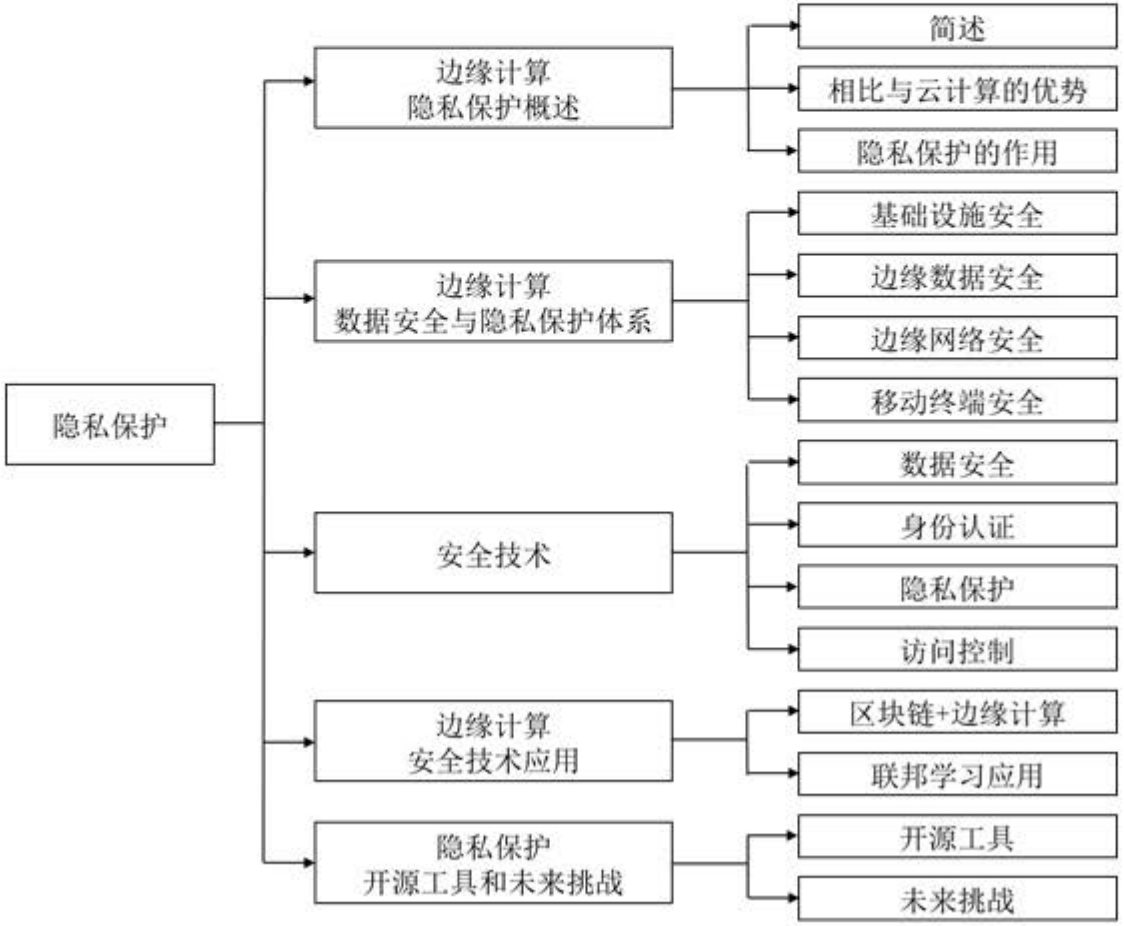
安全与隐私保护

简介

- **章节概览：**


隐私保护
边缘计算
隐私保护概述
简述
相比与云计算的优势
隐私保护的作用
边缘计算
数据安全与隐私保护体系
基础设施安全
边缘数据安全
边缘网络安全
移动终端安全
安全技术
数据安全
身份认证
隐私保护
访问控制
边缘计算
安全技术应用
区块链+边缘计算
联邦学习应用
隐私保护
开源工具和未来挑战
开源工具
未来挑战

目录

边缘计算隐私保护概述

- 简述
- 边缘计算与云计算相比在隐私保护方面的优势
- 隐私保护在边缘计算的作用

简述（1）

- **安全是指达到抵抗某种安全威胁或攻击的能力，横跨云计算和边缘计算，需要实施端到端的防护。**
- **边缘计算有五大问题需要解决：**
  - 体系结构、碎片化、物理安全性、蔓延、用户错误
- **可以从五个方面评价边缘计算的数据安全性：**
  - 机密性、完整性、可用性、身份验证和访问控制、隐私要求

边缘计算隐私保护概述

- 简述
- 边缘计算与云计算相比在隐私保护方面的优势
- 隐私保护在边缘计算的作用

边缘计算的优势（1）

- **降低用户隐私数据泄露的风险**
  - 数据或任务能够在靠近数据源头的网络边缘侧进行计算和执行，为数据安全和隐私保护提供更好的结构化支撑。
- **突破了终端硬件的限制**
  - 移动终端等便携式设备大量参与到服务计算中，实现了移动数据存取、智能负载均衡和低管理成本。

边缘计算的优势（2）

- **允许更多保密算法的应用**
  - 复杂的加密和隐私保护算法也得以应用在更多的边缘计算服务上，从而更好的保障用户隐私。
- **黑客攻击变得困难**
  - 在边缘计算中，黑客想要访问边缘内的敏感信息，就需要渗透到分散的存储系统中以访问边缘内的敏感信息。

