

罗滔. 基于多级鉴权的物联网数据接口管理技术研究[J]. 智能计算机与应用, 2024, 14(12): 176-179. DOI: 10.20169/j.issn.2095-2163.241225

基于多级鉴权的物联网数据接口管理技术研究

罗滔

(中冶南方城市建设工程技术有限公司, 武汉 430223)

摘要: 随着物联网的快速发展,大量的设备和传感器通过数据接口进行数据交互。然而,这种数据交互过程中存在着安全风险,如未经授权的访问、数据篡改和信息泄露等。本文旨在研究并提出一种基于多级鉴权的物联网数据接口管理技术及实现方式,通过多层分级鉴权机制对数据接口服务进行权限管控,同时通过集成安全传输加密技术来进一步提升物联网系统的安全性和可靠性。

关键词: 物联网平台; 鉴权机制; 安全传输; 数据接口管理

中图分类号: TP311

文献标志码: A

文章编号: 2095-2163(2024)12-0176-04

Research on Internet of Things data interface management technology based on multilevel authentication

LUO Tao

(WISDRI City Construction Engineering & Research Incorporation Ltd., Wuhan 430223, China)

Abstract: With the rapid development of the Internet of Things, a large number of devices and sensors interact with each other through data interfaces. However, there are security risks in this data exchange process, such as unauthorized access, data tampering, and information leakage. This paper aims to research and propose a multi-level authentication based IoT data interface management technology and implementation method. By using a multi-level hierarchical authentication mechanism to control the permissions of data interface services, and integrating secure transmission encryption technology, the security and reliability of IoT systems are furtherly improved.

Key words: IoT platform; authentication mechanism; secured transmission; data interface management

0 引言

物联网是指通过互联网连接和交互的各种物理设备、传感器和对象的网络,使得设备能够互相通信、共享数据并自动执行任务,从而实现智能化、自动化和实时化的应用,并且还能将部分数据分析计算功能前置。物联网的构建源于信息技术、通信技术和传感器技术的快速发展,随着计算能力的提升、互联网的普及和传感器成本的降低,越来越多的设备和物体可以连接到互联网,形成一个庞大的物联网生态系统^[1]。物联网的应用涵盖了各个领域,包括智能家居、智能城市、工业自动化、交通运输、医疗保健、农业等。通过物联网,设备可以实时收集和共享数据,实现智能化的决策和操作,提高效率、降低成本、改善生活质量^[2]。

物联网的广泛应用给人们的生活带来了巨大的便利,但同时也面临着安全挑战。数据接口是物联网设备之间进行数据交换的关键环节,对其进行有效管理和安全保护至关重要。本文介绍了多级鉴权的概念,并提出了一种基于多级鉴权的物联网数据接口管理技术,旨在提升当前物联网数据安全接口方面的保障水平,为解决其中存在的问题提供一种可选方案^[3]。

1 技术的发展现状

目前,面对物联网产生的海量数据,众多学者都在致力于高效数据处理和分析技术的探讨及研发。其中,包括数据挖掘、机器学习、人工智能等方法,用于从物联网数据中提取有用信息和知识,因此物联网的安全和隐私保护是当前研究的重要方向。由于

物联网涉及大量敏感数据和设备连接,为了进一步确保数据的机密性、完整性和可用性,有关用户隐私的保护也已成为重要关注的焦点之一^[4]。

在另一层面,为了实现设备之间的互联互通,研究人员和工业界正着力开展更加安全可靠的物联网标准和协议的制定工作,这有助于不同厂商的设备能够无缝地连接和交互,促进物联网的发展和应用^[5]。需要注意的是,物联网是一个涉及多学科交叉的快速发展领域,相关研究涵盖了计算机科学、通信技术、电子工程、数据科学、信息安全等多个领域的知识。研究人员和从业者需要持续关注最新的技术和趋势,以推动物联网数据安全的进一步创新发展。

2 研究的目的及意义

多级鉴权技术对物联网平台在数据管理方面具有重要的意义和作用,主要体现在以下几个方面。

(1) 提供安全保障。物联网平台连接了大量的物理设备和传感器,涉及到大量的数据交换和共享。多级鉴权技术可以确保只有经过授权的设备 and 用户能够访问和操作相关资源,防止未经授权的访问和潜在的安全威胁。

(2) 实现访问控制。多级鉴权技术可以实现细粒度的访问控制,对不同的设备和用户进行权限管理。通过多级鉴权,可以限制特定设备或用户的访问权限,确保数据和系统的安全性。

(3) 管理多种身份和角色。物联网平台中存在各种类型的设备和用户,具有不同的身份和角色。多级鉴权技术可以管理和识别这些不同的身份和角色,并为每个身份和角色分配相应的权限,从而保证资源的合理访问和使用。

(4) 支持复杂的授权策略。物联网平台的应用场景复杂多样,涉及到多种授权策略和场景。多级鉴权技术可以根据具体需求,灵活地配置和管理不同的授权策略,满足不同场景的要求,提供定制化的访问控制方案。

