物联网安全
Internet of Things Security

USLAB

专题三 边缘计算安全

冀晓宇
浙江大学

传统计算模式

- **本地计算：**按照一定规则（如特定指令集）对输入数据进行加减乘除等数学运算，然后输出结果。这中间产生的数据存储在本地计算机的内存或硬盘中

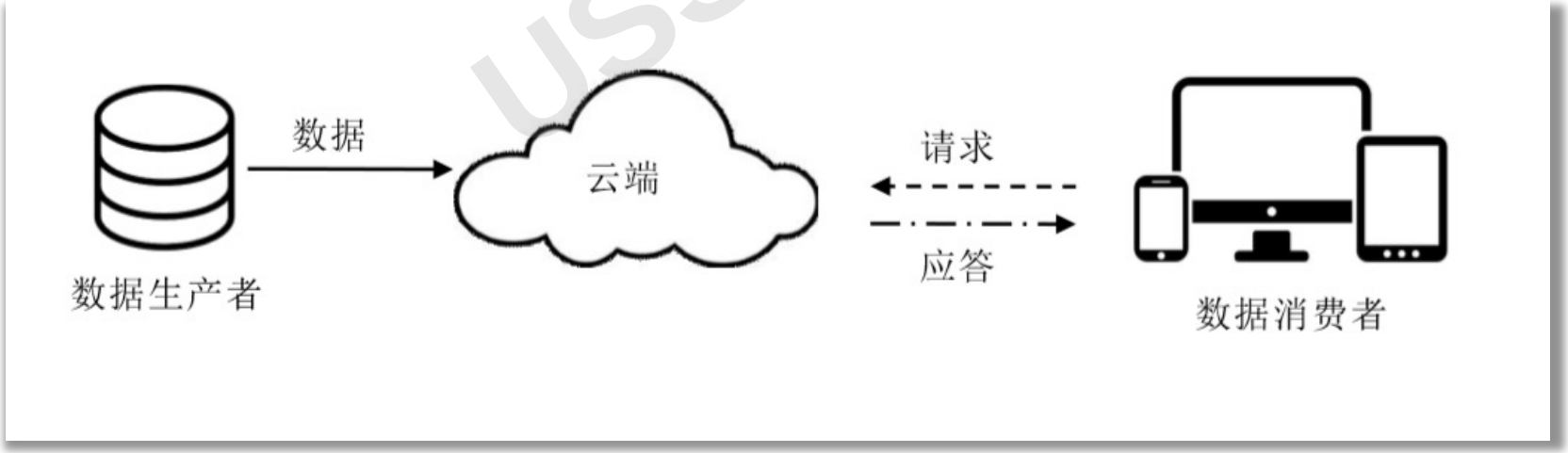
- **特点：**基于大量硬件设备（服务器、存储等）、软件（数据库、中间件等），借助运维团队支持设备和软件的正常运作

- **缺点：**需要组建运维团队支持设备或软件的正常运作，包括安装、配置、测试、运行、升级以及保证系统安全等。其费用对于中小规模的企业是难以承受

USS LAB

云计算模式

- **定义：**是一种基于互联网的计算方式，通过这种方式，共享的软硬件资源和信息可以按需求提供给计算机各种终端和其他设备，使用服务商提供的电脑基建作计算和资源。具有低成本、高效率、开放性和扩展性的优点。



USSLAB

云计算是计算模式发展的终点吗?

USSLAB

传统云计算模型的限制

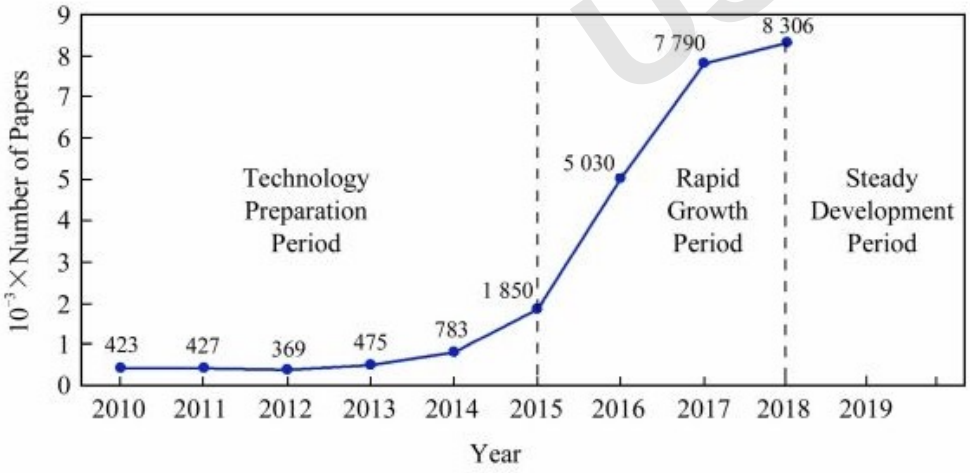
- 万物互联环境下，传统云计算模型不能有效满足万物互联应用的需求，其主要原因有什么？
  - **实时性问题**：数据上传云端再返回延迟大
  - **带宽问题**：直接将边缘设备端海量数据发送到云端，造成网络带宽负载和计算资源浪费
  - **数据隐私**：传统云计算模型的隐私保护问题将成为万物互联架构中云计算模型所面临的重要挑战
  - **成本问题**：海量数据的传输、处理和存储带来巨大成本