边缘计算隐私保护概述

- 简述
- 边缘计算与云计算相比在隐私保护方面的优势
- 隐私保护在边缘计算的作用

隐私保护在边缘计算的作用（1）

- 随着嵌入式智能设备越来越多，隐私数据的安全问题逐渐成为人们最为关心的问题之一。
- 在边缘计算的场景下，数据安全性和隐私保护已成为保护最终用户的业务。

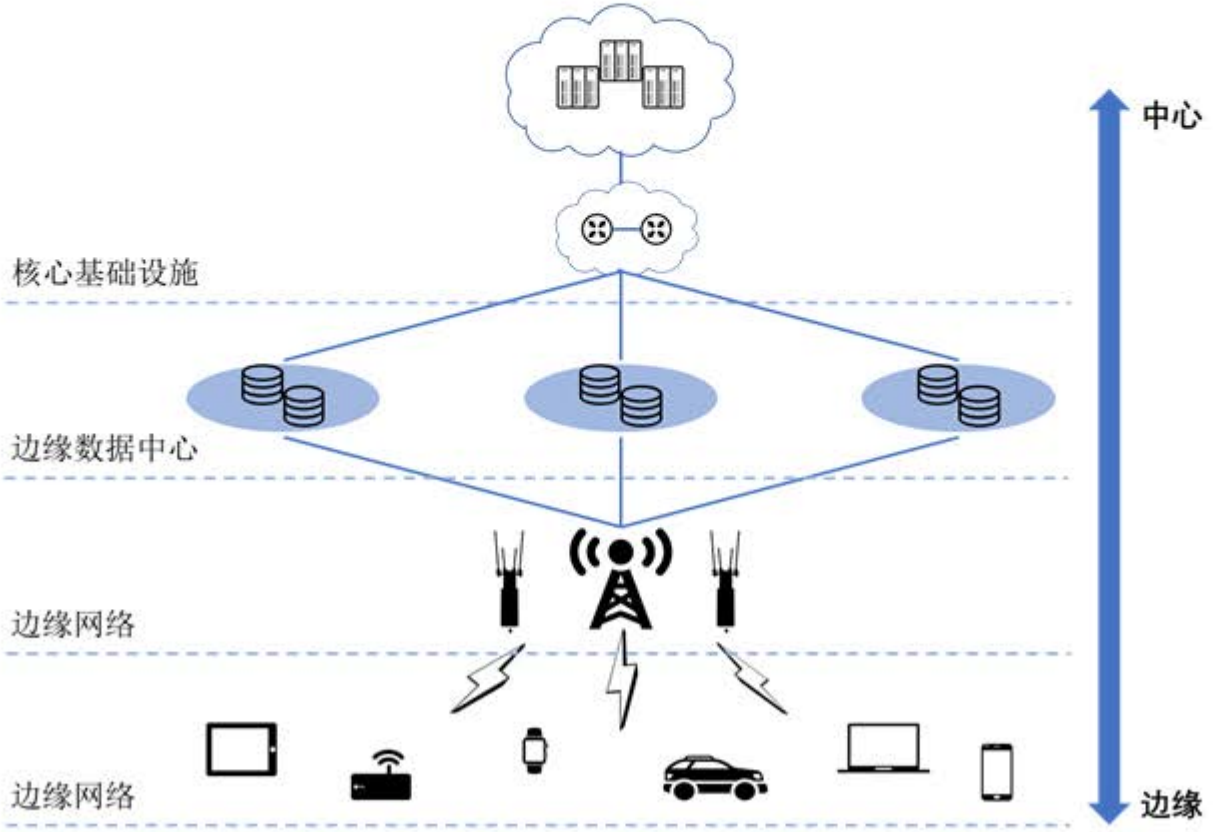
目录

边缘计算数据安全与隐私保护体系

- 简介
- 基础设施安全
- 边缘数据安全
- 边缘网络安全
- 移动终端安全

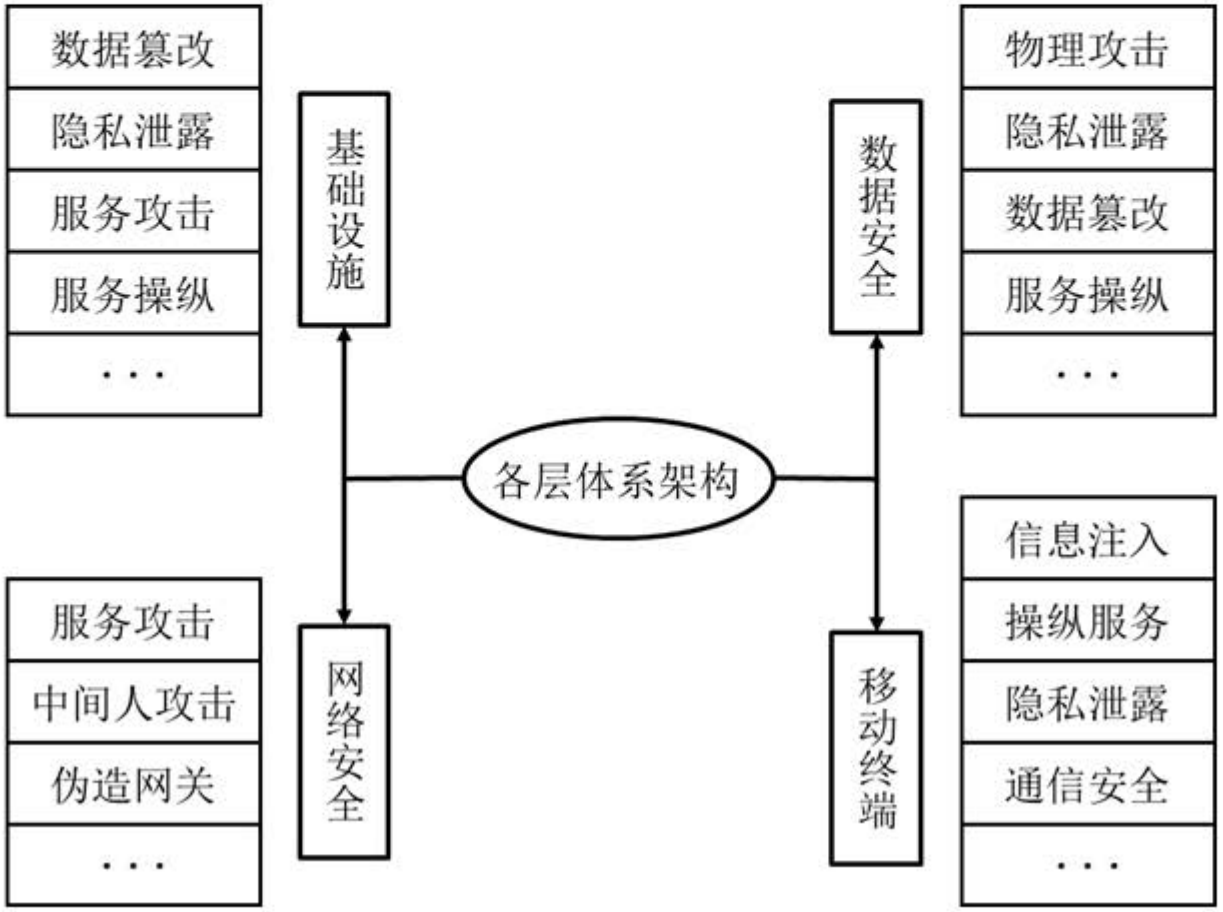
简介（1）

边缘计算的体系架构包括核心基础设施、边缘数据中心、边缘网络和移动终端。



简介（2）

边缘计算的体系架构每一层都存在这一定的安全问题。



边缘计算数据安全与隐私保护体系

- 简介
- 基础设施安全
- 边缘数据安全
- 边缘网络安全
- 移动终端安全

基础设施安全（1）

- **产生隐私安全问题的原因：**
  - 边缘计算服务模式下，通过部署多层次的异构服务器，来实现在各服务器之间的大规模计算迁移，为不同地理位置上的用户提供实时服务和移动代理。
  - 由于这些核心基础结构可能是半信任的或完全不信任的，因此这将带来巨大的挑战，极有可能发生包括隐私泄露、数据篡改、服务攻击、服务操纵等安全隐患。