(5) 促进合作和实现互操作性。物联网平台通常涉及多个厂商和不同的系统组件。通过多级鉴权技术,可以建立统一的身份验证和访问控制标准,促进不同厂商和组件之间的合作和实现互操作性,提高整个物联网生态系统的协同效率。

总的来说,多级鉴权技术可以为物联网的数据管理提供安全保障、实现访问控制、管理多种身份和角色、支持复杂的授权策略,并促进合作和互操作

性。这也是构建安全、可信和可扩展的物联网平台的关键要素之一。

3 主要研究内容

本文设计一种适用于物联网数据接口的多级鉴权机制,主要包括基础鉴权层、业务鉴权层、数据鉴权层和风险控制层。通过分层分级的管控措施和访问方案来达到物联网平台数据接口鉴权管理功能,充分保障数据服务的安全性和可控性。对此可展开研究论述如下。

(1) 基础鉴权层。基础鉴权层是多级鉴权机制的核心层,负责验证设备和用户的身份。具体来说,包括身份验证和身份授权两个关键步骤。其主要功能包括:

① 身份验证:通过用户名和密码、数字证书、令牌等方式验证设备或用户的身份。

② 身份授权:一旦身份验证成功,基础鉴权层将给设备或用户分配鉴权级别和访问权限,以决定其访问资源和执行操作的能力。

(2) 业务鉴权层。业务鉴权层根据特定业务需求和角色定义访问策略,对设备和用户的访问进行细粒度的控制。其主要功能包括:

① 角色管理:定义不同角色和权限,如管理员、操作员、终端用户等,根据其职责和访问需求进行区分。

② 授权策略定义:为每个角色定义具体的授权策略,确定其能够访问的资源、允许的操作和其他访问限制。

③ 访问控制:根据设备或用户的角色和授权策略,对访问请求进行验证和控制,确保只有具备合法权限的设备和用户可以访问和操作资源。

(3) 数据鉴权层。数据鉴权层用于保护物联网平台中的数据资源,确保只有经过授权的设备 and 用户可以访问和使用数据。其主要功能包括:

① 数据访问控制:定义数据资源的访问策略,确定哪些设备和用户可以访问特定的数据资源。

② 数据加密和解密:对敏感数据进行加密,确保数据在传输和存储过程中的安全性。只有授权的设备 and 用户能够解密和使用加密的数据。

③ 数据审计和监控:跟踪和记录数据的访问情况,监控数据的使用和滥用情况,以及及时检测和应对安全事件。

(4) 风险控制层。风险控制层用于识别和应对潜在的安全风险和威胁,确保物联网平台的安全性。

其主要功能包括:

① 异常检测和预警:通过监控设备和用户的行为,识别异常访问和潜在威胁,并及时发出警报和预警。

② 安全策略更新:根据最新的安全威胁和漏洞,不定期更新安全策略和授权策略,以能够持续应对新的安全挑战。

③ 威胁响应和应急措施:当发生安全事件或威胁时,风险控制层能够及时采取相应的响应和应急措施,包括阻止访问、断开连接等,以保护系统和数据的安全。

通过以上4个层次的多级鉴权机制,可以实现对物联网数据接口的全面管理和安全控制,保护设备及用户的身份和数据的安全,降低潜在的安全风险和威胁。同时这种机制具有良好的灵活性、可扩展性和可定制性,能够适应不同物联网应用的需求和安全性要求。

此外,通过基于SSL/TLS协议和IPSec等技术的数据接口加密和安全传输方案可提供强大的安全性和保护机制,确保物联网数据在传输过程中的机密性和完整性。这些技术的数据接口加密和安全传输方案可以有效保护物联网中的数据,防止数据在传输过程中被窃取、篡改或伪造。该技术提供了强大的加密和认证机制,确保数据的机密性、完整性和可靠性。同时,这些方案也支持双向身份验证,确保通信双方的真实性和合法性,从而进一步提升整个物联网系统的安全性和可靠性。

4 系统的主要技术路线

物联网数据接口管理系统的总体架构和实现方式可以根据具体需求和场景而有所不同,本文提出的技术线路主要包括以下关键组件和实现方式:

(1) 数据接口管理器(API Manager)。数据接口管理器是整个系统的核心组件,负责管理物联网数据接口的注册、发布、授权和监控等功能。并提供了用户友好的接口,允许管理员或开发者管理和配置接口的访问权限、限制配额、监控接口使用情况等。

(2) 访问控制和认证模块。用于实现对数据接口的访问控制和认证,确保只有经过授权的用户、设备或应用程序能够访问接口。也可以采用各种访问控制策略,如ACL、RBAC、ABAC等,进行身份验证和权限管理。该模块还可以集成单点登录(SSO)和身份提供商(IdP)等技术,实现跨平台的用户身份验证。

(3) 接口注册和发布模块。用于注册和发布物联网数据接口,使其可供其他应用程序或设备使用。该模块提供了一个统一的接口注册表或目录,记录接口的元数据、访问权限和其他相关信息。开发者可以通过该模块注册新的接口,并定义接口的访问规则和参数。

