# 基于零信任架构的 IoT 设备身份认证机制研究

郭仲勇[1],刘　扬[2],张宏元[1],刘帅洲[1]

(1.河南中盾云安信息科技有限公司,河南 郑州 450018;2.河南工业大学 研究生院,河南 郑州 450001)

**摘　要**:随着物联网技术与互联网经济的发展,新技术态势下的网络安全威胁和风险不断涌现与扩散,新型应用场景致使网络安全边界模糊、增加新的暴露面,安全风险不容忽视。提出基于零信任技术,利用区块链、设备指纹、PKI/DPKI、人工智能、轻量化安全协议和算法等技术作为身份安全基础设施,重点对身份安全基础设施、物联网安全网关、感知网关节点设备等身份认证方案进行设计和优化。最后通过实验与分析,验证方案的实际效果。

**关键词**:零信任;身份认证;设备指纹;区块链;边缘计算

**中图分类号**:TP309　　**文献标识码**:A　　**DOI**:10.19358/j.issn.2096-5133.2020.11.004

**引用格式**:郭仲勇,刘扬,张宏元,等. 基于零信任架构的 IoT 设备身份认证机制研究[J].信息技术与网络安全,2020,39(11):23-30.

# Research on identity authentication mechanism of IoT devices based on zero trust architecture

Guo Zhongyong[1], Liu Yang[2], Zhang Hongyuan[1], Liu Shuaizhou[1]

(1.Henan Cnsecloud Information Technology Co., Ltd., Zhengzhou 450018, China;
2.Granduate School, Henan University of Technology, Zhengzhou 450001, China)

**Abstract**: With the development of the Internet of Things technology and the Internet economy, network security threats and risks under the new technology situation continue to emerge and spread. New application scenarios have caused the blurring of network security boundaries and increased new exposure. Security risks cannot be ignored. Based on zero trust technology, it uses blockchain, device fingerprints, PKI/DPKI, artificial intelligence, lightweight security protocols and algorithms as the identity security infrastructure. The focus is on the design and optimization of identity security infrastructure, IoT gateways, perception gateway node equipment and other identity authentication schemes. Finally, through experiments and analysis, the actual effect of the program is verified.

**Key words**: zero trust; identity authentication; device fingerprint; blockchain; edge computing

## 0 引言

物联网的安全形态体现在其体系结构的各个要素上,安全威胁不仅来自 TCP/IP 网络、无线网络和移动通信网络等传统网络,同时来自感知层。在物联网环境下,黑客利用已存在的 IoT 设备,就可以发起攻击,关联的设备会受到影响,轻则正常功能被阻塞,重则将设备变成感染源,攻击扩展到物联网各层,造成严重损害。

在严峻的安全态势和数字化转型浪潮下,网络安全问题随着新技术的发展呈现出新变化,新的安全需求促使身份与访问控制成为信息系统架构安全的第一道关口[1]。因此,需要重视 IoT 设备的身份安全,升级防护措施,提升 IoT 设备防护能力。

## 1 物联网网络安全挑战

随着物联网中数据和设备规模的扩大,风险也在不断增加,尤其在金融、智慧医疗、智能车联网、工业互联网等涉及民生的领域,物联网安全问题尤为突出,典型安全问题主要体现为以下几个方面。

### 1.1 不安全的物联网协议

绝大多数工控协议在设计之初,仅仅考虑了功能实现、效率、可靠性等方面,较少考虑安全性问题。以 Modbus 协议为例,尽管其已经成为事实上的

工业标准，但存在缺乏认证、授权、加密等安全防护机制和功能码滥用问题，导致关键数据明文传输、敏感信息泄露[2]。以 LoRa 为代表的非授权频段的低功耗广域技术，尽管保持快速发展，但其在安全性上存在诸多问题和挑战，如认证随机数过短容易被重放攻击、认证请求完整性校验码过短容易发生碰撞、加密强度不足容易被破解[3]、终端网络认证凭证没有安全存储介质致使防护等级低等。