基础设施安全（2）

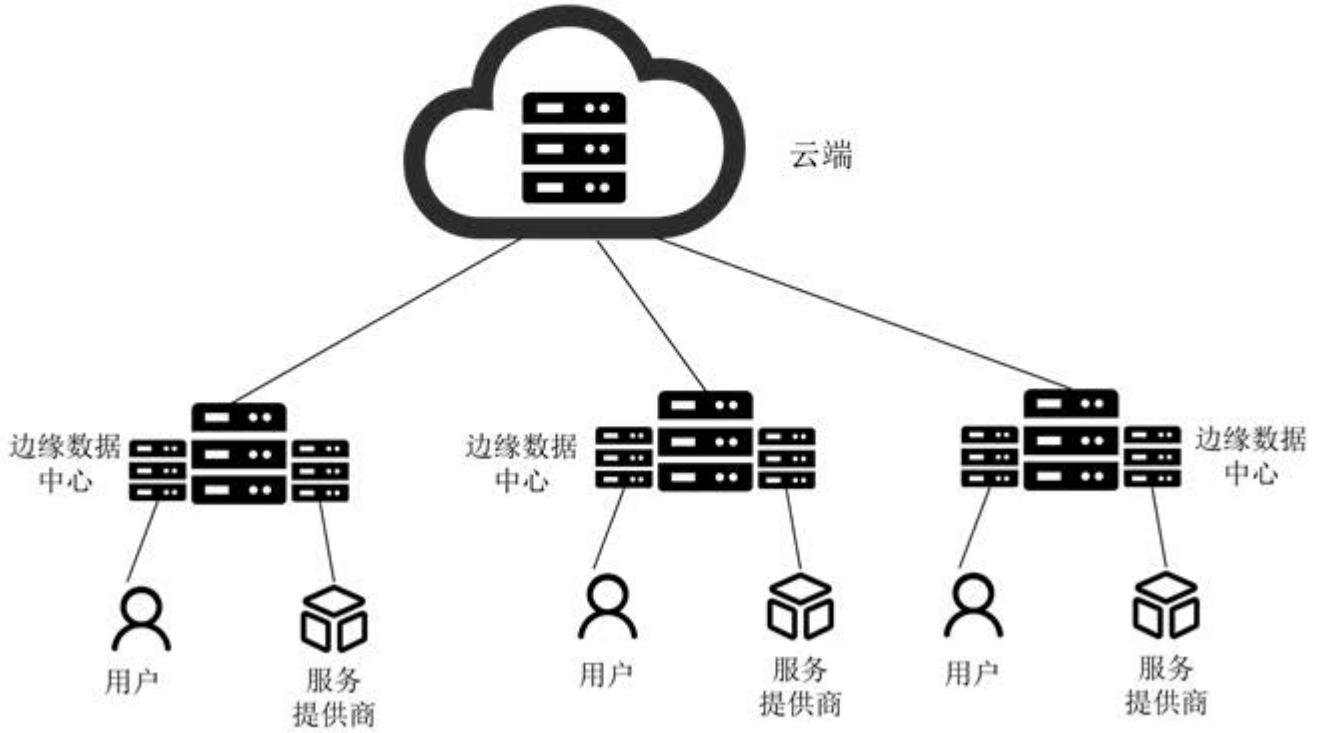
- **解决安全问题的方法：**
  - 解决基础设施安全的方法包括：物理安全机制、可信机制和虚拟化技术等。
  - 物理安全机制是针对物理特征的检测、响应；
  - 可信机制包括可信根、可信启动过程、身份证明、认证过程等；
  - 虚拟化技术是在有能力或重要的主节点实现任务的虚拟化，可隔离病毒发生。

边缘计算数据安全与隐私保护体系

- 简介
- 基础设施安全
- 边缘数据安全
- 边缘网络安全
- 移动终端安全

边缘数据安全（1）

边缘数据中心构架：边缘数据中心、基础设施、多租户虚拟化基础设施。



边缘数据安全（2）

- **产生隐私安全问题的原因：**
  - 边缘计算模式下的分布式并行数据处理方式使边缘计算平台存在数据保密性问题和隐私泄露现象；
  - 面临的安全挑战主要包括物理攻击、隐私泄露、服务操纵和数据篡改等。
- **解决安全问题的方法：**
  - 解决数据安全问题的方法包括：使用数据安全、存储数据安全、迁移数据安全；
  - 目前，在边缘计算数据安全方面，有许多人提出了相关的解决技术。

边缘计算数据安全与隐私保护体系

- 简介
- 基础设施安全
- 边缘数据安全
- 边缘网络安全
- 移动终端安全

边缘网络安全（1）

- **产生隐私安全问题的原因：**
  - 边缘计算通过移动通信核心网络，无线网络和互联网等多种通信的集成来实现物联网设备和传感器的互连，这给这些通信基础设施带来了许多网络安全挑战。
  - 边缘网络中面临的主要安全威胁包括拒绝服务攻击、中间人攻击和伪造网关等。
- **解决安全问题的方法：**
  - 网络安全问题的方法包括：通信安全机制，访问控制、入侵检测、异常行为分析等防护技术，以及协议安全。

边缘计算数据安全与隐私保护体系

- 简介
- 基础设施安全
- 边缘数据安全
- 边缘网络安全
- 移动终端安全

移动终端安全（1）

- **产生隐私安全问题的原因：**
  - 移动终端中的安全威胁主要有终端安全和隐私保护等，具体包括信息注入、操纵服务、隐私泄露、恶意代码攻击、通信安全等风险。
- **解决安全问题的方法：**
  - 移动终端安全问题的方法包括：包括密钥管理、密码套件管理、身份管理、安全策略管理等。