(4) 接口调用和数据传输模块。用于处理数据接口的调用请求和数据传输。能接收来自客户端的请求,并根据访问控制规则验证请求的合法性。一旦验证通过,就会调用相应的接口服务,能将数据传输反馈至客户端。这个模块还负责处理数据格式转换、协议转换和数据加密等操作,以确保数据的安全传输。

(5) 监控和日志模块。用于监控和记录数据接口的使用情况、性能指标和错误日志。可以收集接口调用次数、响应时间、数据传输量等指标,用于性能优化和容量规划。同时,还可以记录错误日志和安全事件,便于故障排查和安全审计。

(6) 集成和扩展接口。物联网数据接口管理系统通常需要与其他系统和平台进行集成,以实现数据的共享和交互。可以提供标准的接口和协议,允许其他系统与之集成。同时,系统也应该具备可扩展性,允许添加新的接口服务和功能模块,以满足不断变化的需求。

在整个研究过程中,如何优化多级鉴权过程的整体性能也是确保系统高效运行的关键。在鉴权过程中,平台将初次鉴权的分析结果基于一定的规则进行缓存,下次相同的鉴权请求到达时,直接从缓存中获取结果,避免进行重复的鉴权操作。缓存可以采用内存缓存、分布式缓存或者使用专门的缓存服务,如Redis等。并通过灵活的缓存配置功能合理设置缓存的过期时间和缓存策略,这样能够一定程度地提高系统的响应速度和吞吐量。

同时在大型的业务系统的应用过程中,物联网平台可能会面临大量的并发请求,为了平衡负载和提高系统的稳定性和性能,可以使用负载均衡技术。负载均衡将请求分发到多个鉴权节点或服务器,确保每个节点都能够处理合理的负载。常见的负载均衡算法包括轮询、最少连接和基于权重等。通过负载均衡,可以提高系统的并发处理能力和响应速度。而针对某些耗时边缘计算过程,平台会为这些计算设计为异步处理,当鉴权请求到达时,可以先返回一个异步任务的标识或状态,然后在后台进行实际的鉴权操作,异步进行鉴权相关数据的保存。这样可

以避免阻塞其他请求,并提高系统的并发性能。

而在系统启动阶段或低峰期,可以提前加载和预热一部分常用的鉴权数据,如用户信息、权限配置等。这样可以减少实际鉴权过程中的查询和计算操作,提高系统的响应速度。预加载和预热可以通过定时任务或者系统启动脚本来完成。

这些优化方案可以根据具体的系统需求和场景进行选择 and 组合使用,以达到提高多级鉴权技术性能的目的。同时,在不同的应用场景下可能还有其他特定的优化方案,需要根据实际情况进行分析和实施。

总体而言,物联网数据接口管理系统的架构应该是灵活、安全和可扩展的,能够管理和控制物联网中的数据接口,并确保数据的安全传输和合理使用。具体的实现方式可以根据具体的应用场景和系统要求进行调整和定制。

5 结束语

本次研究致力于设计和优化物联网平台中的鉴权机制和算法,以确保安全、高效的数据访问和传输。这包括基于密码学的加密算法、数字签名、身份认证协议等。通过研究和创新,可以提出更安全、更快速的鉴权方案,以满足物联网平台数据管理的需求。设计了适应物联网平台的多级鉴权体系架构,包括基础鉴权层、业务鉴权层、数据鉴权层和风险控制层等。通过构建多级鉴权机制,可以实现细粒度

的权限管理和数据安全性保障。研究成果包括多级鉴权框架、协议和接口定义等。

与此同时,在多级鉴权技术研究中,安全和隐私保护也是重要的关注点。本次研究提出了物联网平台中的数据安全问题如身份伪造、数据篡改、信息泄露等问题的解决方案。通过加密算法、访问控制策略和安全协议的研究,可以较好地保护物联网平台中的数据安全和用户隐私。

总之,多级鉴权技术的研究的主要内容包括设计安全高效的鉴权协议和算法、构建多级鉴权体系架构、优化性能和扩展能力、保护安全和隐私等方面。这些研究成果对于确保物联网平台中数据的安全访问和传输具有重要意义,并为实际应用提供了更加充分的理论和实践基础。

参考文献

- [1] 孟鹏,张岩. 基于多级鉴权的物联网身份认证机制[J]. 电子技术与软件工程, 2017,16(10):216-217.
- [2] 李建华,贾春花. 基于多级鉴权的物联网终端访问控制模型[J]. 计算机与数字工程,2018,46(5):965-968.
- [3] 邓小红,王立平,李忠梅. 基于多级鉴权的物联网访问控制技术[J]. 电子与信息学报,2019,41(4):847-852.
- [4] 房玮睿,王春露. 基于缓冲池和多线程的智能交通短信平台设计与实现[C]//中国通信学会第六届学术年会论文集. 广州:中国通信学会,广东省通信管理局,2009:15-19.
- [5] 姜宏岸,王刚. 优先级队列的缓存管理机制的性能分析[J]. 计算机工程与应用,2009,45(25):86-88.