IoT攻击类型涵盖Authentication（认证）、Integrity（完整性）和Availability（可用性）三个维度，通过Technical（技术）和Physical（物理）两种手段实施攻击，可能导致System failure（系统失效）和Security breach（安全破坏）。

Part IV Tiny ML 25%；lecture 11

1 "什么是TinyML"（What is Tiny Machine Learning）？TinyML最显著特征是什么？p22

TinyML是一个快速发展的领域（fast-growing field），它包含三个核心组成部分：

- 算法（algorithms）
- 硬件（hardware）
- 软件（software）

其最显著特征是：

1. 能够执行设备端分析（on-device sensor data analytics）
2. 极低功耗（extremely low power）
3. 功率典型在毫瓦及以下范围（mW range and below）
4. 支持电池供电设备的持续运行ML用例（battery-operated devices）

这段内容简明扼要地定义了TinyML的本质：一个将机器学习部署到低功耗终端设备的技术领域。

2 TinyML工作原理是什么？

TinyML的工作原理是一个完整的"输入-处理-输出"(Input-Process-Output)流程。在输入阶段(Input Stage)，系统通过多样化的传感器(Various Sensors)采集数据(Data Collection)，这些传感器包括运动传感器(Motion Sensors)、声学传感器(Acoustic Sensors)、环境传感器(Environmental Sensors)、图像传感器(Image Sensors)等多种类型，能够捕获不同形式的信息(Information Capture)。在处理阶段(Processing Stage)，系统采用微型计算(Tiny Computing)的方式，直接在资源受限的终端设备(Resource-Constrained Devices)上进行数据处理和分析(Data Processing and Analysis)，这与传统的大型计算(Large Computing)或云端处理(Cloud Processing)方式有明显区别。在输出阶段(Output Stage)，系统根据具体应用需求(Application Requirements)，以不同形式呈现处理结果(Processing Results)。这种端到端的处理流程(End-to-End Processing Flow)使得TinyML能够在微型设备上实现智能化功能(Intelligent Functions)。

这段话围绕：

1. 核心流程(Core Process)
2. 各阶段特点(Stage Characteristics)
3. 实现效果(Implementation Effect)

3 TinyML 的重要性？

1. 微控制器（MCU Microcontroller）的广泛应用

   MCU应用场景极其广泛。而TinyML是MCU的一种重要应用 (Application)。MCU提供了有限的资源：有限内存 (Limited Memory)、有限计算能力 (Limited Computing Power)、有限功耗 (Limited Power Consumption)。TinyML需要通过模型压缩 (Model Compression)、轻量级算法 (Lightweight Algorithms)、优化计算效率 (Optimized Computation)适应这些约束。如果能在这些MCU上运行ML,将极大扩展AI的应用范围。

2. 低成本优势 (Cheap)

- MCU价格低廉部署成本低,易于规模化推广
- 降低了AI应用的准入门槛，使得更多应用场景成为可能

3. 低功耗特性 (Ultra-low Power)

- 功率Power 在毫瓦级别 (mW range)，

- 这使得TinyML可以在电池供电设备battery-powered devices上长期运行。使得移动设备和物联网终端的AI应用成为现实

4. 处理未充分利用的数据 (Unstructured Data)

- 每天产生5 Quintillion（百万亿）字节的IoT数据
- 目前<1%的非结构化数据被分析
- 这就意味着存在大量未被充分利用的数据资源
- 重要性：TinyML可以在数据源头进行处理,充分利用这些未被挖掘的数据价值

总结：这四点从应用范围(Application Scale)、经济成本(Economic Cost)、技术可行性(Technical Feasibility)和数据价值(Data Value)等维度,全面证明了TinyML的重要战略意义。

4 TinyML的挑战？

TinyML的硬件挑战主要源于其运行载体——微控制器(Microcontroller)的固有限制。与微处理器(Microprocessor)相比，微控制器虽具有体积小(tiny size)、成本低(low cost)、功耗低(ultra-low power)的优势，但存在显著的性能差异(Order of Magnitude Difference)。主要体现在：由于微控制器架构上处理器(Processor)内存(Memory)存储器(Storage)输入输出接口(I/O interfaces) 全部集成在同一芯片上，这导致可用资源严重受限(limited resources)；功能上主要面向特定应用(specialized systems)，这导致设计灵活性有限(limited flexibility)；同时在处理能力(processing power)、存储容量(storage capacity)上与通用处理器有巨大差距。这些硬件约束(hardware constraints)直接影响着TinyML的技术路线选择(technical route)和实际应用可行性(application feasibility)，构成了其发展过程中的关键挑战(key challenges)。