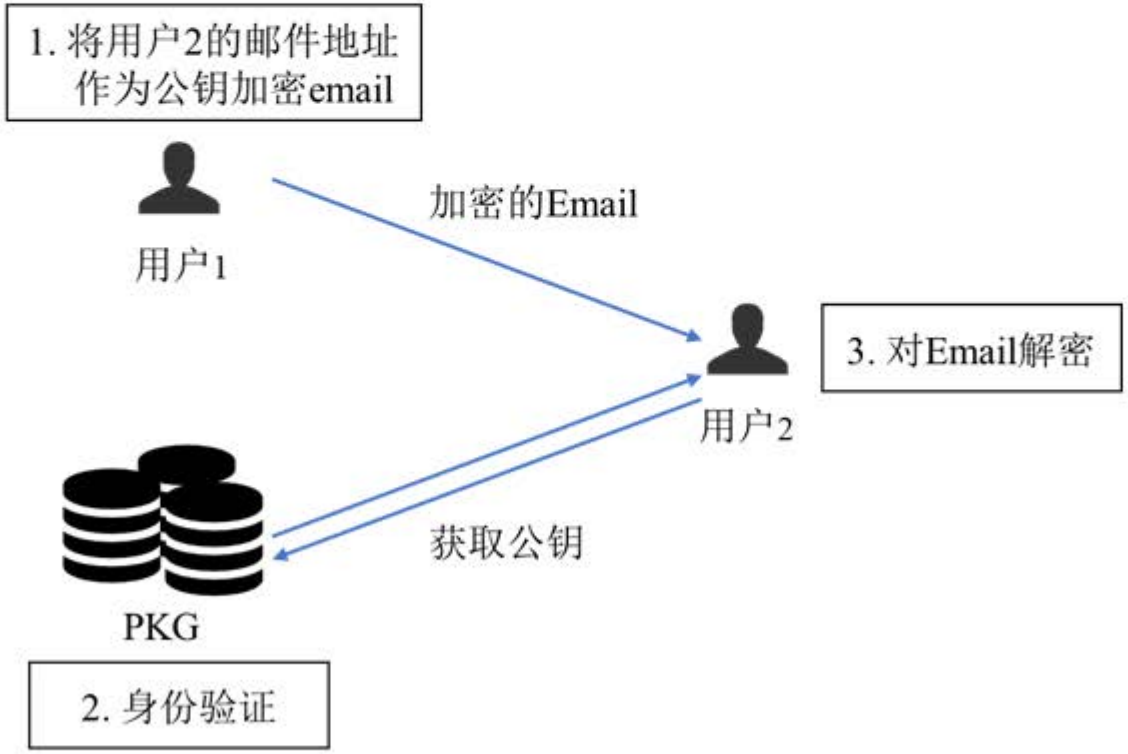
目录

安全技术

- 数据安全
- 身份认证
- 隐私保护
- 访问控制

数据安全（1）

- **基于身份加密（IBE）：**
  - 包含加密、身份认证、解密三个步骤。



数据安全（2）

- **基于属性的加密（ABE）：**
  - 两个实体：负责发布属性密钥和管理用户属性集的可信机构（TA）2.用户包括与数据相对应的消息发送者和接收者所有者和用户；
  - 基于属性的加密是一种基于属性的门限策略，只有用户属性集与密文属性集相交的元素数量达到系统规定的门限参数时才能解密。

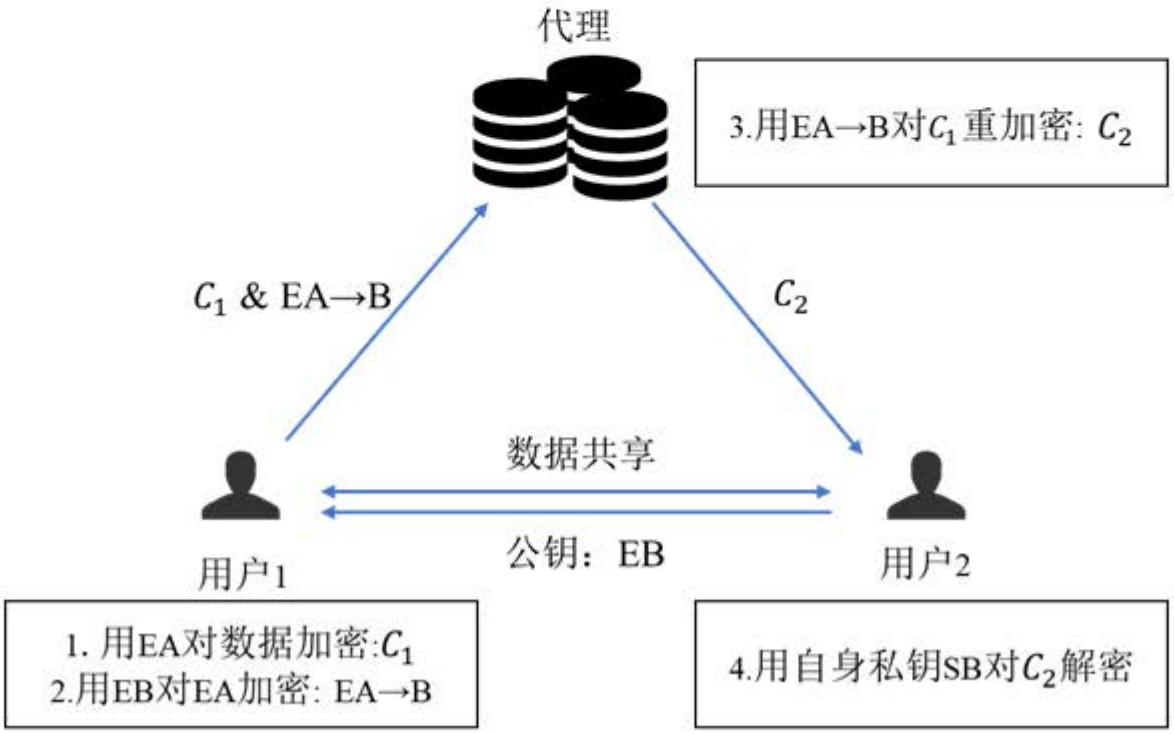
数据安全（3）

- **基于属性的加密（ABE）：**
  - 基于密钥策略属性的加密（KP-ABE）
  - 基于密文策略的加密（CP-ABE）

属性加密类型	应用	支持的策略
ABE	简单	设立门限制
KP-ABE	数据查询	AND，OR，门限制
CP-ABE	接入控制	AND，OR，门限制

数据安全（4）

- **代理重加密（PRE）：**
  - 通过使用代理将一个密钥的密文（消息或签名）转换为另一密钥的密文。



数据安全（5）

- **同态加密：**
  - 允许用户直接使用任意代数计算来操作密文。
  - 同态加密可以划分为：加法同态、乘法同态和全同态。

名称	条件
加法同态	满足：f(A)+f(B)=f(A+B)
乘法同态	满足:f(A)*f(B)=f(A*B)
全同态	同时满足:f(A)+f(B)=f(A+B) f(A)*f(B)=f(A*B)

数据安全（6）

- **可搜索加密：**
  - 可搜索加密可以在保证数据的私密性和可用性的同时，支持密文数据的查询和检索操作。其步骤包括：文件加密、生成陷门、搜索、解密这四部分。
  - 文件加密：用户使用密钥对纯文本文件进行加密并生成索引结构，然后将其密文和索引上载到服务器。
  - 生成陷门：把待查询的关键字加密生成陷门，发送到云端，其他用户或者是云服务商无法从陷门中获取关键词的任何信息。
  - 搜索：服务器以关键字陷门作为输入执行搜索算法，并返回所有包含与陷门对应的关键字的密文文件。
  - 解密：用户使用密钥对服务器返回的加密文档进行解密，得到搜索结果。