### 1.2 不安全的节点

物联网终端普遍存在身份认证的授权机制弱、缺乏必要的安全防护能力等问题，易被攻击者利用，获取用户的身份信息，进而伪造用户身份或通信节点，并向其他终端、接入网关进行入侵和攻击[4-5]。

### 1.3 不可信的终端

物联网终端安全能力普遍较低，易成为攻击者的突破口。攻击者利用安全漏洞入侵并控制终端，发起主动攻击、窃取数据、篡改数据、污染数据源并向决策服务端回传伪造数据。

### 1.4 应用安全风险

物联网终端的应用程序存在逻辑缺陷或编码漏洞等问题，攻击者利用软件漏洞，通过植入木马、病毒等方式入侵或控制终端，并最终导致应用服务失效。

### 1.5 边缘计算带来的安全挑战

边缘计算网络体系中涉及终端智能设备、边缘计算设备、云中心等不同的功能实体。IoT 设备分布在不同的地域，具有移动性、多种方式接入网络的特点，当海量设备同时接入时，传统的集中式安全认证面临巨大的性能压力；5G 物联网装置直接接入 5G 网络云端，可能存在攻击者利用设备的脆弱性，从内部攻击云服务平台的风险；与用户身份相关联的信息存储在半可信的端智能设备、边缘计算设备等功能实体中，极易引发用户身份信息、地理位置信息等隐私泄漏问题[6]。

## 2 物联网终端设备身份认证与授权方案设计

参考零信任架构总体框架[7-8]，设计基于零信任架构的物联网终端设备身份认证与授权方案，为物联网提供安全、高效、灵活的身份管理与身份认证服务，控制对 IoT 设备数据的访问，总体框架如图 1 所示。

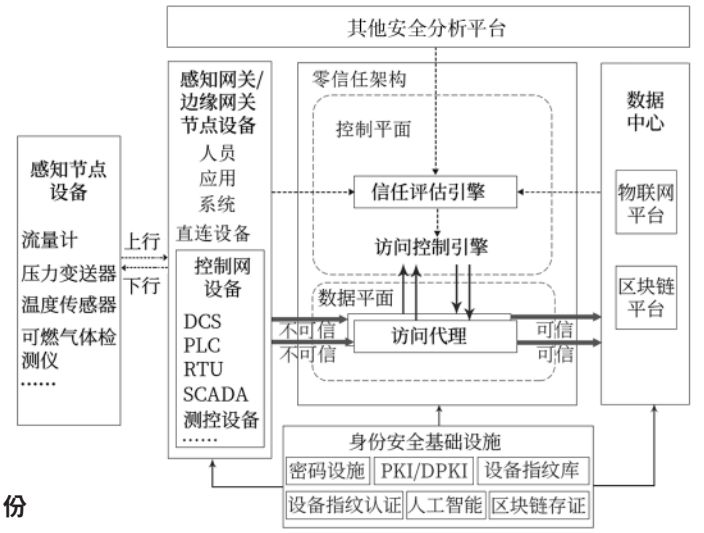


图 1 物联网零信任架构总体框架图

零信任架构遵循“从不信任并始终验证”的安全原则，将身份作为访问控制的基础，实时计算访问控制策略。根据《网络安全等级保护基本要求》(GB/T 22239-2019)，对三级及以上感知节点设备的安全要求为：“应具有对其连接的网关节点设备(包括读卡器)进行身份标识和鉴别的能力；应具有对其连接的其他感知节点设备(包括路由节点)进行身份标识和鉴别的能力”。对三级及以上网关节点设备安全要求为：“应具备对合法连接设备(包括终端节点、路由节点、数据处理中心)进行标识和鉴别的能力；应具备过滤非法节点和伪造节点所发送的数据的能力”[9]。

