边缘计算

第十二章 边缘计算

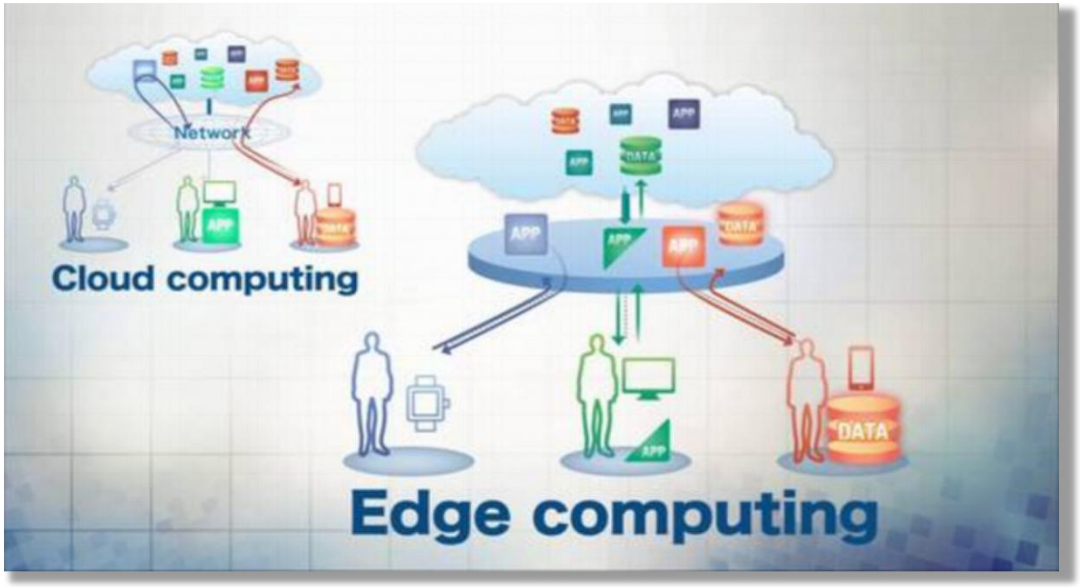
目录

12.1 边缘计算的需求与意义

- 边缘计算基本概念
- 边缘计算的产生背景
- 边缘计算的发展历史
- 小结

1.边缘计算基本概念

- 边缘计算中的“边缘”是相对的概念，是指从数据源到云计算中心路径之间的任意计算、存储和网络资源。可以把这条路径上的资源看作是一个“**连续统**”（连续统指连续不断的数集，是一个数学概念）。
- 从一端（数据源）到另一端（云中心），根据应用的具体需求和实际场景，边缘（edge）可以是这条路径上的一个或多个资源节点。



2.边缘计算的产生背景

- 思科（Cisco）于2012年12月提出“**万物互联**”的概念，这是未来互联网连接和“物联网”发展的全新网络连接架构，是在物联网基础上的新型互联的构建，增加了网络智能化处理功能和安全功能。
- **边缘计算特点：**
  - 任何“物”都将具有语境感知功能、更强的计算能力和感知能力。
  - 基于万物互联的平台应用服务可达到更短的响应时间，同时也会产生大量涉及个人隐私的数据。

3.边缘计算的发展历史

- 在边缘计算产生之前，研究者在探索如何对靠近数据的边缘设备增强数据处理的功能，即计算任务从计算中心迁移到网络边缘的研究。
- **主要典型模型包括：**
  - 分布式数据库模型
  - P2P 模型
  - CDN 模型
  - 移动边缘计算模型
  - 雾计算模型
  - 海云计算