安全技术

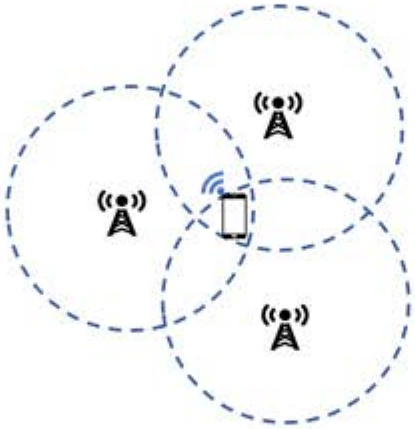
- 数据安全
- 身份认证
- 隐私保护
- 访问控制

身份认证（1）

身份认证的主要研究内容包括单一域内身份认证、跨域认证和切换认证。

用户位置固定
单个信任域得身份验证

(a)单域认证



用户位置固定
不同信任域得身份验证

(b)跨域认证

用户位置动态变化

(c)用户位置动态变化

身份认证（2）

- **单域身份认证：**
  - 单个信任域中的身份验证主要用于解决每个实体的身份分配问题。
  - 边缘计算中的实体在获得服务之前必须先从授权中心进行身份验证。
- **跨域身份认证：**
  - 关于互连边缘服务器的不同信任域实体之间的身份验证机制。
  - 从其他相关领域到边缘计算环境寻找该问题的解决方案。
- **切换认证：**
  - 由于边缘设备的高度移动性，移动用户的地理位置经常发生变化，传统的集中式身份验证协议不适用。
  - 切换认证是解决高移动性用户认证的一种有用的认证传输技术。

安全技术

- 数据安全
- 身份认证
- 隐私保护
- 访问控制

隐私保护（1）

- **数据隐私保护**
  - 数据隐私是主要挑战之一，因为用户的私人数据处理过后会从边缘设备转移到异构分布式的边缘数据服务器或者是云服务器上。
- **身份隐私保护**
  - 边缘计算范式中用户身份隐私的保护尚未引起广泛关注，仅有一些在移动云计算环境下的探索性研究成果。

隐私保护（2）

- **位置隐私保护**
  - 用户可以通过将其请求和位置信息提交给服务器来从基于位置的服务提供商（LBSP）获得各种服务。
  - 私有位置信息可能会由于用户不知道LBSP服务器是否受信任而泄漏，这将对保护在我们的日常生活中广泛使用的此类位置信息提出巨大的隐私挑战。

安全技术

- 数据安全
- 身份认证
- 隐私保护
- 访问控制

访问控制（1）

- **基于属性的访问控制**
  - 基于属性的加密是控制云计算中数据访问的一项杰出技术，可以很好地应用于分布式体系结构，并可以通过基于用户属性建立解密能力来实现细粒度的数据访问控制。
- **基于角色的访问控制（RBAC）：**
  - 对系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。
  - 每种角色对应一组相应的权限，一旦用户被分配了适当的角色后，该用户就拥有此角色的所有操作限权。
  - 可以通过用户到角色和角色到对象的权限映射机制提供灵活的访问控制和权限管理。

目录

边缘计算安全技术应用

- 区块链+边缘计算
- 联邦学习

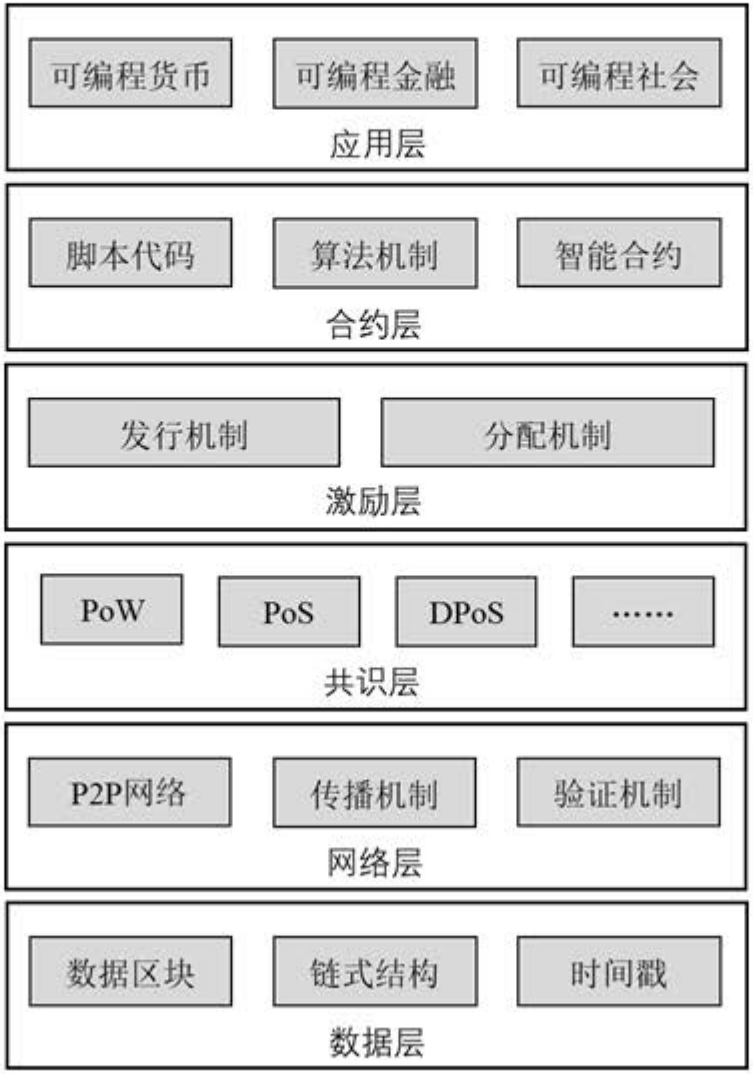
区块链+边缘计算（1）

- **边缘计算与区块链融合能提高物联设备整体效能：**
  - 移动边缘计算可以为区块链提供服务，存储和处理传回的数据，并优化和修正各种设备的工作状态和路径。
  - 存储在边缘服务器中的数据可以在区块链的帮助下保证数据的可靠性和安全性。
- **区块链以及应用：**
  - 区块链是比特币的基础支撑技术，其本质上是一个去中心化的数据库
  - 区块链技术是一个不依赖第三方、通过自身分布式节点进行网络数据的存储、验证、传递和交流的一种技术方案。

区块链+边缘计算（2）

- **区块链包括：**
  - 数据层：封装底层数据区块、相关数据加密和时间戳等网络层：包括分布式组网机制、数据传播机制和数据验证机制
  - 共识层：封装网络节点的各类共识算法
  - 激励层：包括经济激励的发行机制和分配机制等
  - 合约层：封装各类脚本、算法和智能合约
  - 应用层：封装了区块链的各种应用场景和案例

区块链+边缘计算（3）


可编程货币
可编程金融
可编程社会
应用层
脚本代码
算法机制
智能合约
合约层
发行机制
分配机制
激励层
PoW
PoS
DPoS
……
共识层
P2P网络
传播机制
验证机制
网络层
数据区块
链式结构
时间戳
数据层

区块链+边缘计算（4）

- **区块链以及应用：**
  - 比特币作为区块链的首个应用，它是一种基于密码学去中心化的货币，比特币的点对点传输意味着一个去中心化的支付系统。
  - 区块链另一个较为广泛的应用以太坊，它是一个开源的有智能合约功能的公共区块链平台，具有可编程性。