本文重点对数据中心、身份安全基础设施、物联网安全网关、感知网关节点设备、感知节点设备的身份认证及数据安全进行设计和优化。

### 2.1 身份安全基础设施

身份安全基础设施主要由密码设施、PKI/DPKI、设备指纹库、人工智能、区块链等功能子系统组成，如图 2 所示。


图 2 身份安全基础设施功能子系统

#### 2.1.1 密钥管理

密钥管理包括认证密钥管理、密钥载体合规性、密钥算法合规性、会话密钥管理等功能。

(1)认证密钥管理：实现认证密钥的生成、分发、验证、更新、存储、备份、有效期、销毁及密钥周期管理功能；

(2)密钥载体合规性：采用合规的密码算法芯片，密钥存储及密码运算均在芯片内实现，确保密钥及密码运算的安全性。

(3)密钥算法合规性：采用标准的 API 函数提供密码服务，支持国密 SM1、SM2、SM3、SM4、SM9 等系列商用密码算法和 AES、RSA、SHA256 等国际主流密码算法，提供数据加解密、签名验证、杂凑等密码运算服务，实现信息的机密性、完整性和有效性保护。

(4)会话密钥管理：实现会话密钥协商生成、存储、销毁、备份、有效期、恢复及密钥周期管理功能。

(5)密码服务中间件：密码中间件提供通用的、标准化的密码服务，提高模块的可重用性，降低开发难度。

2.1.2 PKI/DPKI

(1)公共密钥基础设施(PKI)：对接证书签发机构，用于在证书生命周期中对数字证书的规范管理。实现对自然人、机构及设备等数字证书及密钥签发，提供证书验证、数字签名、数据加解密、应用系统接口等服务。

(2)分散式公钥基础设施(DPKI)：对接证书签发机构，采用分布式身份标识(DID)为物联网分配全局唯一的标识[10]，为设备实体颁发身份凭证并存储在身份安全基础设施的区块链中，赋予设备可声明、可验证的自主身份，保障数据来源的真实有效性。设备实体作为凭证所有者建立连接时，需要向凭证验证者提供身份声明，验证者通过对链上的凭证验签来验证设备实体的身份声明，通过验签则授权访问相应的资源。

2.1.3 设备指纹库

基于设备硬件参数、系统配置、网络环境、传感器、信号等多维度的设备信息，通过模型算法生成唯一的设备标识符，即设备指纹。设备指纹的生成规则放到云平台服务器中，在设备管理的注册环节根据设备参数自动生成设备指纹，存放在设备指纹库中。设备登录认证过程中，根据采集到的多维度设备信息，云平台服务器模型算法对采集的数据进行分析，计算该设备的设备指纹，与设备指纹库进行匹配，实现增强认证。

2.1.4 人工智能

通过采集硬件信息、软件信息、环境信息和网络信息，经过机器学习、集成模型、深度学习，智能调整权重、升降规则，实施数据平面和控制平面特定规则、过滤和检测异常数据等。将硬件设备 ID、地理坐标、网络地址等属性建立学习模型，计算设备指纹信息。设备指纹信息用于网络身份认证，每次数据采集时根据实际设备信息可动态计算设备指纹信息，根据安全级别要求，结合学习模型，可适配设备信息全因素身份认证或者部分因素身份认证[11]。

2.1.5 区块链存证

运用区块链技术的去中心化和不可篡改，同时结合司法创新，构建区块链存证子系统。

(1)数据存证管理：支持数据结果存证、原数据存证，并进行数据目录记录，可让需求匹配到所需数据，并通过 Hash 确定数据存证的对比验证数据的有效可信。

(2)智能合约管理：通过智能合约自动执行物联网安全网关接入云平台的认证、授权以及上传终端数据，通过共识机制在云平台节点之间进行共识出块、上链存储。

(3)查验管理：根据区块 ID、受理号等信息在链上进行查验、浏览。

2.2 物联网安全网关设计

根据部署位置、计算和存储能力的不同，物联网网关可分为感知层网关、边缘层网关、平台层网关，部署在图 1 的感知网关节点、边缘网关节点和物联网平台中。本文将符合保密要求的具有身份认证、授权与数据安全等功能的网关统称为物联网安全网关，子系统如图 3 所示。