- 物联网时代下，上述问题将更加恶化！

USSLAB

边缘计算

- 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
- 2016年，边缘计算爆发



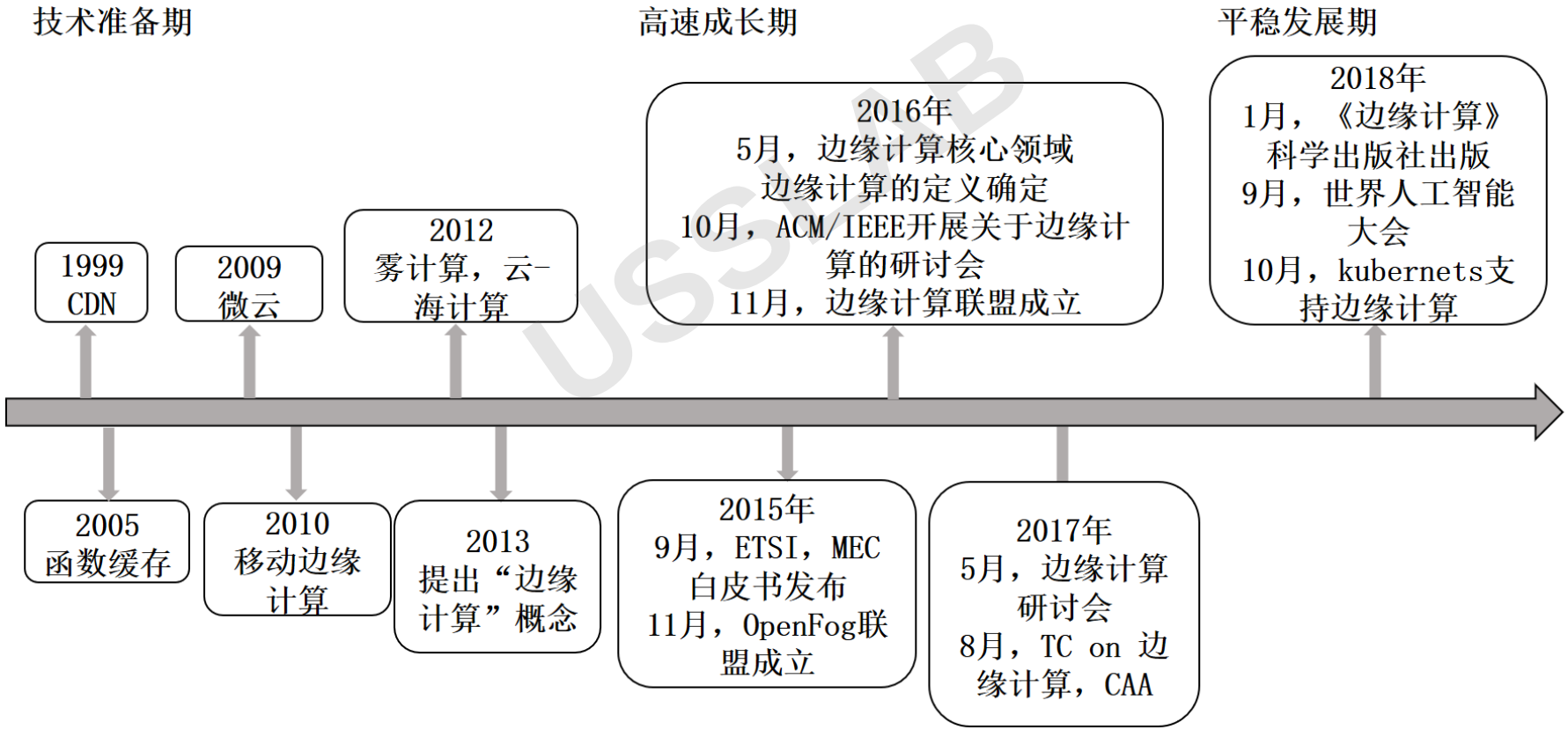
码	名称	最新	涨幅%	总市值
K0860	边缘计算	1145.18	6.13	6425亿
00971	高升控股	5.01	10.11	54.5亿
00851	高鸿股份	7.22	10.06	65.5亿
00711	京蓝科技	8.00	10.04	81.9亿
00017	网宿科技	14.29	10.01	348亿
00353	东土科技	13.86	10.00	71.6亿
00213	佳讯飞鸿	9.02	10.00	53.7亿
00977	浪潮信息	27.60	10.00	356亿
00175	朗源股份	6.84	9.97	32.2亿
00370	安控科技	4.33	9.90	41.5亿

A股中和边缘计算的涨停股

USSLAB

发展历史

- **研究发展：**技术准备期、高速成长期、平稳发展期



边缘计算发展历史

边缘计算定义

- **定义：**边缘计算指在**网络边缘**执行计算的一种新型计算模式。
- 边缘计算和面向数据的计算模型是分不开，解决数据传输、计算和存储过程中的计算负载、数据传输带宽、隐私保护等问题
- 具体对数据的计算包括：上行的云服务和下行的万物互联服务

SSSLAB

边缘计算的几个核心概念

- **边缘**：是个相对的概念，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
  - 终端：手机、电脑、摄像头、机顶盒、网联汽车、电网终端设备
  - 也可是WiFi接入点、路由器、蜂窝基站等，又称为边缘服务器

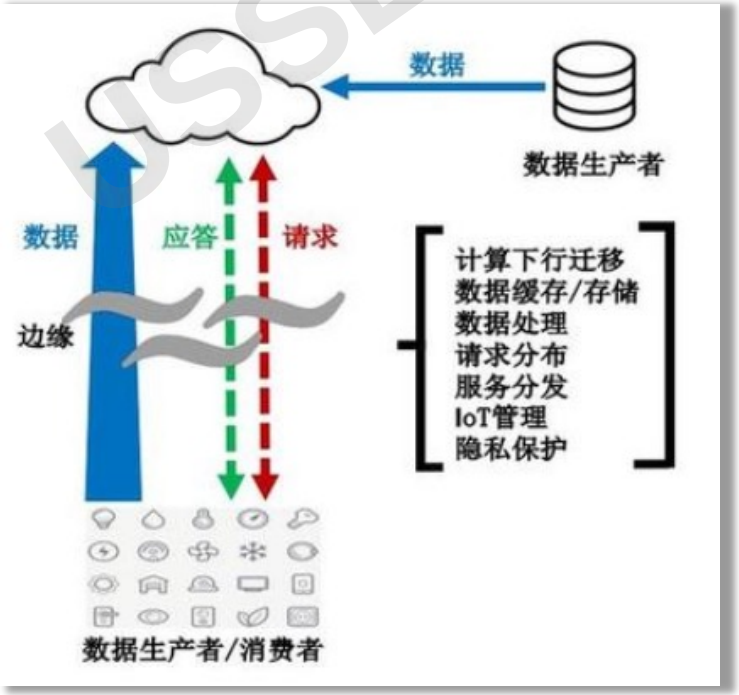
- **计算**：物联网各类业务中数据的处理操作
  - 如自动驾驶目标识别、路径规划等
  - 安全计算，如设备状态检测、异常检测等

JSSLAB

边缘计算模型和特点

- **特点：**
  - 计算任务从计算中心迁移到网络边缘，计算任务部分或者全部在边缘完成
  - 边缘设备既是数据生产者，又是数据的消费者

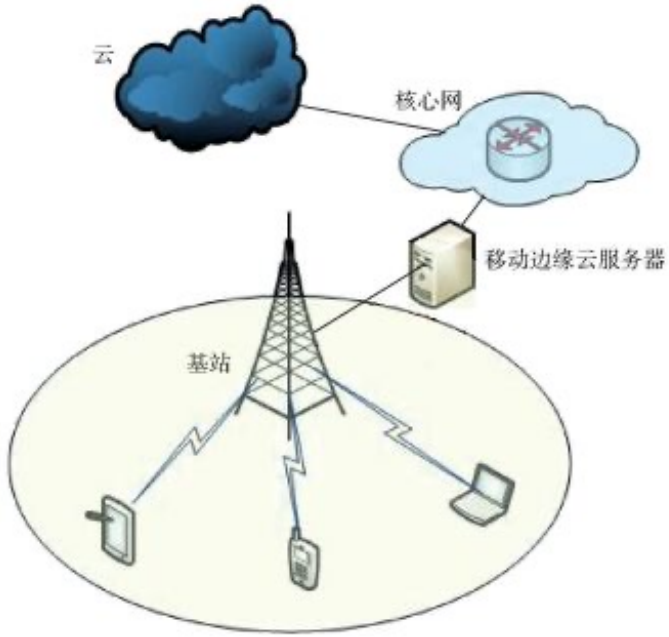
边缘计算模型



USSLAB

移动边缘计算

- **移动边缘计算**(mobile edge computing，MEC)：将移动计算任务迁移到附近的网络边缘服务器，如蜂窝网络基站等，为移动应用程序和服务提供低延迟、高带宽数据处理能力的计算方式
- **边缘计算 vs. 移动边缘计算：**
  - **边缘计算模型**中的终端设备具有较强的计算能力，倾向于将移动计算任务在边缘终端上完成
  - **移动边缘计算模型**强调在云计算中心和边缘设备间的边缘服务器上，主要针对移动网络场景，如将基站作为边缘服务器，完成数据计算