区块链+边缘计算（5）

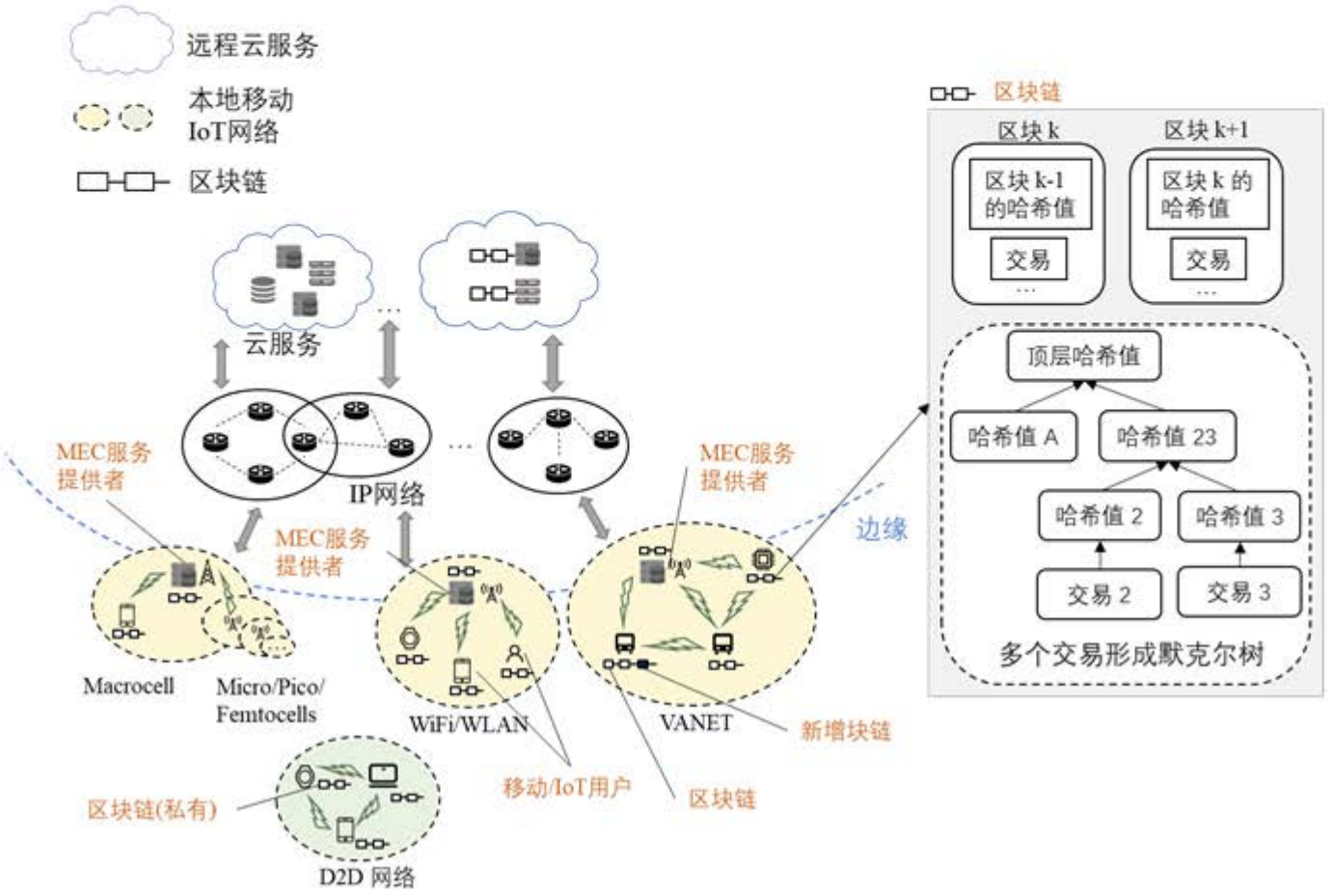
- **边缘计算为区块链服务提供资源和能力：**
  - 资源层面：区块链可以和终端节点共用边缘计算节点资源，进而可以节省云计算的开销。
  - 通信层面：区块链在边缘计算节点上的部署，降低了通信时延，从终端用户的角度，传播的路径更加可控
  - 能力层面：边缘服务器提供了强大的存储容量以及独立而机密的环境。

区块链+边缘计算（6）

- **区块链为边缘计算提供信任：**
  - 作为大规模分布式去中心化系统，区块链通过哈希链及共识算法，提供了数据永久保存及防篡改特性，可以有效地辅助解决边缘计算环境中各类安全问题。
  - 通过有效利用区块链的去中心化特性，亦可以构建去中心化文件系统、去中心化计算系统等。

区块链+边缘计算（7）

- **区块链为边缘计算提供信任：**



区块链+边缘计算（8）

- **区块链+边缘计算产生促进效应：**
  - 通过将区块链合并到边缘计算网络中，可以大大提高系统的网络安全性，数据完整性和计算有效性。
  - 边缘计算的结合使系统拥有大量计算资源和分布在网络边缘的存储资源，从而有效地减轻了功率限制设备的区块链存储和挖掘计算负担。
- **区块链+边缘计算集成需求：**
  - 身份认证：具有多个交互服务提供商，基础架构和服务的边缘计算环境中，需要验证实体的身份。
  - 适应性：需具有适应不断变化的环境的灵活性，以允许对象或节点自由连接或离开网络。

区块链+边缘计算（9）

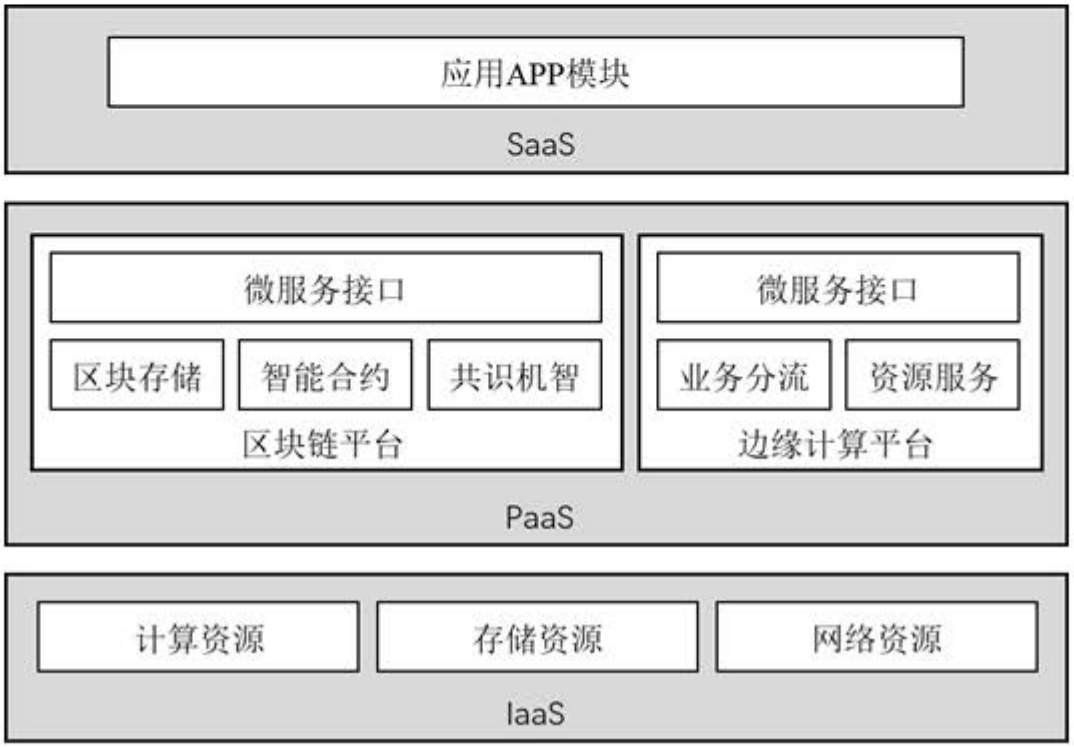
- **区块链+边缘计算集成需求：**
  - 网络安全：区块链与边缘计算的集成，可维护大规模分布式边缘服务器提供方便的访问，并可以进行更有效的监控。
  - 数据完整性：通过边缘计算的分布式存储资源，通过边缘服务器以及基于区块链的框架来为数据完整性服务复制数据。