图 3 物联网安全网关功能子系统

(1)安全管理

安全管理子系统包括如下内容：

①身份认证：物联网终端与安全网关进行通信时，需要通过轻量级安全认证协议或算法，进行双向认证。物联网安全网关与云平台通信时，由身份安全基础设施进行双向身份认证。

②安全传输：物联网终端与安全网关传输数据，需要通过安全协议或轻量级算法，对指令和采集的数据进行加密传输。物联网安全网关与云平台通信时，可根据安全传输协议、安全芯片、加密卡、安全TF卡、数字证书等，实现数据的加密传输。

③防火墙：支持配置防火墙策略的包过滤，可以根据需求定制访问控制策略、访问控制表、NAT规则等保障网络不受外界攻击；物联网终端向安全网关传输数据时，能够阻止来自上层信息网的威胁。

④协议识别与过滤：识别协议类型，根据协议白名单，阻断非授权的网络数据包。

⑤VPN：支持配置IPSec、GRE、L2TP、OpenVPN、数字证书，通过隧道技术、加解密技术、密钥管理技术和身份认证等技术，建立虚信道，在链路层和网络层，加密与压缩隧道数据，保障数据安全传输。

⑥更新保护：为了保障操作系统内核安全，防止系统文件被恶意篡改更新，只有经过数字签名并被认证的系统文件才会被更新运行。

⑦访问控制：对物联网安全网关的管理访问权限按账户类型进行分级管理。通过入侵检测引擎以及访问控制引擎，能够对物联网接入设备进行安全访问控制、疑似业务阻断，有效降低来自感知层的业务风险，减少网络层的攻击行为。

(2)密钥管理

内容与2.1.1节密钥管理相同。

(3)系统管理

系统管理子系统包括如下内容：

①对安全网关进行管理，如注册管理、权限管理、网络接口配置、网络服务配置、静态路由、状态监管、系统时间、系统日志、配置管理、固件升级、用户管理、主机属性管理等。

②对子网内的节点进行管理，如获取节点的标识、现场名称、资产编号、定位源、LBS上报间隔、心跳间隔、流量上报间隔、状态、属性、能量等，以及远程实现唤醒、控制、诊断、升级和维护等。

(4)轻节点管理

在物联网安全网关中部署区块链BaaS服务提供的SDK，提供数据上链、数据验证、区块交易查询等接口功能。

①数据上链：数据采集程序调用上链接口，上传采集到的数据及其业务编号，云平台共识节点服务器对接收到的待上链数据进行共识，共识成功后上链存储。

②数据验证：根据数据业务编号，通过调用区块链BaaS服务数据验证接口验证所存储数据是否被篡改。

③区块交易查询：根据业务编号查询数据所在交易、所在区块以及所在交易的源数据。

(5)边缘计算

在“云边端”一体化网络架构下，重点解决边缘节点引入带来的物联网身份认证、数据安全和隐私保护等问题。

①在网关中配置加密板卡，通过中间件提供的API实现身份认证、数字签名、数据安全、隐私保护等功能[12]，有效减缓网络带宽压力，降低处理时延。

②在网关中提供足够的网络、计算、存储、应用等核心服务能力的开放计算方式，可实现传感器数据的收集、分析与处理，并与云平台协同工作，能够通过历史数据进行自我训练和学习。

2.3 物联网感知网关节点设备

感知网关节点设备位于底层现场，能够对采集的数据进行汇总、处理或数据融合，并进行转发。为防止数据被篡改，可调用BaaS服务，将数据上传区块链节点存证。

(1)身份标识与鉴别：根据分类分级安全管理要求，可采用密码芯片、低功耗加密板卡/密码模组、可信芯片+可信操作系统、软件SDK等多种安全载体，可存储密钥，提供多种密码运算服务。对感知网关节点设备进行升级并设定唯一性标识，能对网关节点设备(包括读卡器)进行双向身份鉴别，能够对数据进行加密传输。