3.1 边缘计算的典型模型

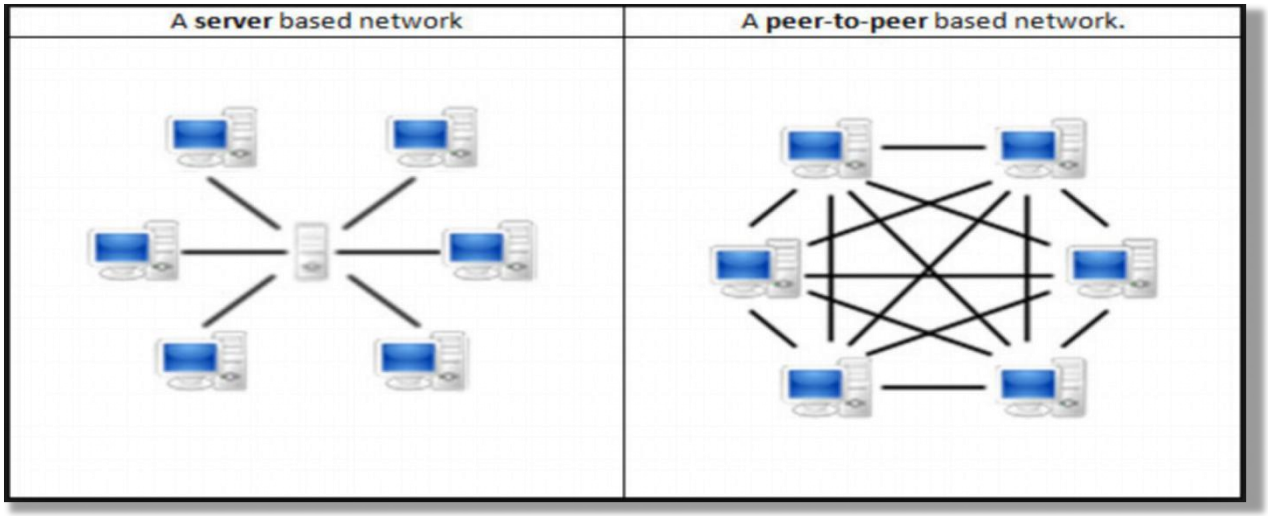
1. 分布式数据库模型

- 分布式数据库将数据存储在多台计算机上，且操作不局限于单台设备，允许在多台设备上执行事务交易，以此提高数据库访问的性能。
- **特点：**
  - 需要空间较大且数据隐私性较低，对多数据库的分布式事务处理而言，**数据的一致性技术**是分布式数据库要面临的重要挑战。
  - 较少关注设备异构计算和存储能力，主要用于实现数据的分布式存储和共享。

3.1 边缘计算的典型模型

2. 对等网络模型

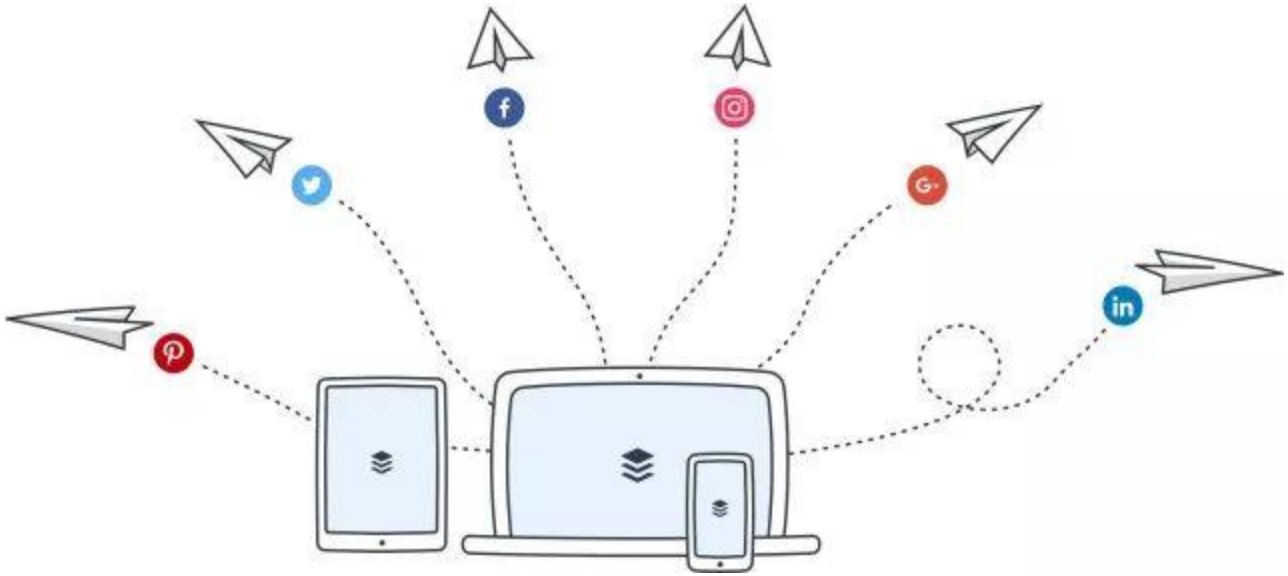
- P2P 计算（peer-to-peer computing，P2P）是较早将计算迁移到网络边缘的一种文件传输技术。
- 特点：
  - 边缘计算模式与P2P 技术具有很大程度的**相似性**，但前者对后者在新技术和新手段上进行拓展，将P2P 的概念扩展到网络边缘设备，涵盖P2P 计算和云计算的融合。



3.1 边缘计算的典型模型

3. 内容分发网络

内容分发网络（content distribution networks，CDN）通过在网络边缘部署缓存服务器来降低远程站点的数据下载延时，加速内容交付。边缘计算的概念最早可以追溯到2000 年左右内容分发网络技术(CDN)的大规模部署。



3.1 边缘计算的典型模型

4. 移动边缘计算

- 移动边缘计算（mobile edge computing，MEC）是在接近移动用户的无线接入网范围内，提供信息技术服务和云计算能力的一种新型网络结构。利用移动边缘计算，可将密集型移动计算任务迁移到附近的网络边缘服务器。
- **比较：**
  - **移动边缘计算模型**强调在边缘服务器上完成终端数据的计算任务，但移动边缘终端设备基本被认为不具有计算能力。
  - **边缘计算模型**中的终端设备具有较强的计算能力，因此，移动边缘计算类似一种边缘计算服务器的架构和层次，作为边缘计算模型的一部分。

3.1 边缘计算的典型模型

5. 雾计算

- 思科于2012 年提出雾计算（fog computing），并将雾计算定义为迁移云计算中心任务到网络边缘设备执行的一种高度虚拟化的计算平台。边缘计算和雾计算概念**具有很大的相似性**,在很多场合表示同一个意思。
- **比较：**
  - 边缘计算除了关心基础设施，也关注边缘设备，更强调边缘智能的设计和实现。
  - 雾计算更关注后端分布式共享资源的管理。

3.1 边缘计算的典型模型

6. 海云计算

- 中国科学院于2012年开展“海云计算系统项目”的研究，通过“云计算”系统与“海计算”系统的协同和集成，增强传统云计算能力，其中，“海”端指由人类本身、物理世界的设备和子系统组成的终端（客