区块链+边缘计算（10）

- **区块链+边缘计算集成需求：**
  - 可验证的计算：边缘计算中的外包计算可以扩展到大量计算。
  - 低延迟：区块链与边缘计算的集成，实现传输等待时间与计算等待时间之间的理想折衷。

区块链+边缘计算（11）

- **区块链+边缘计算的技术实践：**
  - **区块链+边缘计算的服务模式按照：IaaS服务模式、PaaS服务模式、SaaS服务模型三种服务模式进行规划。**



区块链+边缘计算（12）

- **区块链+边缘计算的技术实践：**
  - 区块链+边缘计算的服务模式按照：IaaS服务模式、PaaS服务模式、SaaS服务模型三种服务模式进行规划。
  - 区块链+边缘计算的框架：包含终端节点（设备）和边缘服务器（Fog）的基于私有区块链的本地网络、基于区块链的P2P服务器网络。
- **边缘计算+区块链的挑战：**
  - 可伸缩性增强：当将可伸缩性与去中心化和安全性一起考虑时，如何提高边缘计算与区块链融合的可伸缩性成为了一个难题。
  - 安全性和隐私性：边缘的外包服务会引起新的安全性和隐私性挑战。

区块链+边缘计算（13）

- **边缘计算+区块链的挑战：**
  - 自组织：随着边缘计算节点的增长，网络和应用程序的管理将成为巨大的挑战。
  - 功能集成：为了区块链与边缘计算网络共存，需要进行服务类型和安全级别的集成，使其具有灵活性和稳定性。
  - 资源管理：边缘计算和区块链结合，服务器的协作更加的紧密。

边缘计算安全技术应用

- 区块链+边缘计算
- 联邦学习

联邦学习（1）

- 联邦学习，主要思想是在基于多个设备上的数据集构建机器学习模型。
- 其主要优点是可以有效提高终端数据和个人数据隐私安全。
- 联邦学习特点：各个数据都保留在本地，不会泄露给别人、多个参与者联合建立虚拟的共有模型、各个参与者身份和地位对等。

联邦学习（2）

- **联邦学习解决问题和使用场景：**
  - 多方数据补充，用在样品数量不够充足，数据维度不够丰富的场景；
  - 保护数据隐私/核心价值，整个学习训练过程，没有传输任何原始数据，用来保护数据隐私安全。
- **联邦学习技术及优点：**
  - 联邦学习的步骤：Selection、Configuration、Reporting。
  - 联邦学习的优点：隐私保护性、降低延时、安全性扩展、中央服务器存在、数据传输问题、单方数据污染。

联邦学习（3）

- **联邦学习隐私保护的主要算法：**
  - 联邦学习的主要算法包括：FedAvg、联合随机方差降低梯度算法（FSVGR）、和CO-OP算法。
  - 常见的算法：FedAvg、FedProx、FSVGR、FedMA、LoAdaBoost算法。
  - FedAvg：借助主服务器来初始化训练，在该服务器上主机共享一个整体的全局模型。通过随机梯度下降算法（SGD）进行优化。
  - FedProx：要求每次迭代从新选择所需工具，执行本地更新并将其分组在一起以生成全局更新，以实现更好的性能和更好的异构性。

联邦学习（4）

- **联邦学习隐私保护的主要算法：**
  - 联邦学习隐私保护的主要算法：
  - FSVGR：进行一次完整的计算后，每个客户端上会有很多更新。每次更新都会通过对数据进行随机排列并执行来实现。
  - FedMA：全局模型是通过图层以及具有相同功能的隐藏元素进行匹配和平均构造。
  - LoAdaBoost：应用于医疗行业中，实现对医学数据的处理。

联邦学习（5）

- 联邦学习的应用：
  - Google键盘查询建议：Gboard
  - 视觉对象检测：FedVision
  - 药物发现：FL-QSAR

联邦学习（6）

- **联邦学习的应用：Google键盘查询建议：Gboard**
  - Gboard用于移动设备的虚拟键盘。
  - 通过对用户和Gboard的互动方式的观测来实现对训练数据的收集。
  - Gboard依靠Android的Job Scheduler来管理后台操作。
  - 实现对跨设备的负载的管理。

联邦学习（7）

- **联邦学习的应用：视觉对象检测：FedVision**
  - FedVision使用了基于YOLOv3的视觉对象检测框架。
  - 其六个组成部分：配置、任务计划程序、任务管理器、资源管理器、联邦学习服务器、联邦学习客户。
- **联邦学习的应用：药物发现：FL-QSAR**
  - FL-QSAR使用了水平的联邦学习架构，对定量结构-活性关系（QSAR）进行研究，进一步实现药物的发现。