TinyML在软件方面的挑战主要体现在三个层面：操作系统(Operating System)、库(Libraries)和应用(Applications)。在操作系统层面，TinyML需要使用实时操作系统Real-Time Operating System (RTOS)，这类系统需要在严格的时间约束(time constraints)下运行，采用基于事件驱动(event-driven)而时间共享(time-sharing)的任务处理机制；在库层面，最大的挑战是可移植性(Portability)问题，需要在代码通用性(code universality)和执行效率(execution efficiency)之间做出权衡；在应用层面，则需要面对资源受限(resource constraints)、实时性要求(real-time requirements)和功耗管理(power management)等问题。这些软件挑战与硬件限制相互关联，共同影响着TinyML系统的性能表现和实际应用效果。

注释：实时操作系统（RTOS）是一种用于实时计算应用的操作系统（OS），能够处理具有严格时间限制的数据和事件。RTOS与时间共享操作系统不同，后者通过调度程序、数据缓冲区或在多任务或多程序环境中固定任务优先级来管理系统资源的共享。

TinyML在机器学习方面的挑战主要体现在模型规模(Model Size)与设备资源(Device Resources)的矛盾上。从模型演进历程(Model Evolution)来看，主流机器学习模型~~(如AlexNet, VGGNet, ResNet, MobileNet)~~虽然在准确率(Accuracy)上不断提升，但模型大小(Model Size)从几十MB到数百MB不等，而典型的MCU（如Arduino Nano 33）只有256KB的RAM(Random Access Memory)，这种巨大的资源差距(Resource Gap)构成了核心挑战(Core Challenge)。为解决这一问题，主要采用三种模型压缩技术(Model Compression Techniques)：通过剪枝(Pruning)消除不重要的权重(Eliminate Unimportant Weights)，通过量化(Quantization)降低数值精度(Reduce Numerical Precision)，以及通过知识蒸馏(Knowledge Distillation)将大模型的能力迁移（transfer to）到小模型中(Transfer Learning from Large to Small Models)。这些技术都在试图解决同一个核心问题：如何在极其有限的资源约束(Limited Resource Constraints)下，保持模型的性能表现(Model Performance)。

这段话围绕：

1. 核心矛盾(Core Contradiction)
2. 具体体现(Practical Manifestation)
3. 解决方案(Solution Approaches)
4. 本质问题(Fundamental Issue)

5 对TinyML模型评估指标

1. 主要评估指标概览：

- 混淆矩阵(Confusion Matrix)

2 x 2 Confusion Matrix

WESTER AUSTRAL

		PREDICTED CLASS	
		P	N
ACTUAL CLASS	P	TRUE POSITIVE (TP)	FALSE NEGATIVE(FN)
	N	FALSE POSITIVE (FP)	TRUE NEGATIVE(TN)

分类器 Classifier

目标 Goal

ERR = (FP + FN) / (FP + FN + TP + TN) = 1 - ACC

ACC = (TP + TN)/ (FP + FN + TP + TN) = 1- ERR

- 精确率、召回率(Precision, Recall)和F1分数(F1 Score)
- 平衡准确率(Balanced Accuracy)
- ROC曲线(Receiver Operator Characteristics Curve)

2. 关键术语(Terminology)：

- 真正例(True Positive, TP): 目标存在，分类器正确识别
- 真负例(True Negative, TN): 目标不存在，分类器正确识别
- 假负例(False Negative, FN): 目标存在，分类器未识别
- 假正例(False Positive, FP): 目标不存在，分类器错误识别

3. 核心指标计算：

A. 准确率和错误率：

- 错误率(ERR) = (FP + FN)/(FP + FN + TP + TN)
- 准确率(ACC) = (TP + TN)/(FP + FN + TP + TN)

B. 关键比率：

- 真 正 例率(TPR) = TP/(TP+FN)
- 假 正 例率(FPR) = FP/(FP+TN)
- 敏感度(Sensitivity) = TPR
- 特异度(Specificity) = TN/(TN+FP)

C. 精确率和召回率：

- 精确率(Precision) = TP/(TP+FP)
- 召回率(Recall) = TP/(TP+FN)

D. F1分数：

- F1 = 2×(Precision×Recall)/(Precision+Recall)

4. 平衡准确率(Balanced Accuracy)：

- 计算：(Sensitivity + Specificity)/2
- 特点：在不平衡数据集上表现更好

5. ROC曲线：

- 作用：展示不同阈值下TPR和FPR的关系
- 评估：曲线越接近左上角，性能越好
- 衡量：通过曲线下面积(AUC)进行量化评估

这些指标共同为TinyML模型性能评估提供了全面的度量标准