4. 小结

- 本节介绍了边缘计算是一个**连续统**，边缘计算的边缘是指从数据源到云计算中心路径之间的任意计算、存储和网络资源。讨论大数据处理和万物互联的发展和挑战，有助于理解边缘计算这一新型计算模式的产生背景。

- 本节同时回顾了分布式数据库、P2P、内容分发网络、移动边缘计算、雾计算、海云计算等面向数据的计算模型的发展历史，介绍了边缘计算的发展现状。

12.2 边缘计算基础

- 分布式计算
- 边缘计算的基本概念
- 边缘计算的关键技术
- 边缘计算与云计算
- 边缘计算与大数据
- 小结

1.分布式计算

- 分布式计算是通过互联网将许多计算机节点互联，将单台计算机无法完成的计算任务，分解成多个任务分配到网络中多个计算机执行，将各个节点的执行结果整合成最终结果并返回，即是指在分布式系统上执行的计算。
- 分布式计算技术主要包括：
  - 中间件技术
  - 网格计算技术
  - 移动Agent技术
  - P2P计算
  - Web Service 技术

1.边缘计算技术

1.中间件技术

- 中间件是一种处于操作系统和分布式应用软件的中间层的软件技术，用于屏蔽分布环境中操作系统与网络协议的异构性。IBM 在20 世纪60 年代实现了具有中间件功能的客户信息控制系统（customer information control system，CICS）
- 技术细分：
  - 基于远程过程调用的中间件
  - 面向消息的中间件数据库中间件
  - 面向对象的中间件（主流）

1.边缘计算技术

2.网格计算技术

- 网格计算是通过高速网络整合地理上分散的软硬件资源，完成大规模复杂计算和数据处理的任务。
- **网格技术应用的两类模式：**
  - 基于分布式计算资源支持作为服务，提供在线计算或存储支持。
  - 由松散连接的计算机网络构成的一个用来执行大规模计算任务的虚拟超级计算机。

1.边缘计算技术

3.移动Agent技术

- 移动Agent 可以在异构网络和分布式计算环境中自主、自动地迁移，并与其他Agent 相互通信。
- 在不同网络结构中，移动Agent 遵循一定的原则，寻找匹配的资源信息，取代客户来完成任务，根据需要自主生成子Agent。
- 移动Agent 系统中，每个Agent 独立工作，在需要的时候可以协作完成任务。

1.边缘计算技术

4.P2P技术

- 通过将网络中的终端设备串联，整合网络中的空闲资源，最大程度地实现资源共享、分布式计算。
- 在P2P 网络中的每个节点贡献空闲资源，并利用资源定位机制发现其他节点的可用资源，进行彼此的资源共享。P2P技术能够最大化地利用网络资源。
- 特点：
  - 开放性、自组织性、自治性、分布性

1.边缘计算技术

5.Web Services技术

- 是对象/组件技术在互联网中的延伸，是部署在Web 上的对象/组件的一种分布式计算技术。
- **Web Services 技术：**
  - 主要目标：现有的众多异构平台基础上，构建一个与平台、语言无关的通用技术层，不同平台上的应用程序可以依靠该技术顺利运行。
  - 技术目的：解决互操作性有限的问题，从而改善并扩展分布式计算的功能。

2.边缘计算的基本概念

- 在万物互联的时代，万物互联不仅包括物联网环境下的“物”与“物”之间互联，还包括具有语境感知的功能、更强的计算能力和感知能力的“人”与“物”的互联。

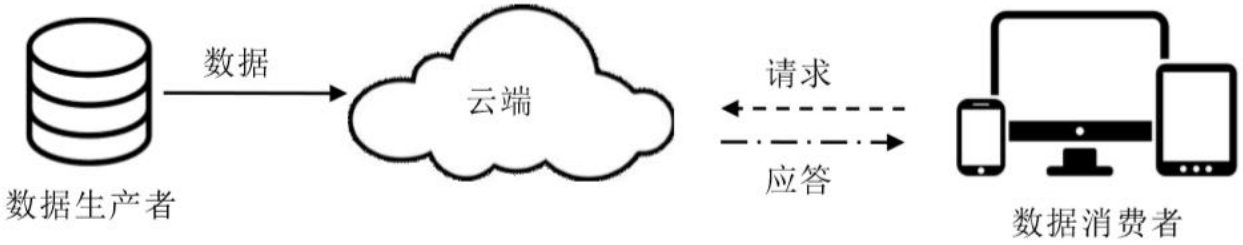


图*-* 所示为传统云计算模型

2.1 传统云计算模型的限制

- 万物互联环境下，传统云计算模型不能有效满足万物互联应用的需求，其主要原因有：
  - 直接将边缘设备端海量数据发送到云端，造成网络带宽负载和计算资源浪费。
  - 传统云计算模型的隐私保护问题将成为万物互联架构中云计算模型所面临的重要挑战。
  - 万物互联架构中大多数边缘设备节点的能源是有限的，而GSM、WiFi 等无线传输模块的能耗较大。

2.2 边缘计算的优势

- 利用边缘设备已具有的计算能力，将应用服务程序的全部或部分计算任务从云中心迁移到边缘设备端执行，这将有利于降低能源消耗，同时也可生产数据。
- 在源数据上传至云中心之前，在边缘设备执行预处理，以减少传输的数据量，降低传输带宽的负载。在边缘设备处理个人身体健康数据等隐私数据，用户隐私会得到更好地保护。