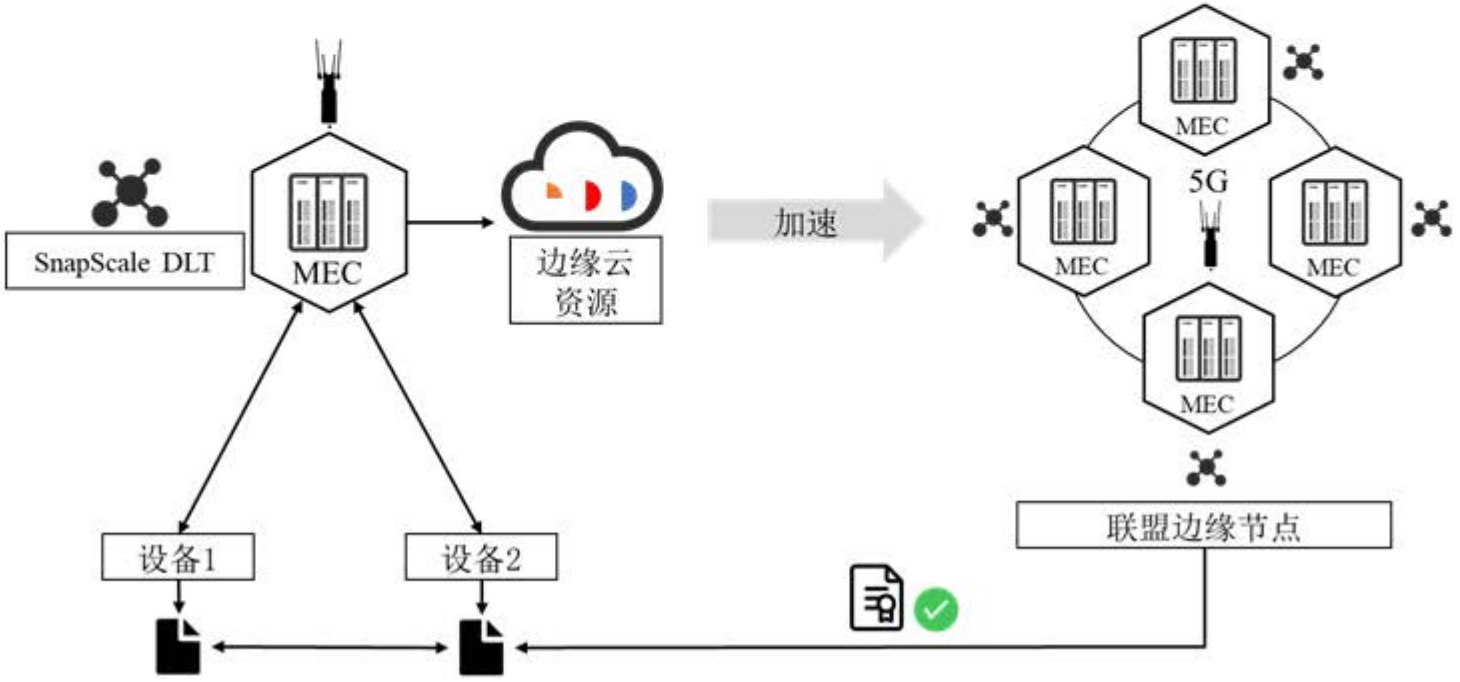
目录

隐私保护开源工具和未来挑战

- 隐私保护的开源工具
- 隐私保护未来挑战

隐私保护的开源工具（1）

- **ENIPRO：**
  - 融合云计算及区块链技术，致力于在移动网络边缘构建去中心化的物联网基础服务设施，孕育一个全新的边缘应用生态。

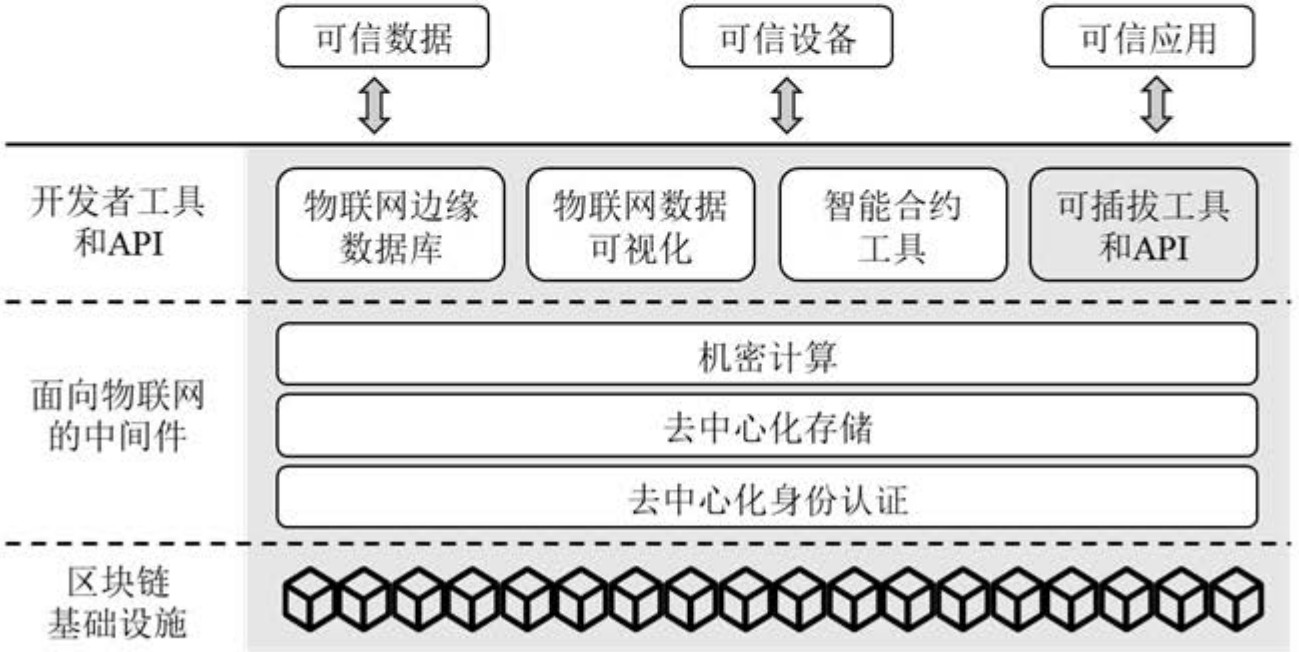


隐私保护的开源工具（2）

- **BlueJay OS：**
  - BlueJay OS针对工业特性，兼容各类工业通讯协议，能够安全快速并且简单的进行互联通讯和数据处理。
  - BlueJay OS的支持下能够实现全程加密数据交换，适用于各类需要互联与边缘计算的应用场景。

隐私保护的开源工具（3）

- **IoTex：**
  - 是一个全方位、由区块链技术、物联网中间件和多种开发工具共同组成的综合技术平台，为可信应用、设备和可信数据赋能。



隐私保护开源工具和未来挑战

- 隐私保护的开源工具
- 隐私保护未来挑战

隐私保护未来挑战（1）

- 边缘计算中基于多授权方的轻量级数据加密与细粒度数据共享新需求。
- 分布式计算环境下的多源异构数据传播管控和安全管理问题。
- 边缘计算的大规模互联服务与资源受限终端之间的安全挑战。
- 面向万物互联的多样化服务以及边缘计算模式对高效隐私保护的新要求。

本章小测

- 五个安全性能评价指标分别是什么?
- 边缘计算相较于云计算在用户安全性与隐私保护方面的优势。
- 边缘计算的体系架构可以划分为哪几个层次?
- 数据安全与隐私保护研究体系由哪四个部分组成?
- 简要说明隐私保护的未来挑战有哪些。