(2)指令及数据安全：对于身份认证及数据传输过程中相关参数、指令和数据进行加密传输。

(3)协议识别与过滤：识别协议类型，根据协议白名单阻断非授权的网络数据包。

(4)上链存证：部署区块链系统“轻节点”服务，通过将采集到的数据经过协议转换、分析处理后，进行签名打包处理，调用区块链系统BaaS服务，完成数据的上链存证。

身份认证流程如图4所示。

2.4 物联网感知节点设备

根据应用场景的不同主要分为单一功能终端和通用智能终端。单一功能终端仅满足单一应用或

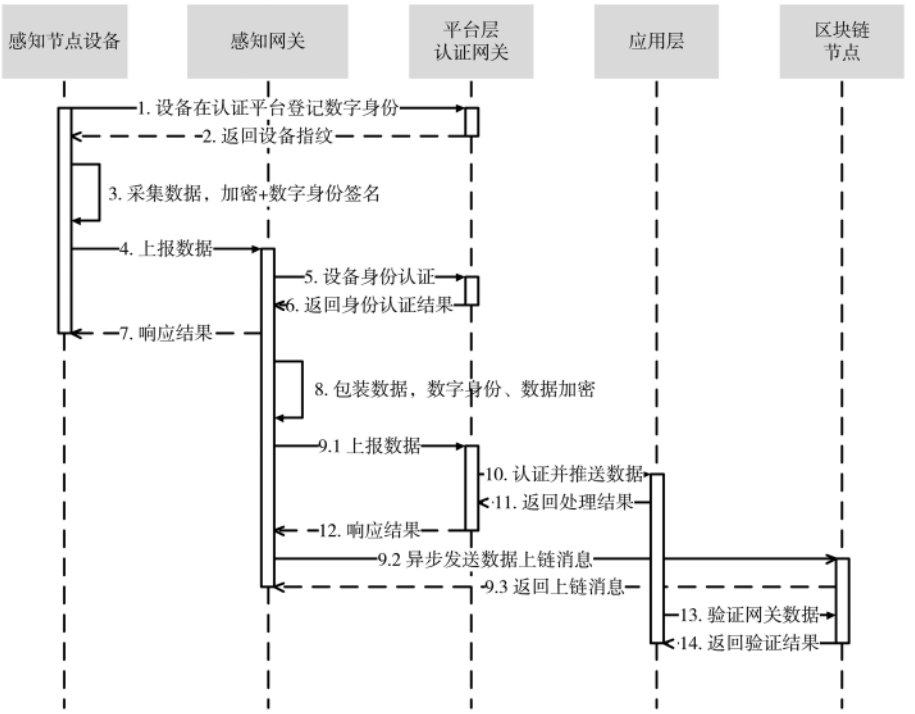


图 4 物联网安全网关节点设备身份认证流程

单一应用的部分扩展，感知芯片或设备只能自动感知外部环境变化和通信。通用智能终端能满足更多场合的应用，能对传感器进行调节，适应周边环境的运动能力，具有网络连接的有线、无线多种接口方式，甚至预留一定的输出接口用于对其他感知节点设备进行身份鉴别与控制。

(1)身份标识与鉴别：对于感知芯片或设备，由于计算和存储资源有限，可采用轻量级密码算法加密信息帧的数据、差错校验域进行加密算法增强。也可以定制轻量化安全协议，添加扩展选项，在信息帧中传输感知芯片或设备的唯一指纹，能对物联网安全网关节点设备进行双向身份鉴别，对数据进行加密传输。对于智能处理能力的终端设备的身份标识与鉴别设计，可参考物联网安全网关节点设备。

(2)指令及数据安全：对于身份认证过程中相关参数以及指令和数据进行加密传输。

(3)协议识别与过滤：识别协议类型，对其连接的网关节点设备(包括读卡器)，根据协议白名单，阻断非授权的网络数据包；对其连接的其他感知节点设备(包括路由节点)，能够识别协议类型，进行协议过滤并解决一包多发、粘包、冗余数据等问题。