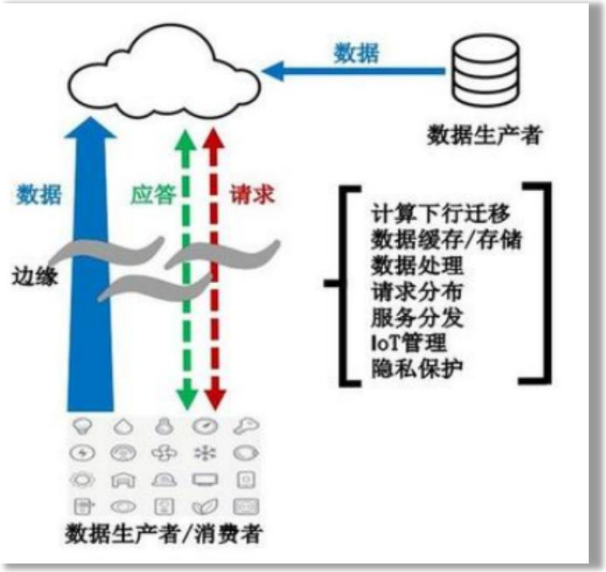


图*-* 所示为边缘计算模型

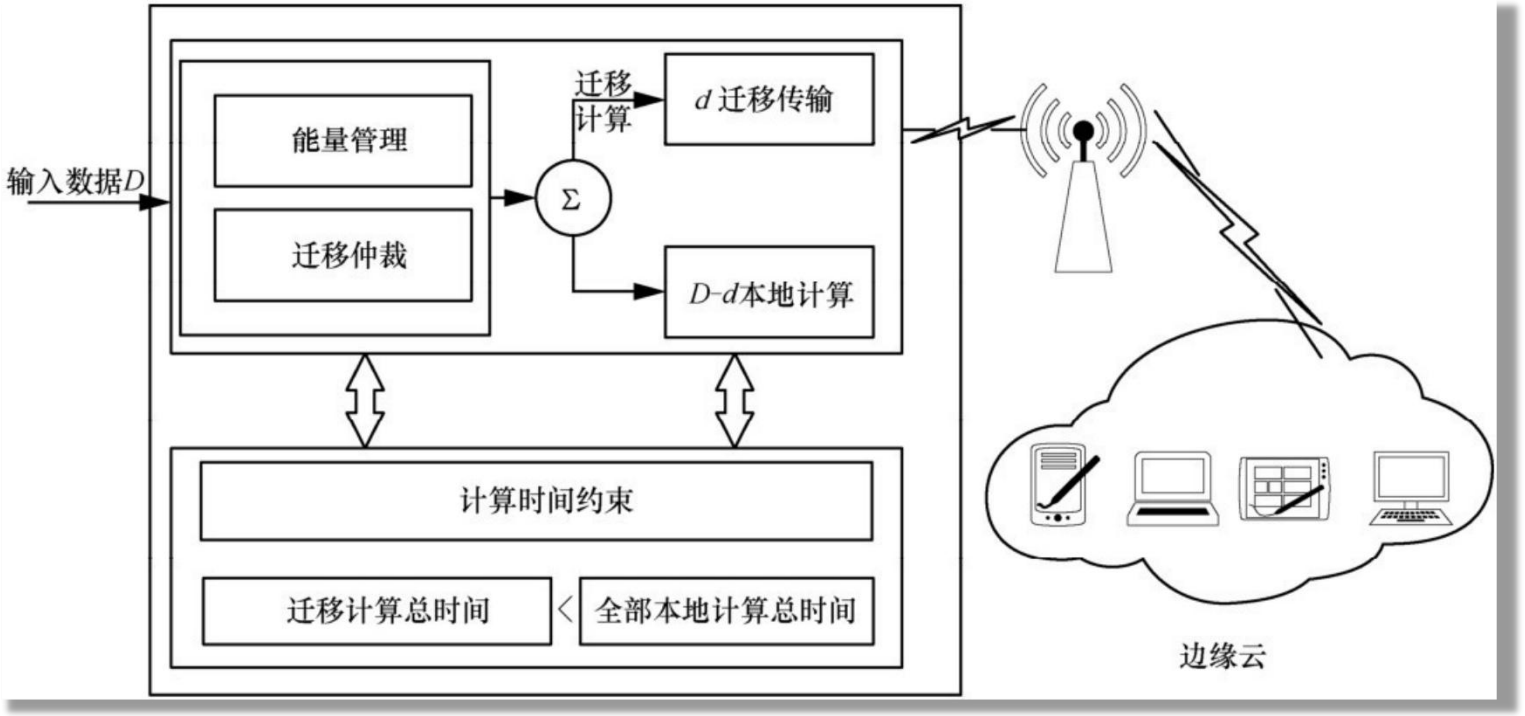
3.边缘计算的关键技术

- **边缘计算的关键技术主要包括：**
  - 计算迁移
  - 5G通信技术
  - 新型存储系统
  - 轻量级函数库和内核
  - 边缘计算编程模型

3.边缘计算的关键技术

1. 计算迁移

- 云计算模型中，计算迁移的策略是将计算密集型任务迁移到资源充足的云计算中心的设备中执行。



3.边缘计算的关键技术

1. 计算迁移

- 边缘计算中的计算迁移策略是在网络边缘处，将海量边缘设备采集或产生的数据进行部分或全部计算的预处理操作，过滤无用数据，降低传输带宽。
- 根据边缘设备的当前计算力进行动态的任务划分。
- 计算迁移中的重要问题：
  - 任务是否可以迁移、按照何种决策迁移、迁移哪些任务、执行部分迁移还是全部迁移等。