USSLAB

边缘计算的优势

- **缓解网络带宽和数据中心压力**：利用边缘设备已具有的计算能力，将应用服务程序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
- **增强服务响应能力**：边缘计算在用户附近提供服务，近距离服务保证较低的网络延迟，简单的路由也减少网络抖动。5G等技术将为边缘计算系统的降低数据延迟、增强相应性能
- **保护数据隐私**：在数据上传至云中心之前，在边缘设备执行预处理，以减少传输数据量，降低传输带宽负载。在边缘设备处理个人身体数据等隐私数据，用户隐私会得到更好地保护

USTLAB

边缘计算 vs 云计算

- **云计算**：云计算将所有计算放在云端处理，特点包括云服务器规模庞大、高可靠性、可拓展性、资源虚拟化等
- **边缘计算**：边缘计算在边缘设备提供用户所需的服务和云端计算功能

USSLAB

边缘计算 vs 云计算

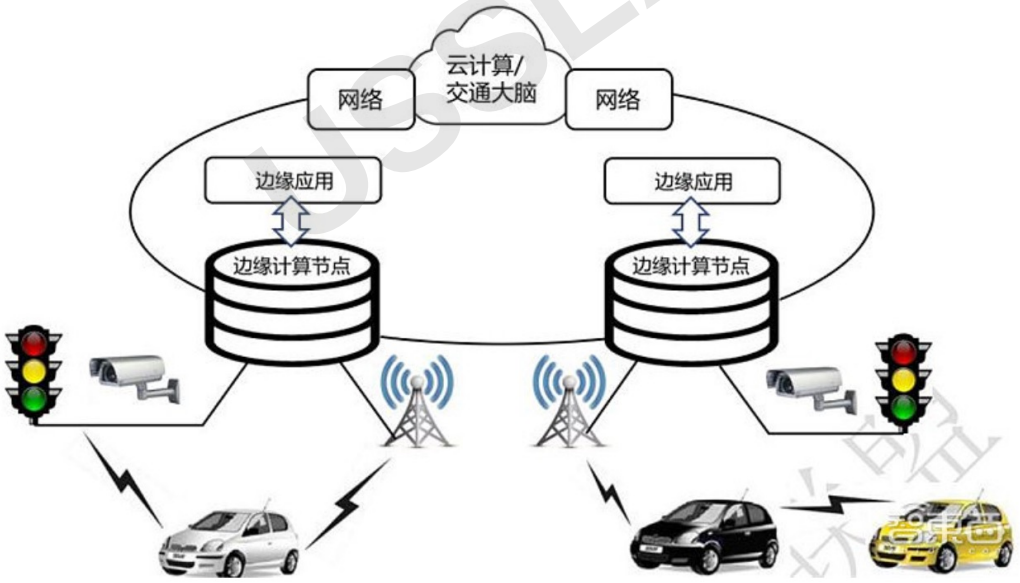
- 边缘计算是对云计算的补充和延伸，为移动计算、物联网等提供更好的计算范式
- 相互依赖：
  - 边缘计算模型需要云计算中心的强大计算能力和海量存储的支持
  - 云计算需要边边缘设备对于海量数据及隐私数据的处理，从而满足实时性、隐私保护和降低能耗等需求

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

USC LAB

边缘计算 + 云计算：“云边协同”

- **云边协同**：边缘计算、云计算关键都是解决数据的存储、传输和处理。云边协同是云计算与边缘计算的互补协同，同时利用边缘计算和云计算的优势，达到数据处理任务分配均衡、传输带宽需求和存储空间需求优化



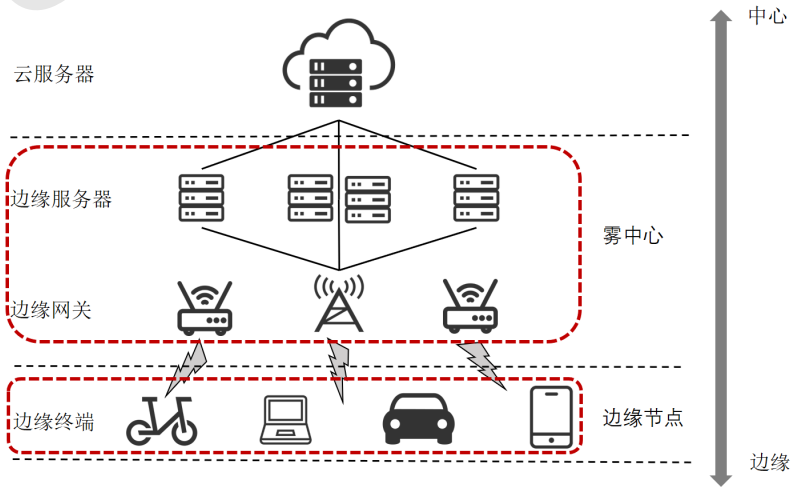
云边协同在智慧交通场景中的应用

边缘计算 vs. 雾计算

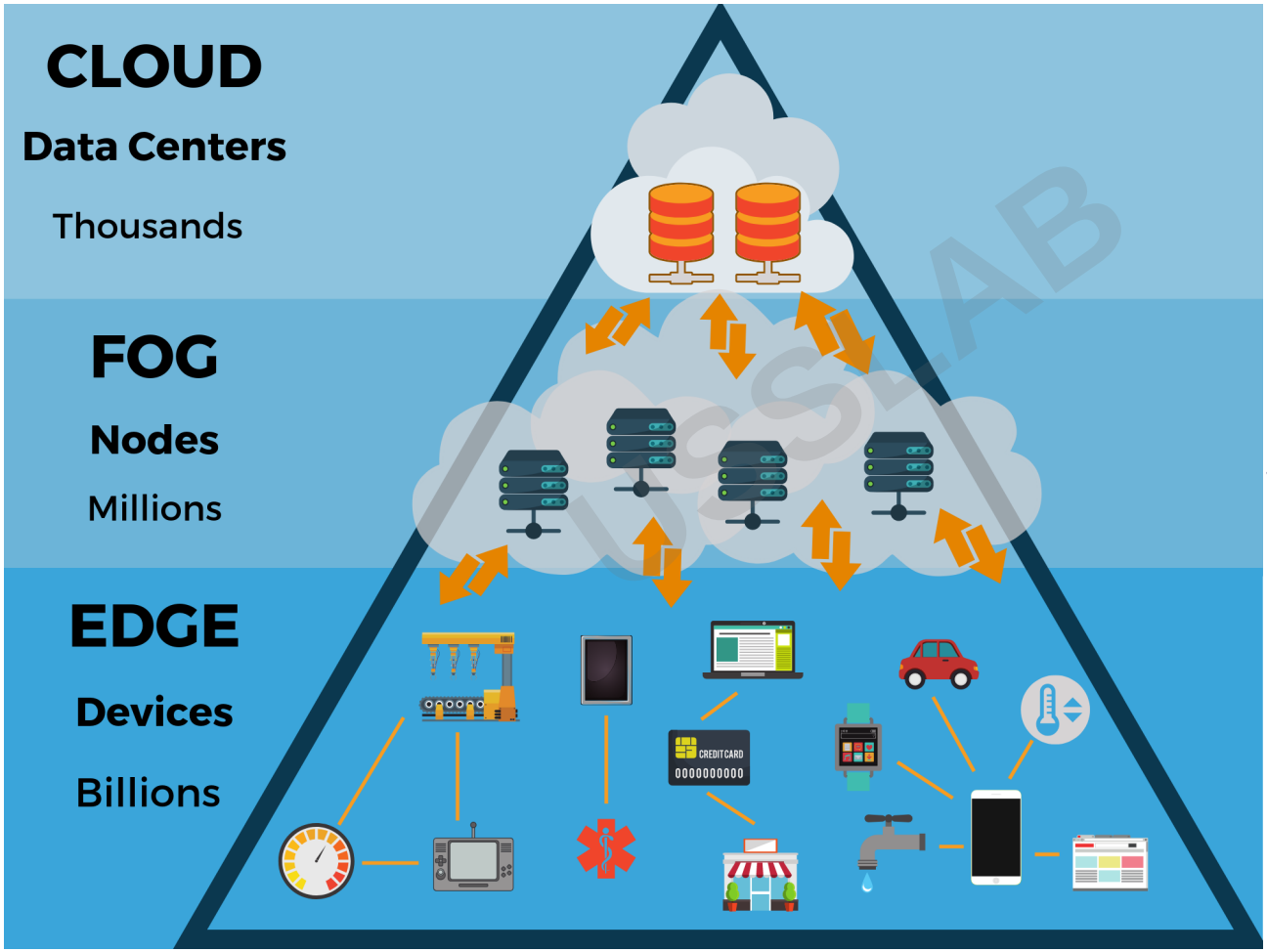
- **雾计算：**强调在网络边缘和中心云之间的层次结构中进行计算和数据处理，雾计算节点通常具有更强大的计算和存储能力，如路由器、交换机和专用服务器
- **相同点**：分布式计算范式，将计算从云推移至网络边缘，学术界、工业界中两者名词经常互换使用
- **不同点**：边缘计算侧重于将计算任务推向数据产生源头的终端；雾计算侧重于将数据在雾端具有较强算力的各类服务器，例如网关等