感知节点设备身份认证流程如图 5 所示。

## 3 实验流程与结果分析

### 3.1 实验环境

实验环境主要有多种气体检测设备、感知网关、平台层认证网关、零信任安全接入与监管应用及区块链节点。感知网关为汉威 SS100，主机标配为 Linux 系统，支持 C/C++二次开发，支持本地硬盘最大 12 TB 容量，支持防火墙、OPENVPN、安全审计黑白名单 IP 地址、MAC 地址协议过滤等功能。采用云安链搭建联盟链、中盾多维身份认证服务器作为平台层认证网关，构建零信任安全接入和数据中心实验环境。

### 3.2 实验效果

#### 3.2.1 多种气体检测设备与感知网关身份认证及数据安全

实验使用多种气体检测设备采集数据，使用感知网关接收数据并对数据进行分析。本次实验中设备将提前到感知网关进行注册登记，并在平台层认证网关注册数字身份。感知网关每次接收数据都会对设备进行身份认证，身份认证过程如下：

(1)$s_1=H(\mathrm{UID}+M_1+e_1)$，$H()$为 SM3 算法函数，设备对采集数据原文 $M_1$、设备唯一标识 UID 与设备指纹 $e_1$ 进行摘要运算得出签名结果 $s_1$，$s_1$ 用于设备的身份验证。

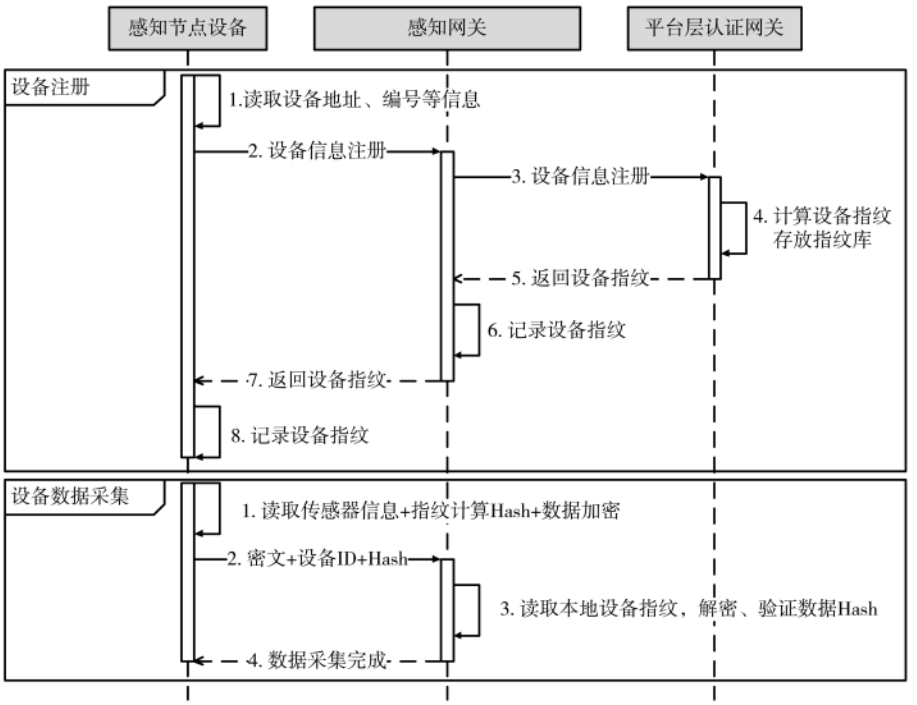


图 5 物联网感知节点设备身份认证流程

(2)$M^1=E(M_1,e_1)$,$E()$为 SM4 算法加密函数;加密采集数据原文,得出密文 $M^1$。

(3)$d=\mathrm{UID}+M^1+s_1$,将设备 UID、采集数据密文 $M^1$、签名结果 $s_1$ 拼接得出新的传输数据为 $d$。

(4)感知网关解析 $d$,得到设备 UID、采集数据密文 $M^1$、签名结果 $s_1$,感知网关根据设备 UID 查询出本地留存设备指纹为 $e_2$。

(5)$M_2=D(M^1,e_2)$,$D()$为 SM4 算法解密函数;解出数据 $M_2$。

(6)设备指纹身份认证为比较签名,动态计算摘要 $s_2=H(\mathrm{UID}+M_2+e_2)$;比较 $s_1$ 与 $s_2$ 是否一致,如果一致,设备身份认证通过,$M_2$ 为有效数据。