3.边缘计算的关键技术

2. 5G 通信技术

- 为了满足各种延时敏感应用的需求，世界各国正在加快部署5G 网络的步伐。提供10Gps以上的峰值速率、更佳的移动性能、毫秒级时延和超高密度连接。
- **5G 业务的三个技术场景：**
  - 增强移动宽带（eMBB）：面向虚拟现实/增强现实等极高带宽需求。
  - 海量机器类通信（mMTC）：面向智能交通等高连接密度需求。
  - 超可靠低时延通信（uRLLC）：面向无人驾驶、无人机等时延敏感的业务。

3.边缘计算的关键技术

3. 新型存储系统

- 边缘计算在数据存储和处理方面具有较强的实时性需求，相比现有嵌入式存储系统而言，边缘计算存储系统更具有低延迟、大容量、高可靠性等特点。数据特征具有更高的时效性、多样性和关联性。
- 非易失存储介质（non-volatile memory，NVM）能够较好地改善现有存储系统I/O 受限的问题。传统的存储系统软件栈大多是针对机械 硬盘设计开发，并没有真正挖掘和充分利用非易失性存储介质的最大性能。

3.边缘计算的关键技术

4. 轻量级函数库和内核

- 边缘设备由于硬件资源的限制，难以支持大型软件的运行。
- 由不同厂家设计生产的海量边缘设备，具有较强的异构性且性能参数差别较大，在边缘设备上部署应用非常困难。
- 基于VM 的虚拟化技术是一种重量级的库，部署延时较大，不适用于边缘计算模型。
- 资源受限的边缘设备更加需要轻量级库和内核的支持，消耗更少的资源及时间，达到最好的性能。

4.边缘计算与云计算

- 云计算特点：1.云服务器规模庞大;2.高可靠性;3.可拓展性;4.虚拟化
- 边缘计算是对云计算的补充和延伸，为移动计算、物联网等提供更好的计算平台。
  - 边缘计算模型需要云计算中心的强大计算能力和海量存储的支持。
  - 云计算也同样需要边缘计算中边缘设备对于海量数据及隐私数据的处理，从而满足实时性、隐私保护和降低能耗等需求。

比较内容	边缘计算	云计算
目标应用	物联网或移动应用	一般互联网应用
服务器节点的位置	边缘网络(网关、wifi接入点和蜂窝基站等)	数据中心
客户端与服务器的通信网络	无线局域网，4G/5G等	广域网
可服务的设备(用户)数量	数十亿计	数百万计
提供的服务类型	基于本地信息的服务	基于全局信息的服务

5.边缘计算与大数据

边缘计算与云计算技术的融合

- 边缘计算与云计算关键技术是解决大数据的存储、传输和处理等重要问题的主要方法之一。
  - 利用边缘计算和云计算的优势以达到大数据处理任务分配均衡、大数据传输带宽需求和存储空间需求优化。
- 公共安全领域内的视频大数据和智能健康领域内的医疗大数据对存储、传输和计算的实时性需求较大。
  - 实时性检测需求场景下，利用医疗大数据的价值为智能医疗进行服务，多边缘端协同数据处理。

5.边缘计算与大数据

医疗大数据处理中需要解决的问题

- 在医疗大数据的处理中需要解决的问题：如何利用边缘计算技术在处理边缘敏感隐私数据的同时，实现共享医疗大数据，从而实现其根本价值。视频大数据处理的实时性较低，这直接影响公共安全领域对突发事件的判定和决策。

6. 小结

- 本节首先介绍分布式计算技术，然后给出基于双向计算流的边缘计算模型，阐述构建一个边缘计算系统涉及的关键技术，包括计算迁移、 5G 通信技术、新型存储系统、轻量级函数库和内核、边缘计算编程模型等。