JSSLAB

雾计算



云计算 vs. 雾计算 vs. 边缘计算 vs. 移动边缘计算



如果面向移动应用，采用无线通信，在基站上进行数据计算，则称为移动边缘计算

边缘计算相关技术

- **AI算法**
  - 边缘AI
  - 模型压缩等
- **网络通信**
  - 5G通信技术
- **计算任务分配**
  - 计算迁移
  - 负载均衡
  - CDN网络技术

USSLAB

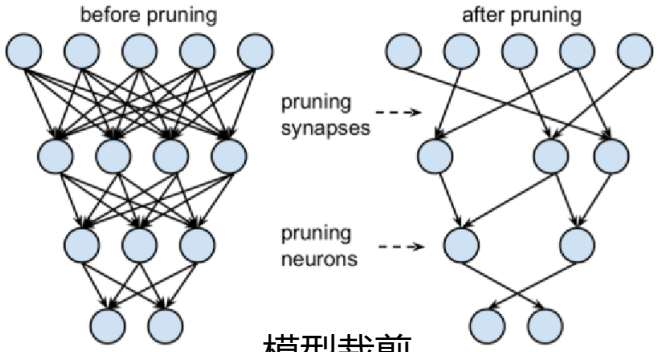
人工智能技术

- **边缘AI**：结合人工智能和边缘计算，使得人工智能算法在能够边缘计算设备上运行，减少对云端的依赖，提高响应速度和隐私保护。
- AI模型在边缘设备部署实现边缘计算，面临问题包括：
  - 资源受限：计算、存储、通信、供电等资源
  - 隐私和安全：边缘设备处理敏感数据，模型部署在边缘处。可以被物理抵近攻击，窃取模型和隐私数据，例如通过功耗侧信道头模型等
- 边缘AI涉及到的技术
  - 模型压缩剪枝
  - 模型高效设计
  - 硬件定制优化
- 热点：大模型端侧部署的优化问题

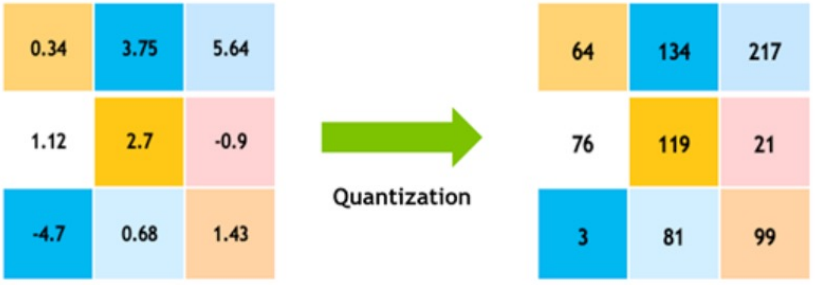
USLAB

边缘AI – 模型压缩和计算优化

- **模型压缩和优化**：旨在减少模型的大小、计算复杂度和存储需求，从而使模型在资源受限的环境中更高效地运行
- **模型压缩方法**
  - **模型剪枝Pruning**：移除冗余不重要的神经元或连接，减少模型参数，减少模型大小和计算量，同时保持模型性能。包括权值剪枝Weight pruning、结构化剪枝Structured pruning、非结构化剪枝Unstructured pruning
  - **模型量化Quantization**：将模型权值和激活从高精度格式转换为低精度格式（如32位浮点数→8位整数），从而减小模型大小、加快推理速度，并能够在特定硬件平台（尤其是嵌入式设备）运行，但牺牲了一定精度



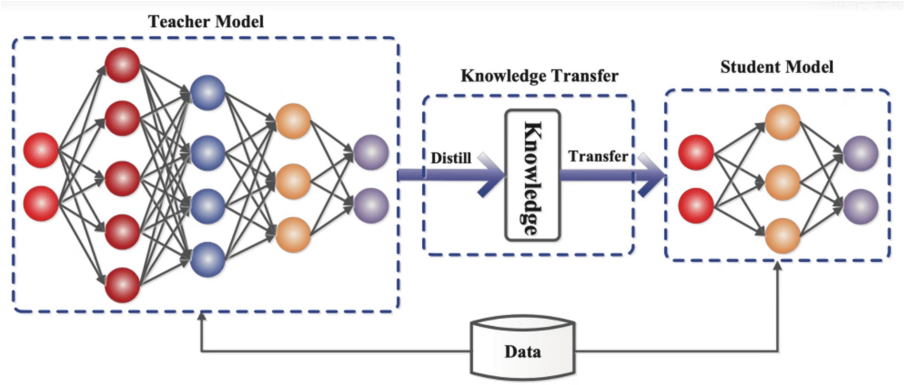
模型裁剪



模型量化

边缘AI – 模型压缩和计算优化

- **模型压缩和优化**：旨在减少模型的大小、计算复杂度和存储需求，从而使模型在资源受限的环境中更高效地运行
- **模型压缩方法**
  - **知识蒸馏Knowledge Distillation**：通过将复杂模型（教师模型）的知识萃取蒸馏出来，传递给简单的模型（学生模型）来实现模型压缩。学生模型可以保持教师模型相似似的性能，但计算和存储成本更低。
  - **低秩分解Low-Rank Factorization**：将权重矩阵分解成多个低秩矩阵，从而减少参数数量，有效减少模型尺寸和计算复杂度