本节实验多种气体采集数据如表 1 所示,密文传输数据 $M^1$ 如图 6 所示,检测整体耗时为 512 ms,设备唯一标识 UID、设备指纹 $e_1$ 和设备采集数据原文 $M_1$ 如下:

表 1 多种气体采集数据

| 测量气体 | 测量值 |
|---|---|
| $CO_2$ | 408 ppm |
| CO | 38 ppm |
| NO | 7 ppm |
| $O_2$ | 21.7% |
| $SO_2$ | 2.2 ppm |
| $O_3$ | 0.03 ppm |
| $NO_2$ | 2.8 ppm |
| $H_2S$ | 0.2 ppm |

UID:16fe1d0d136f484119be14db137d7e8b

$e_1$:df9a1470174e405f1f6619ca6c2200c6

$M_1$:01980026000700d900160003001c0002

### 3.2.2 感知网关与平台层身份认证及数据安全

感知网关可通过设备证书来进行身份认证,通信前需要在平台层认证网关进行登记注册感知网关信息。感知网关与平台层认证网关之间通过协商密钥对数据加密传输,感知网关将数据上传到平台层认证网关的同时,调用 BaaS 服务接口将数据 Hash 上链存证。

本次测试的感知网关的 UID 为:73e92e30461c4e-48b0b21d7f0099481b,协商密钥为:f156d32edcbc488f9-1736e37a606db70。

(1)感知网关数据上传

感知网关将数据通过平台层认证网关的接口,将数据拼接为 JSON 格式上传到平台层认证网关。感知网关需要使用在平台层认证网关注册的非对称密钥对需要上传的数据通过 SM2 算法进行签名,平台层认证网关对接收到的签名值进行验证。平台层认证网关的接口如表 2 所示。

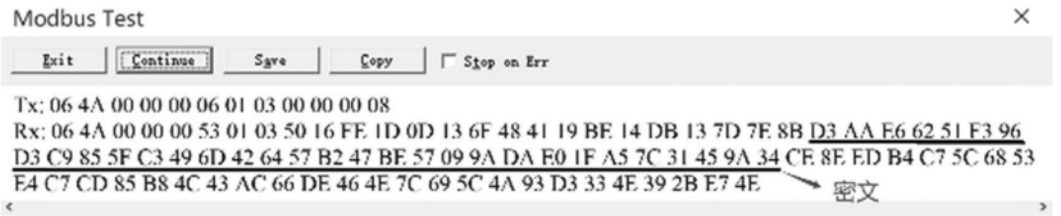


图 6 感知网关接收多种气体检测设备密文数据

表 2 平台层认证网关接口

| 字段名 | 类型 | 说明 |
|---|---|---|
| timestamp | String | 时间戳 |
| nonce | String | 随机数 |
| uid | String | 网关 id |
| signa | String | 签名值 |

本实例发送的测试数据的 URL 参数如下：

UID=73e92e30461c4e48b0b21d7f0099481b&timestamp=1600067951000&nonce=9e166f89042e401bb677f63b574359d5&sign=MEUCIAbnReYtkLM6Gpljxe+/Ggd+BfbcNjiR5HJsLPLEhYuIAiEA3OVGMSJOi0/VeeQH4z/DAr+LfXpVmBvcHn3vlySqs5A=

Post 密文为：

/ijXMp5E+d1wNw0OB7S2v62MLIMznr0kNOHOUUPb9i/wb4g0Z68k0CKmTvx1u2SzNofZ0EFOej867LpxGFUZ4TSMX+l9zG/AZ6HxUT3TzFrO/yYb5xMjGR2FGrFeDwaE0ZN/WZN26YOhj0bkFq2iTg==