- **边缘计算与云计算的关系：**

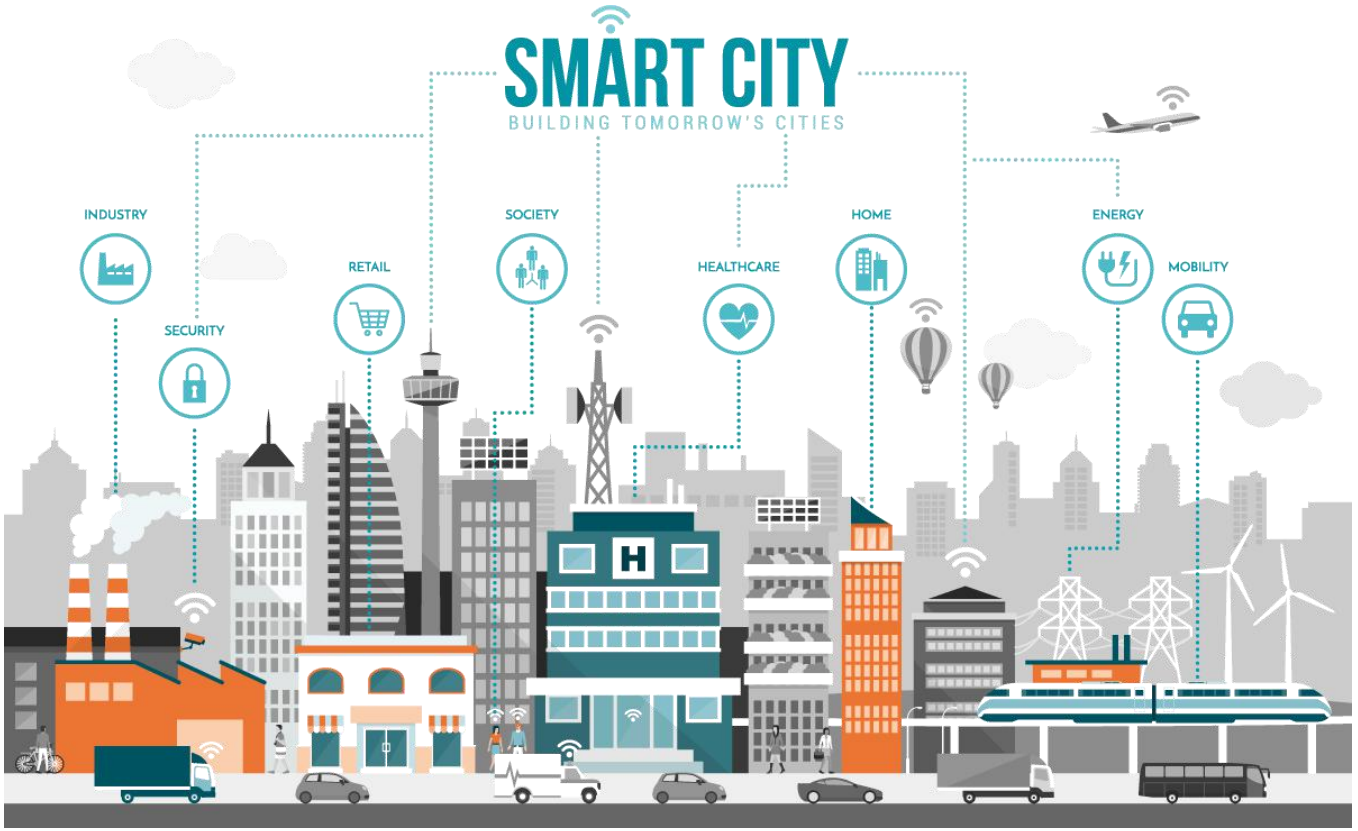
边缘计算并不是为了取代云计算，而是对云计算的补充和延伸，两者是相辅相成、相映生辉的关系。而边缘计算与云计算相结合，将更加有效地解决大数据处理所面临的问题。最后探讨边缘计算自身的优势，以及在应用、架构、能力与服务、边缘计算理论等方面面临的主要挑战

12.3 边缘计算典型应用

- 典型应用介绍
- 协同边缘
- 云计算任务前置
- 边缘计算视频监控系统
- 小结

1.典型应用介绍——智慧城市

- 未来智慧城市的基础设施建设将进一步呈现物联网化。其中边缘计算可作为智慧城市中一种较理想的平台。



1.典型应用介绍——智慧城市

边缘计算用于智慧城市的优势：

- **大数据量：**
  - 云计算模型对海量数据会引起较重传输带宽负载和较长传输延时。在网络边缘设备进行数据处理将是一种高效的解决方案。
- **低延时：**
  - 边缘计算模型可以降低数据传输时间，简化网络结构。
- **位置识别：**
  - 基于地理位置可进行数据实时处理和收集，而不必传送到云计算中心。

1.典型应用介绍——智能家居

- 智能家居设备涉及范围不断扩大，对设备联动场景的要求加大。其中边缘计算可作为智能家居系统的平台。

1.典型应用介绍——智能家居

边缘计算用于智能家居的优势：

- **大数据量：**
  - 利用边缘计算平台，视频等各种数据在本地可得到筛选、处理。
- **低延时：**
  - 边缘计算避免有限的网络带宽对数据传输的影响，系统能够更高效地收集、分析数据并作出相应的反馈 (eg.开关灯、查看监控摄像头)。
- **隐私保护：**
  - 将数据的传输和使用控制在家庭范围内，将敏感信息从源数据中剥离，是对用户隐私的一种保护措施。

2.协同边缘

- 协同边缘是连接多个数据拥有者的边缘，这些数据拥有者在地理上是分布的，但具有各自的物理位置和网络结构。类似于点对点的边缘连接方式，在数据拥有者之间提供数据的共享。
- **协同边缘方案：**
  - 移动目标识别框架 deep chameleon
  - 分布式神经网络框架 DDNN
  - FLARE 架构

3.云计算任务前置

基于边缘加速的网页平台

- 根据用户设备的环境可确定数据分配和传输方法，基于边缘加速的网页平台模型（edge accelerated web platform，EAWP）改善传统云计算模式下较长响应时间的问题。
- 购物车数据可被缓存在边缘节点，相关的操作可在边缘节点上执行。当用户的请求到达边缘节点时，新购物车视图立即推送到用户设备。边缘节点与云中心的数据同步可在后台进行。
- 在移动视频转码应用中，端部署中具有有限性；无线信道易不稳定。这些因素导致用户体验较差。