知识蒸馏

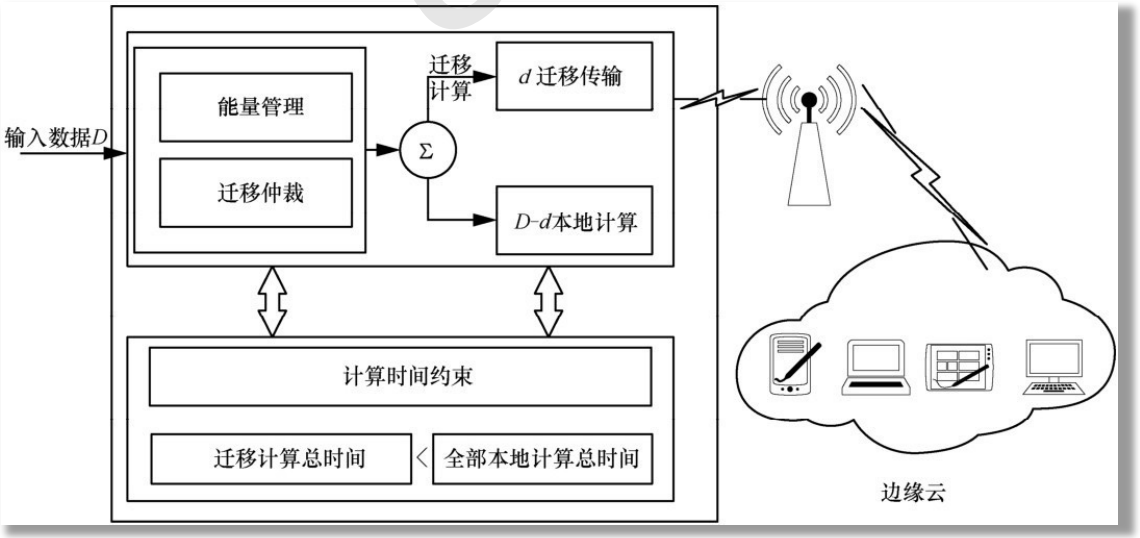
VSSLAB

计算迁移(Computation Offloading)

- 背景：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
- 由于边缘节点通常受计算资源、存储空间约束。需要通过无线网络分发、上传资源消耗量大的任务到边缘计算服务器，使得移动终端在运行大型应用时具有更短的响应时间和更长的电池续航时间等
- 边缘计算中计算迁移内涵
  - 云数据中心计算任务下沉
  - 计算任务迁移至资源丰富的节点
  - 边缘设备资源共享

计算迁移(Computation Offloading)

- 边缘计算中的计算迁移策略是在网络边缘处，将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，迁移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，部分迁移还是全部迁移



计算迁移
整体框架

USSLAB

负载均衡(Load balancing)

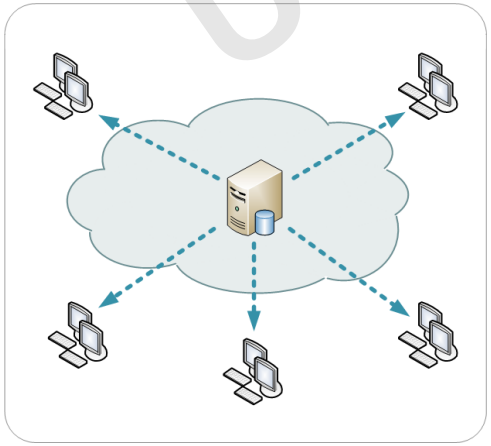
- **定义**：将工作负载（如计算任务、数据处理）动态分配到多个边缘节点或设备上，以提高系统性能、资源利用率和服务质量
- 与传统负载均衡不同，边缘计算将计算和数据处理任务分散到接近数据源或用户的设备上，从而减小延迟、节省带宽，并提高可靠性和安全性。常见方法包括：
  - **静态负载均衡**：预先将不同的任务分配给固定的边缘节点。适用于负载变化不大、任务情况较为稳定的场景
  - **动态负载均衡**：根据运行时系统状态（如节点的负载、网络条件等）动态调整任务分配
  - **基于任务类型的负载均衡**：根据任务的特性（如计算密集型、数据密集型）将其分配给最适合的边缘节点。例如，数据密集型任务分配给拥有大存储容量的节点
  - **地理位置感知负载均衡**：根据用户或数据源的地理位置，将任务分配给其地理位置相对较近的边缘节点，以减少网络传输延迟

DSLAB

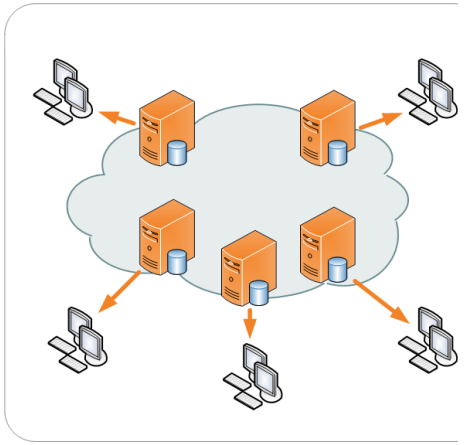
CDN内容分发网络

- **内容分发网络**：content distribution networks(CDN) 是一种通过互联网互相连接的网络系统，利用靠近用户的服务器，快速可靠地将音乐、影片、应用程序、文件等网络内容分发给用户
- **核心思想**：根据网络内容的长尾效应，将频繁访问内容放置在缓存服务器并尽可能靠近用户端
- 比喻：总店 vs. 分店。
- 相关公司：Akami, Amazon，网宿科技、蓝汛等

