隐式证书下的椭圆曲线数字签名算法的批认证方法

申请号：CN201811598108 .X

专利号：ZL201811598108 .X

专利名称：边缘计算场景下支持异构终端匿名接入的轻量级认证方法

专利申请时间：2018 .12 .26

专利授予时间：2020.07.28



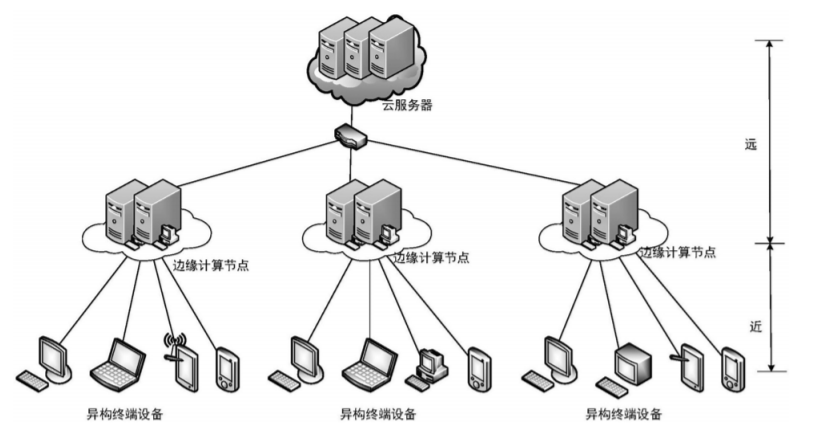
## 摘要

本发明提出了边缘计算场景下支持异构终 端匿名接入的轻量级认证方法。该发明利用云平 台为每个终端设备创建伪身份来隐藏其真实的 身份信息，同时还可以对恶意终端设备进行追 溯，在终端设备接入边缘计算节点认证过程中， 边缘计算节点可以在不与云平台通信的情况下 实现对所有接入的设备身份的合法性进行验证， 且不会学习到终端真实身份信息，保障了终端设 备的身份隐私性，提高了接入认证的效率，且可 以抵御重放攻击等常见威胁，增强了整个边缘计 算系统的安全性与可靠性，解决边缘计算场景下 资源受限的终端设备接入认证问题。

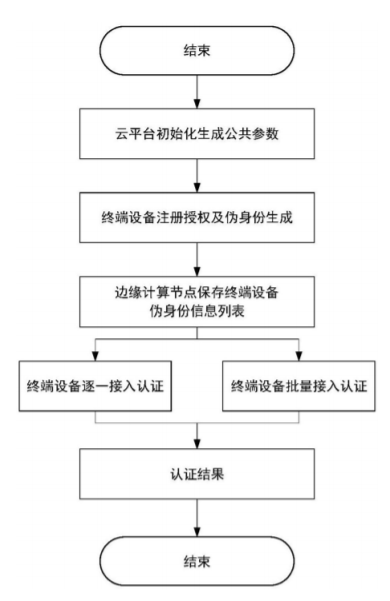
## 可能应用的场景

该发明提出的轻量级接入认证方法，能够支持对海量设备同时发送接入 请求时的批量认证，且可以实现终端设备的匿名认证和恶意终端设备的追溯，提高了海量异构终端并发接入的身份认证效率和隐私性。

该发明结合边缘计算场景下的“云—边—端”三层体系架构，提出了一种边缘计算场景下支持异构终端匿名接入的轻量级认证方法，该方法能够适用于计算资源和存储资源受限的终端设备。



该发明的边缘计算三层体系架构示意图



边缘计算场景下支持异构终端匿名接入的轻量级认证流程图