3.云计算任务前置

移动视频转码存在的问题及解决方案

- 在移动视频转码应用中，端部署中具有有限性；无线信道易不稳定。这些因素导致用户体验较差。
- 一些改善视频传输的方法，如自适应比特率流、可伸缩视频编码（SVC）、渐进式下载等，视频转码已成为视频数据传输的一种优化技术。
- Jongwon Yoon等提出一种在无线边缘运行低成本的视频转码解决方案，具有如下优点：
  - 透明性、低成本和可扩展性

4.边缘计算视频监控系统

城市安全视频监控系统

- 城市安全视频监控系统主要应对因万物互联的广泛应用而引起的新型犯罪及社会管理等公共安全问题。
- 首先，构建一种基于边缘计算的视频图像预处理技术。
- 其次，为了降低上传的视频数据，基于边缘预处理功能，构建基于行为感知的视频监控数据弹性存储机制。

12.4 边缘计算安全与隐私保护

- 安全概述
- 安全威胁及挑战
- 主要安全技术
- 边缘计算与物联网安全
- 边缘计算安全实例
- 小结

1.安全概述

边缘计算面临挑战

- 边缘计算作为一种新兴事物，面临着许多的挑战，特别是安全和隐私保护方面。

边缘计算存在安全问题

- 应用安全 拒绝服务攻击、越权访问、软件漏洞、权限滥用等。
- 网络安全 恶意代码入侵、缓冲区溢出、窃取、篡改、伪造数据等。
- 信息安全 数据丢失或泄露、数据库破解、备份失效等。
- 系统安全 计算机硬件损坏、操作系统漏洞、恶意内部人员等。

2.安全威胁及挑战

边缘计算面临挑战

- 边缘计算安全威胁分析，主要分为物理安全、网络安全、数据安全和应用安全。

2.安全威胁及挑战

2.1 物理安全问题

- 由于边缘计算设备不再像云计算中心那样，在具备安全措施的固定场所中运行，而是大多在对外开放且不受控制的环境中运行（如地铁、隧道、工厂等），物理设备位置不安全，并且相对于物联网终端设备，边缘计算设备数据具有更高的价值。因此，基础设施更容易受到攻击。
- 自然灾害带来的威胁主要是指自然界中的不可抗力所造成的设备损毁、链路故障等使边缘计算服务部分或完全中断的情况。
- 运行威胁主要是指在边缘计算设备运行过程中，由间接或自身原因导致的安全问题，如能源供应、冷却除尘、设备损耗等。

2.安全威胁及挑战

2.2 网络安全问题

- 边缘设备具有对数据分析处理的能力，并且位于开放的环境中，不确定因素大大增加，已有的固定网络和移动网络远远不能满足需要，网络的吞吐量、普适性等都将出现质的变化。
- DDoS攻击：边缘计算网络下的DDos 攻击有两种形式：一种是针对边缘数据中心，一种是针对终端。
- 典型的蜂窝设备支持2G、3G 和4G 网络，并在存在多个可用网络的情况下，倾向于选择具有最高信号强度的网络，这允许未经授权的第三方建立自己的高信号强度2G伪基站，附近的客户可能会附加到伪基站。

2.安全威胁及挑战

2.3 数据安全问题

- 边缘计算设备部署的应用属于不同的应用服务商，接入网络属于不同的运营商，导致边缘计算中多安全域共存，多种格式数据并存。在这种环境下如何保证数据的安全存储和处理成为影响边缘计算安全的重要威胁。
- 边缘计算设备位于靠近数据源的网络边缘侧，相对于位于核心网络中的云计算数据中心可以收集更多用户高价值的敏感信息，包括位置信息、生活习惯、社交关系等。

2.安全威胁及挑战

2.4 应用安全

- 在多种安全域和接入网络共存的情况下，如何对用户身份进行管理和实现资源的授权访问。
- **安全策略：**
  - 用户要求边缘计算服务提供商能够在多租户环境下提供访问控制功能。
  - 其次，访问控制应支持用户基本信息和策略信息的远程提供，还应支持访问控制信息的定期更新。
  - 最后，对于高分布式数据的访问本身就是一个重要的挑战。

3.主要安全技术

3.1 身份认证

- 基于口令的认证是最简单也是最常用的身份认证方法，而许多用户经常采用诸如自己或家人的生日、电话号码等，极易造成密码泄露。
- IC 卡是一种内置集成电路的卡片，卡片中存有与用户身份相关的数据，可以认为是不可复制的硬件。
- 动态口令技术是一种让用户的密码按照时间或使用次数不断动态变化，每个密码只使用一次的技术。
- 生物特征认证是指采用每个人独一无二的生物特征来验证用户身份的技术。不同的人具有相同生物特征的可能性可以忽略不计，因此几乎不可能被仿冒。

3.主要安全技术

3.2 访问控制

- 访问控制可以限制用户对应用和关键资源的访问，防止非法用户进入系统及合法用户对系统资源的非法使用。
  - **基于角色的访问控制模型**：权限和角色相关，角色是实现访问控制策略的基本语义实体。
  - **基于属性的访问控制**：根据相关实体属性的动态变化，适时更新访问控制决策
  - **基于任务的访问控制**：以任务为中心的，并采用动态授权
  - **基于对象的访问控制**：将访问控制列表与受控对象相关联，同时允许策略和规则进行重用、继承和派生操作

3.主要安全技术

3.3 入侵检测

入侵检测通常包括检测、分析、响应和协同等一系列功能，能够发现系统内未授权的网络行为或异常现象，收集违反安全策略的行为并进行统计汇总，从而支持审计分析和统一安全管理决策。