据统计，Internet上超过80%的用户重复访问20%的信息资源



主从网络：向中央服务器请求资源

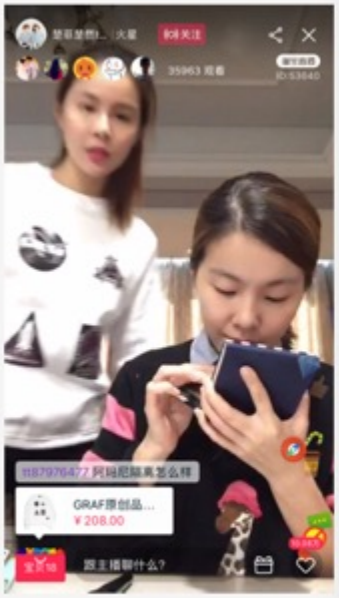


CDN：向最近的存储服务器请求资源

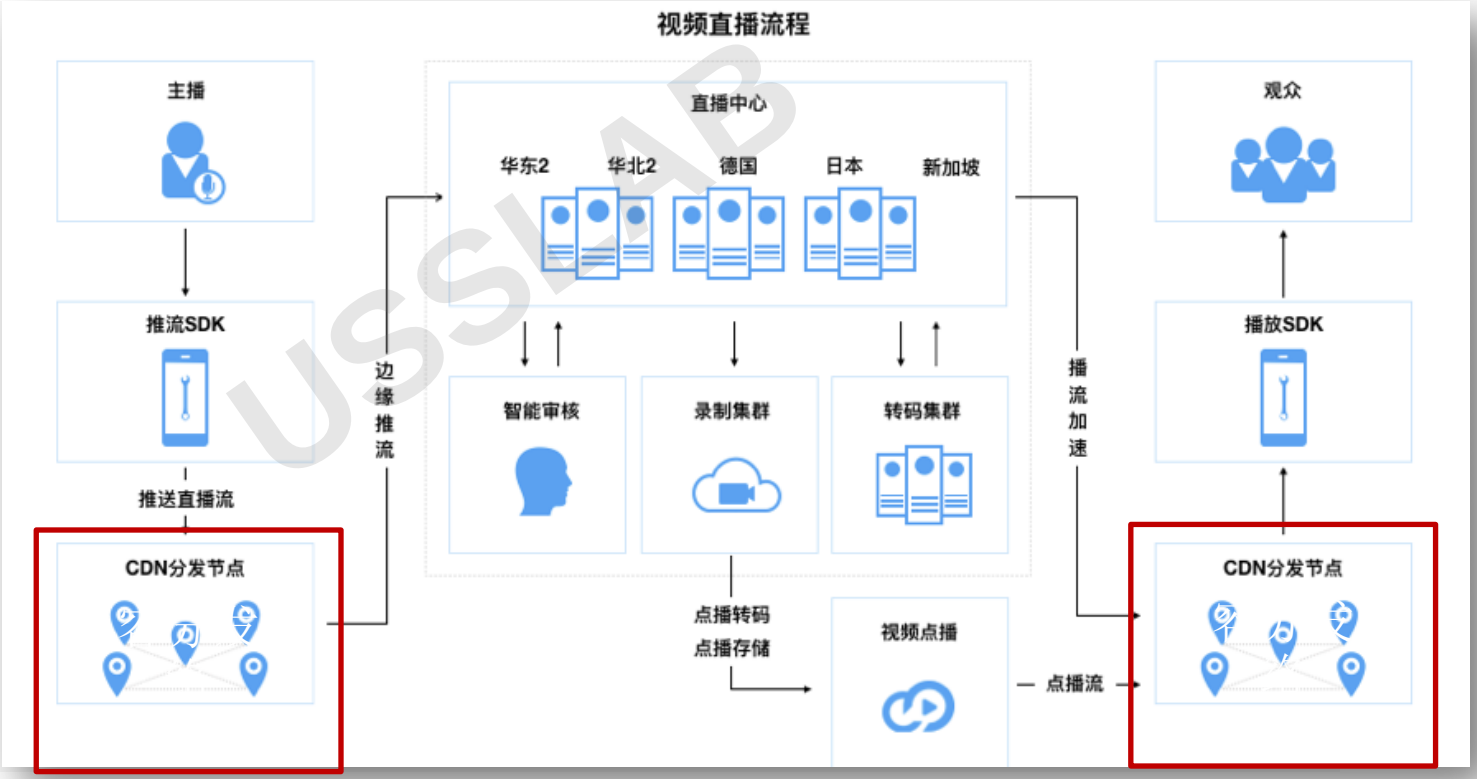
USSLAB

CDN网络的应用

- 应用场景：视频播放、直播等



手机直播



USSLAB

边缘计算安全威胁

边缘计算面临的安全威胁

- 边缘计算面临所有终端安全问题、软硬件和算法安全问题

威胁分类 / 安全威胁	威胁来源		威胁作用点				威胁结果			
	外在威胁	内部脆弱	应用层	数据层	网络层	基础设施层	数据泄露	网络阻塞	权限获取	响应异常
侧信道攻击	■					■	■			
DDoS	■				■			■		■
身份伪造	■				■	■	■		■	
恶意注入	■		■			■	■			■
加密欠缺		■		■			■		■	
隐私侵犯	■	■		■			■			

USSLAB

威胁来源

- **外部威胁：**外部威胁构成多样，本质是边缘节点或边缘服务器需要计算分发、协同计算，因此节点间交互多
  - 常见的外部威胁包括DDoS、侧信道攻击、木马注入、身份伪造

- **内部威胁：**内部威胁是由于设备的内在脆弱性，例如边缘节点的大量异构导致难以进行统一有效的管理；同时计算能力有限，对数据的机密性、完整性等保护不充分
  - 常见的内部威胁包括了加密欠缺和隐私侵犯

JSLAB

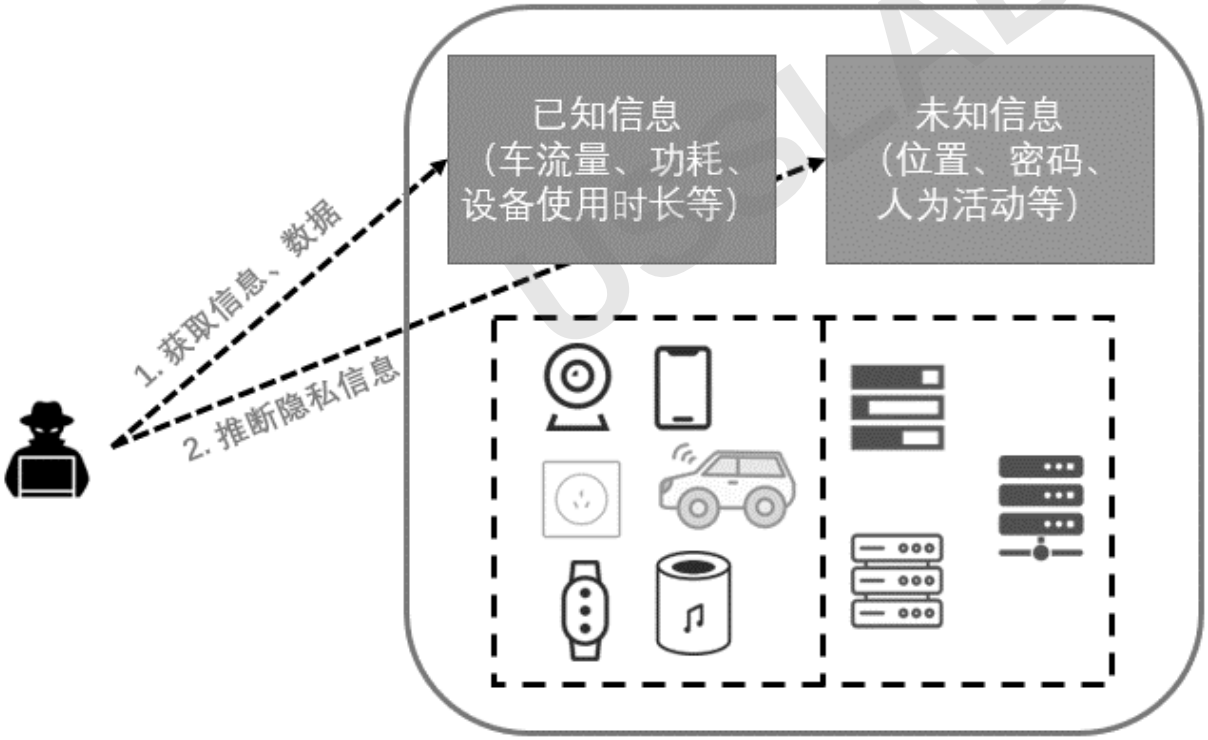
威胁作用点

- **应用层面**：开发者使用不同开发语言、代码习惯差异、数据读写权限不同等将引入应用安全隐患
- **数据层面**：边缘计算数据包含了用户个人隐私、业务信息等敏感数据，因此大多数边缘计算安全问题与数据及隐私保护有关
- **网络层面**：边缘计算中大多基于5G等无线通信信道，这类开放广播信道容易受到干扰攻击，常见的如DDoS攻击、侧信道攻击等
- **基础设施层面**：由于边缘节点物理距离更近，且边缘节点的硬件与操作系统具有简易性，无法构建完整的防火墙和漏洞检测机制，因此容易受到身份伪造攻击、侧信道攻击乃至针对节点的物理破坏攻击