Post 密文为数据量检测设备 id、采集数据时间戳、本次采集唯一序号以及采集到的数据经过 SM4 算法加密后的密文。

平台层认证网关通过身份验证，并根据协商密钥解密出 Post 明文内容为：

["16fe1d0d136f484119be14db137d7e8b,1600067951000,13057926245061795 84,01980026000700d900160003001c0002"]

数据上传耗时为 98 ms。

(2)感知网关数据上链存证

感知网关调用区块链接口，将数据经过 SM3 算法计算后的 HASH 上传到区块链节点，数据上链的接口定义如表 3 所示。

感知网关上链存证数据如图 7 区块链浏览器所示。

## 4 结论

“新基建”促进物联网产业新发展，促进消费性、公共性、生产性物联网终端应用渗透到各行各业，这些联网设备将会产生大量数据。如何安全有效地利用这些数据和发掘数据价值、提高社会生产效率、优化资源、降低成本是物联网发展的重点。在工业物联网场景中，传感技术与计算机技术、通信技术融合与协同所带来的数据安全与身份安全保护的难度也将面临巨大挑战。本文针对物联网安全问题提出基于零信任技术，从云网边端综合治理，打造云、边、端一体化协同解决方案，提供更高效的身份认证服务，便于各子系统之间实时数据的安全交流和共享，推动数字经济快速发展。下一步将对物联网安全开展进一步研究，对物联网的攻击、检测和

表 3 数据上链的接口定义

| 字段 | 说明 |
|---|---|
| extension | 上链内容 |
| Sign | content 字段内容签名，算法为 SM3WithSM2 |
| version | 版本号，默认为 1.0 |
| content | 交易信息，内容为 JSON 字符串 |
| content.UID | 上链身份标识 |
| content.type | 业务合约类型 |
| content.hash | 上链内容 Hash |
| content.timestamp | 时间戳 |


图 7 浏览器查验感知网关上链存证数据

防御等多方面进行切入，完善系统性研究。

参考文献


[1] 李雄.多种环境下身份认证协议的研究与设计[D].北京：北京邮电大学，2012.

[2] 杨庚，许建，陈伟，等.物联网安全特征与关键技术[J].南京邮电大学学报(自然科学版)，2010，30(4)：20-29.

[3] 武传坤.物联网安全关键技术与挑战[J].密码学报，2015，2(1)：40-53.

[4] 钱明茹.物联网中基于属性的安全访问控制研究[D].沈阳：辽宁大学，2013.

[5] 张玉婷，严承华，魏玉人.基于节点认证的物联网感知层安全性问题研究[J].信息网络安全，2015(11)：27-32.

[6] 张佳乐，赵彦超，陈兵，等.边缘计算数据安全与隐私保护研究综述[J].通信学报，2018，39(3)：1-21.

[7] KINDERVAG J.Build security into your network′s dna：the zero trust network architecture[R].Forrester Research Inc，2010：1-26.

[8] 中国信息通信研究院，奇安信科技集团股份有限公司.网络安全先进技术与应用发展系列报告：零信任技术[R].中国信息通信研究院安全研究所，2020.

[9] 马力，祝国邦，陆磊.《网络安全等级保护基本要求》(GB/T 22239-2019)标准解读[J].信息网络安全，2019(2)：77-84.

[10] PATEL A，BUCHNER D J.Generating and managing decentralized identifiers：U.S.，Patent 10，742，411[P].2020-08-11.

[11] 姚远，孔德春，李亮.基于设备基因图谱的物联网终端身认证法研究[J].江苏通信，2019，35(6)：38-41.

[12] 岳勇，郭仲勇.5G 架构下物联网安全与智能应用设计与实现[J].信息周刊，2020(4)：1-4.


(收稿日期：2020-09-30)


作者简介：

郭仲勇(1973-)，男，本科，主要研究方向：信息安全、区块链技术、物联网安全。

刘扬(1978-)，女，博士，教授，CCF 专委委员，主要研究方向：分布式计算、云计算、区块链。

张宏元((1993-)，男，本科，主要研究方向：信息安全、区块链技术。