- **误用检测技术：**
  - 根据网络攻击行为和方法建立一个入侵信息库，那么IDS（入侵检测系统），将捕获到的网络行为特征与入侵规则库中的特征信息进行比较
- **异常检测技术：**
  - 是指根据用户的行为和系统资源的使用状况来判断是否存在网络攻击。

3.主要安全技术

3.4 隐私保护

隐私保护技术大体可以分为基于数据失真、基于数据加密和基于限制发布三类技术。

- **数据失真技术：**通过扰动（perturbation）原始数据来实现隐私保护
- **基于数据加密技术：**采用加密技术在数据挖掘过程中隐藏敏感数据的方法，具体应用通常会依赖于数据的存储模式和站点的可信度及其行为。
- **限制发布：**即有选择地发布原始数据、不发布或者发布精度较低的敏感数据，以实现隐私保护。

3.主要安全技术

3.5 可信执行

- 可信执行环境是指在不可信的设备上一个独立于不可信操作系统而存在的可信的、隔离的、独立的执行环境。
- 基于内存加密实现的可信执行环境，一般采用直接在应用层进行隔离，它的权限级别 为ring-3，主要支持两种硬件技术：Intel软件防护扩展和AMD 内存加密技术。
- Intel系统管理模式和ARM TrustZone 技术都采用限制内存访问的方式来创建可信执行环境。

3.主要安全技术

3.6 多方计算

- 安全多方计算的主要目的是解决一组互不信任的参与方之间保护隐私的协同计算问题。
- 安全多方计算的研究主要集中在普适安全性、公平性、效率以及量子构造等几方面。安全多方计算的特性使其可以运用在边缘计算环境中保护用户数据安全和个人隐私。

4.边缘计算与物联网安全

4.1 隐私保护

- 引入边缘计算，物联网设备可以将数据保存在本地边缘计算设备上，边缘计算设备具备充足的资源执行隐私保护算法，有效保护传递给云端的数据隐私。

4.2 态势感知

- 边缘计算模式下，借助边缘计算中心，通过网络内设备的日志、警报等，对整个局域网的安全状况进行分析和评估。
- 边缘计算中心之间互相协作，建立分布式的网络感知平台。

4.边缘计算与物联网安全

4.3 设备更新

- 保证在没有互联网的情况下，用户能快速稳定的进行设备升级，及时安装安全补丁。
- 边缘设备定期对内网设备状态进行检测，将检测结果上传到云端进行分析，及时发现可能的安全漏洞和威胁。

4.4 安全协议

- 互联网中的安全协议 IPSec、TLS 等涉及大量的公钥运算，可以使用协议代理、证书托管的方式，协助物联网中的资源受限设备执行安全协议。

5.边缘计算安全实例

5.1 数据保护模型

- 针对边缘计算中的数据保护和性能问题的方案：
  - 基于区域的信任感 （RBTA）模型，用作区域边缘节点之间的信任转换；
  - 引入基于边缘的隐私感知角色访问控制（FPRBAC），用于边缘节点的访问控制；
  - 开发移动管理服务，以处理用户和边缘设备位置的变化。

5.边缘计算安全实例

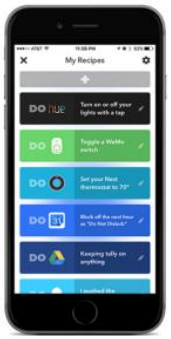
5.2 海豚音攻击

- 通过利用超声波传声器的非线性来对现代智能手机注入语音命令。通过利用麦克风电路的非线性，调制的低频音频命令可以被语音识别系统成功地解调、恢复。

5.边缘计算安全实例

5.3 ContextIoT

- 一种基于边缘计算的权限访问系统——ContextIoT，在本地边缘计算平台上，通过支持敏感操作的细粒度上下文识别提供上下文完整性，帮助用户执行有效的访问控制，抵抗现有常见的恶意软件攻击，提高边缘计算平台的安全性。



1 Light switch(4)
2 Door lock
3 Presence sensor(2)
4 Motion sensor(3)
5 Contact sensor
6 Temp. measure.
7 AC
8 Heater
9 Coffee machine
10 Crockpot
11 Leak detector(2)
12 Fan
13 Power meter
14 Alarm(2)
15 Smoke detector(2)
16 Humidity sensor
17 Luminance sensor
18 Speakers
19 Window shade
20 Doorbell

5.边缘计算安全实例

5.3 Octopus

- Octopus 是基于边缘计算的物联网安全认证方案，是第一个在端—边缘—云网络体系架构下，实现边缘网络中终端和边缘服务器之间的安全相互认证。

6. 小结

- 边缘设备威胁：由于更靠近网络边缘侧，网络环境更加复杂，并且边缘设备对于终端具有较高的控制权限，导致其在提高万物互联网络中数据传输和处理效率的同时，不可避免地带来一些安全与隐私威胁。

- 对边缘计算进行全方位的安全防护。保证边缘计算系统提供服务的安全性和系统自身的安全性，是需要达到的目标。为此，需要清晰的认识边缘计算安全框架和业务流程，设计安全的边缘计算架构，对边缘计算进行全方位的安全防护。

Quiz One

- 用自己的语言回答：什么是边缘计算、云计算、雾计算？

Quiz Two

- 为什么边缘计算中数据库是很重要的？