USSLAB

具体安全威胁——侧信道攻击

- **安全威胁**：一种作用在边缘计算终端节点或者边缘计算服务器的外部安全威胁，使用不敏感的可公开访问的信息来推测用户隐私和模型隐私数据



边缘计算侧信道攻击示意图

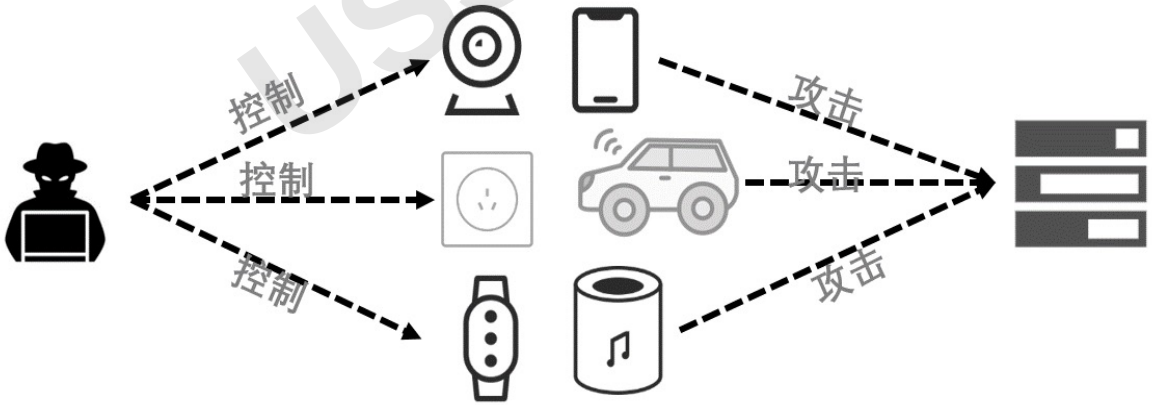
侧信道攻击与边缘计算

- **面更大**：边缘计算的海量互联节点使攻击面更广、攻击能力更强。比如在边缘计算场景下，AI算法经过压缩之后，从云端下沉到边缘设备部署，攻击者可通过节点通信数据包、计算功耗等侧信道信息，推理AI模型、训练数据，甚至是干扰破坏边缘计算。
- **易接近**：边缘节点的通信方式使攻击者更容易“接近”它们。攻击者拥有更多可操纵的边信道（WiFi、蓝牙、ZigBee等通信方式）。攻击者可以破坏或靠近边缘设备，利用无线通信信道、功耗信道和针对智能手机的信道进行攻击。
- 案例：边缘AI模型窃取攻击、电磁攻击等

USSLAB

DDoS攻击

- **安全威胁：**边缘计算面临的网络层的外部攻击，攻击者旨在利用分布式资源破坏由一个或多个边缘计算服务器提供的正常服务，造成网络拥塞和响应异常
- 传统的DDoS攻击发生在攻击者从受感染的分布式设备向目标设备发送数据包



DDoS攻击示意图

USSLAB

DDoS攻击与边缘计算

- **边缘计算DDoS：**边缘节点服务器容易成为DDoS攻击的发起者和受害者
  - **攻击者**：边缘计算的终端设备数量庞大，且具备计算能力。一旦遭受攻击，边缘节点集群将成为DDoS攻击的强力发起源，结合各终端设备的计算能力，攻击规模和威力将是传统互联网DDoS攻击的数十乃至百倍，如Mirai病毒
  - **受害者**：一旦边缘服务器关键节点成为DDoS攻击的被攻击目标，其连接的和提供服务的下游节点均可能受到影响

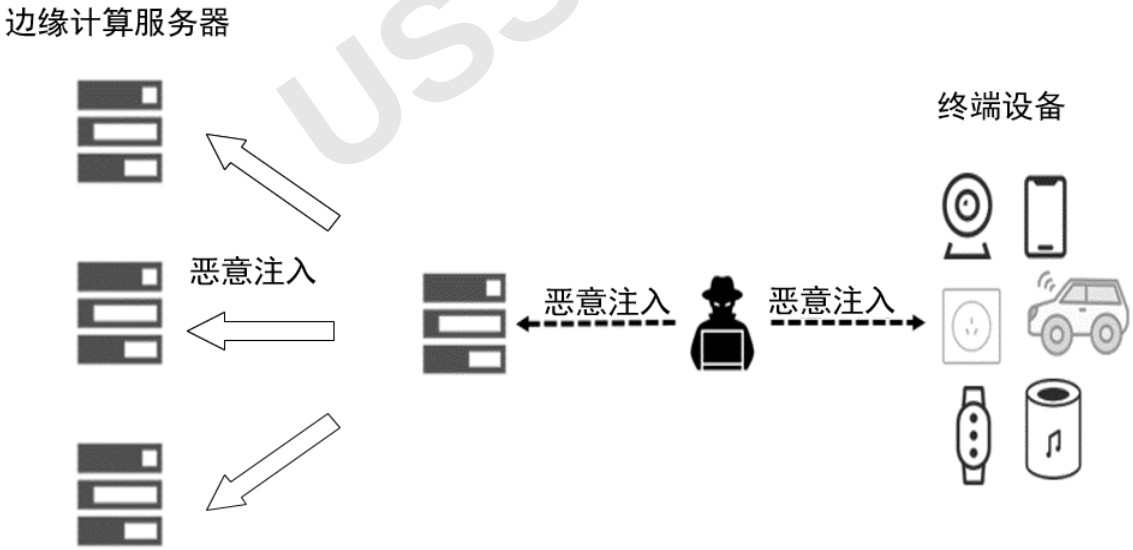
身份伪造攻击

- **安全威胁**：身份伪造威胁是一种外部攻击方式，通过网络层和终端软硬件的脆弱性，进行提权和数据窃取等操作
- 挑战：边缘计算节点数量大，设备登录认证存在弱口令等漏洞，且防护方法简单
  - **身份认证部署困难**：在边缘计算中，计算资源的限制导致无法部署如云计算场景中完整的身份认证技术，并且由于边缘计算节点数量多且异构，更加难以部署统一有效的身份认证技术
  - **身份认证过程复杂**：传统的云计算身份认证是单向的，而在边缘计算中，身份认证为双向且认证场景多变：单一域身份认证、跨域身份认证、切换认证

USLAB

恶意注入攻击

- **安全威胁**：一种作用在边缘计算应用和基础设施上的外部攻击，如通过将恶意代码注入到边缘计算应用和边缘服务器操作系统中
  - 边缘服务器端：面临SQL注入攻击
  - 终端：面临各类恶意信号和恶意代码攻击



恶意注入攻击示意图

USSLAB

恶意注入与边缘计算

- **边缘计算设备防护措施不完备**：在边缘计算下，边缘设备和低级别的边缘计算服务器几乎无法受到传统防火墙的保护，相比之下更加容易受到恶意注入的攻击

- **恶意注入途径多样**：由于终端设备的高度异构，并且边缘计算中的设备数量巨大，每种设备的防护水平不一，因此攻击者可以通过不断尝试不同设备来尝试注入攻击。

- **节点家族同源特性**：边缘计算节点软件、硬件具有家族同源特性，使得攻击在一个节点成功之后可以通过网络继续攻击其它相关节点

CSSLAB

加密欠缺

- **安全威胁**：一种作用在边缘计算应用和数据层面的内部威胁，攻击者利用可导致数据机密性被破坏
- **边缘计算自身资源有限**：在海量终端互联的背景下，边缘节点分配给数据加密的资源不足。对全部数据进行全部加密的方法在边缘计算中并不完全可行
- **辅助加密设备成本限制**：针对资源有限的边缘设备，使用额外的加密设备辅助保护数据隐私，在理论上是一种可行的方案。但是考虑到边缘计算节点数量巨大，对于数据加密要求不一，为所有的边缘计算节点添加辅助加密设备在经济上不可行
- 替代方案：选择优先级高的敏感数据进行加密

IOSSLAB

隐私侵犯

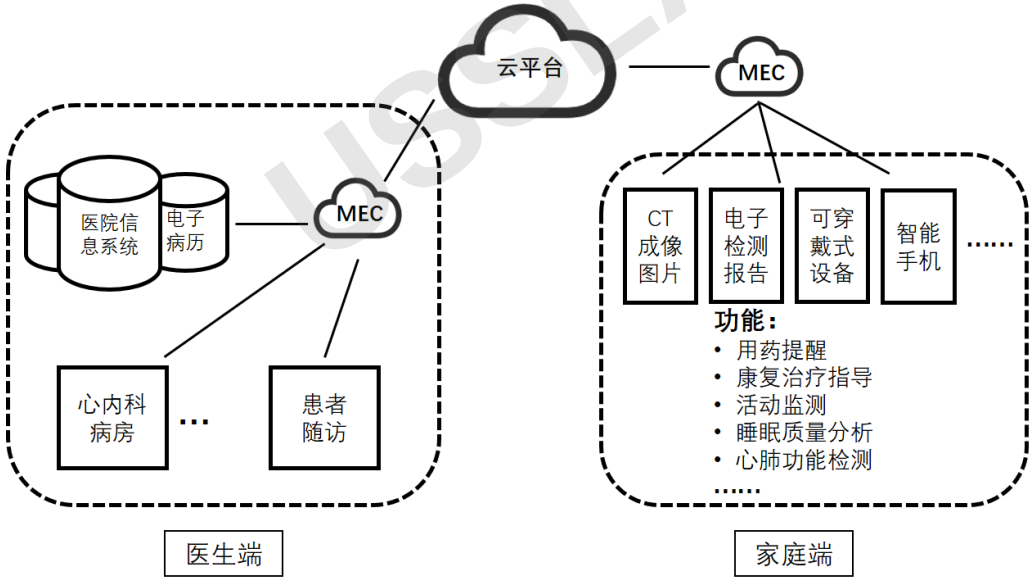
- **安全威胁**：一种作用于边缘计算应用和数据层的，以破坏数据隐私特性为目标的安全威胁
- 隐私侵犯是所有计算范式中都要面临的安全问题，因用户的敏感数据和个人信息存储在边缘节点和服务器，需要同时解决边缘设备和服务器上的数据隐私保护问题
- 趋势：Edge AI中涉及到用户训练数据、AI模型隐私等，这些隐私成为新型的隐私侵犯对象
- 隐私侵犯对象
  - **边缘设备：**各类智能设备，如智能手环，记录用户疾病诊断记录、病情、用户当前所在位置、用户睡眠时间段等
  - **边缘服务器：**部署着各类应用和边缘AI算法

边缘计算案例

USSLAB

边缘计算 + 智慧健康

- **智慧健康：**
  - 提供更高效、便捷的医疗服务，简化医疗流程，公平、开放的医疗资源供给，打破医学数字信息“孤岛”
- **边缘设备/服务器：**核磁共振仪、手环、手机等



智慧医疗场景：足不出户便可获得医疗健康服务

USSLAB

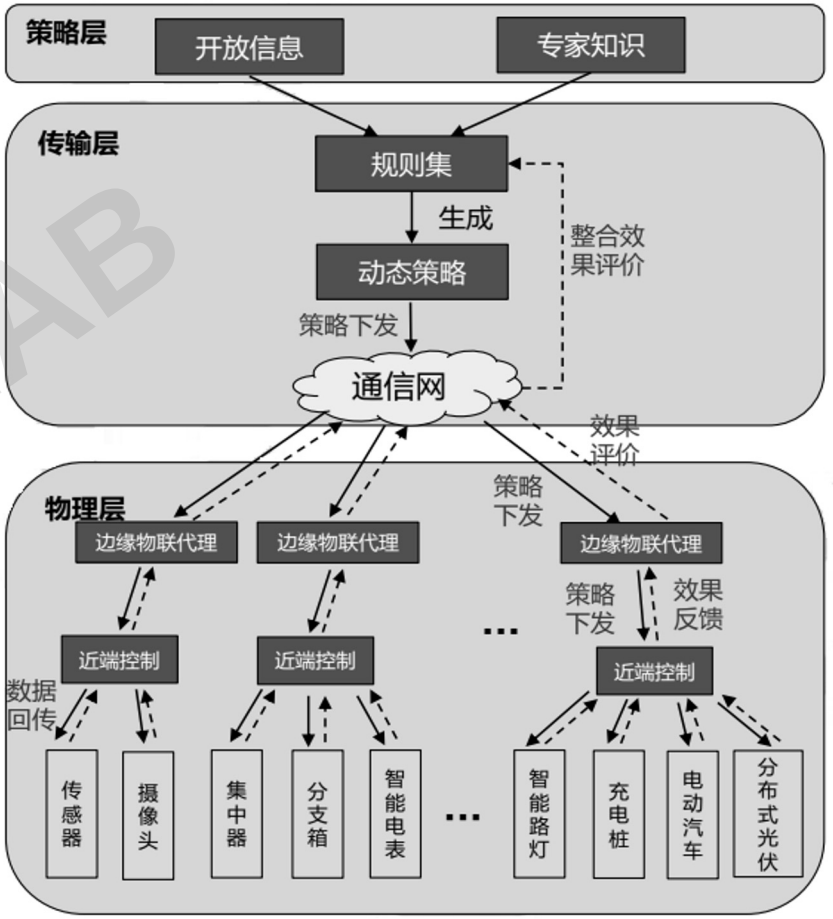
边缘计算 + 智慧健康

- **边缘计算安全问题：**可穿戴设备在体积、功耗、成本等多方面受限，计算能力弱、存储空间不足
- **威胁一：身份伪造威胁**
  - 远程诊疗受到中间人攻击或伪造医护人员身份的威胁，攻击者可能执行窃取敏感医疗数据、谎报诊疗结果乃至恶意执行手术等任务
  - 医疗传感器、执行器不具备双向认证能力，其管理密码容易被字典攻击破解，攻击者得以控制医疗设备
- **威胁二：隐私侵犯威胁**
  - 智能手机、手环等边缘节点将用户的疾病诊断、位置、睡眠记录等上传至可信度未知的数据分析服务商
  - 健康分析模型基于数据推理得到的结果未必可信，可能将正常用户误诊为患有某种疾病，引起用户恐慌

USSLAB

边缘计算 + 电力物联网

- **电力物联网：**规模大、种类多、业务复杂
- 边缘设备：融合终端、集中器、摄像头、充电桩……
- 问题：需设计新的管控技术，针对电力物联终端设备进行管理和数据分析
- **方法：引入利用边缘物联代理**
- **案例：**基于功耗侧信道的边缘安全监测



电力边缘物联代理

USSLAB

总结：边缘计算特点

- 掌握边缘计算模式的定义和特点
- 掌握边缘计算和云计算、雾计算的相同和差异性
- 了解边缘计算的相关技术
- 掌握边缘计算的安全威胁，尤其是和边缘计算特点相结合的威胁来源、特性及危害

USSLAB