**可信计算在工业物联网安全领域研究与应用**

**1. 引言**

工业物联网（IIoT）是指工业应用的传感器和仪器设备通过互联网相互连接形成复杂的网络结构，该网络采用物联感知和通信技术收集工业数据，并对数据进行分析，工业物联网技术优化了生产过程、提高了生产效率、降低了制造成本、改善了产品质量，其目的是最终实现将传统工业提升到智能化的新阶段。工业物联网技术为生产带来便利的同时，它的开放性、复杂性和异构性也带来了巨大的安全风险，例如数据泄露、设备入侵、恶意攻击等，威胁着工业生产的安全性和稳定性。因此，必需采用有效的物联网设备安全接入方案，才能保证访问控制、入侵防范等安全机制的实施。

可信计算的基本思想是构建一个信任根，将构建的信任根作为起点来构建信任链。从信任根开始逐步到硬件平台、操作系统、应用认证与信任，最终认证与信任将拓展到整个计算机系统。该方法从源头上确保了整个系统的可信度，同时将信任关系通过网络连接延伸到整个信息系统。可信平台控制模块（TPM/TPCM）是可信平台的唯一可信根，包含可信度量根、可信存储根、可信报告根。它是集成在可信计算节点上的防护部件、由软硬件和固件所组成，与计算机的软硬件、固件并行连接在一起，用来建立与保障信任源点。

基于此，文章对可信计算在工业物联网设备安全领域的研究与应用进行讨论。

**2. 工业物联网信息安全问题分析**

工业物联网的安全问题主要来自以下四个层面。

感知层面临的安全风险主要是设备安全问题。大部分工业物联网传感器、仪器设备等感知终端设备安全防护较弱，而且常常部署在无人值守的不安全的物理环境中，容易被攻击者进行篡改，一旦某个传感器或控制器被攻击者控制，可能导致整个生产过程失控，甚至引发安全事故。

网络层面临的风险主要是通信安全问题。物联网通信协议多样，但工业物联网对实时性和多任务很强的需求，无法承载复杂的密码算法和安全协议，数据传输的机密性和完整性很难得到保证。

平台层面临的风险主要是接口安全问题。由于工业物联网系统的设备数量庞大、分布广泛，管理和维护难度也相应增加。如何保证工业物联网设备的正确接入，而且保证每个新接入的设备都是可信的。而且大部分工业物联网系统通信协议都是很多年前设计的基于串行连接进行网络访问，设计时通常把通讯的可用性和实时性放在第一位，对安全性的考虑不足，通讯协议对身份认证、数据加密等方面的考虑也显得不够。

应用层面临的安全风险主要是数据安全和隐私保护。由于工业物联网系统中包含有大量的有价值的数据，这些数据在传输和处理过程中很有可能被窃取或篡改，如何保证这些数据不被窃取、如何在数据被篡改后及时发现并阻止数据进一步传输，成为一个有待解决的问题。

对工业物联网系统的攻击手段，主要分为对工业数据的攻击、对设备互联性的攻击、对设备的真实性的攻击，由于这些攻击手段通常软硬结合，使得肉眼很难发现问题所在。外部对工业物联网的攻击技术与手段也日益先进、复杂、成熟，工业物联网所面临的安全威胁日益严峻。

**3. 可信计算技术在工业物联网领域的应用**

可信计算是解决工业物联网接入安全的有效技术，利用可信网络连接技术可以有效确保所接入网络设备的安全性和真实性，为确保系统初始环境可信,系统加载代码时进行可信验证。采用动态方式来度量系统运行时的内核代码、应用程序代码、关键数据结构等,实现对系统运行代码的实时监控。同时对存在的代码漏洞采取相应的应急措施,大大提高代码的稳定性。对身份认证、平台认证基于可信证明机制,能够实现可信网络的连接,避免恶意的设备接入。

何申等人提到了一种物联网边界安全接入系统，如图3-1所示。

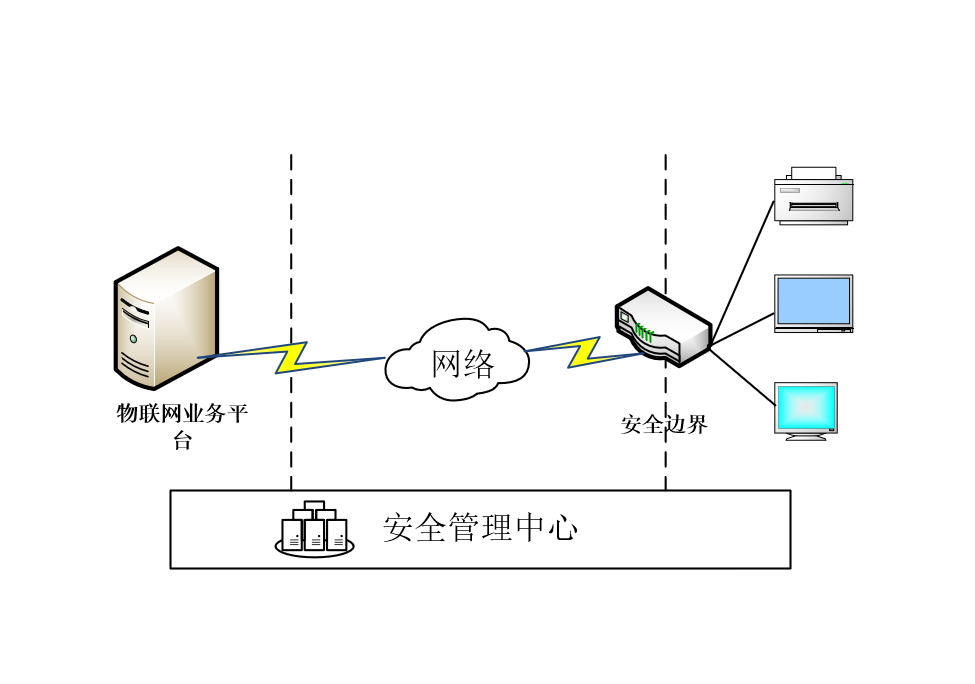


图3-1 物联网边界安全接入系统

在该系统中，安全管理中心是整个系统的大脑，对物联网系统的系统环境、物联网设备以及网络进行统一的安全可信管理。网关设备的可信技术从可信启动、可信静态度量、可信动态度量3方面入手。可信启动依赖于TPM先于CPU启动，获取硬件系统控制权，在完成对系统引导程序、系统内核、内存初始盘的可信度量后，才将控制权放权给系统，保证了系统初态可信性。内核安全机制持续对系统服务、应用程序、内核模块和动态库等进行监控。静态度量机制包括可信白名单模块（包含全系统的可执行程序的特征）和完整性度量模块（计算可执行程序特征的完整性度量值与白名单库对比，从而主动免疫未经授权或不符合预期的执行程序启动），从而实现防止恶意代码和恶意软件运行。动态度量模块实时监控对系统内的所有关键进程、模块、可执行代码等进行实时度量和控制，从而保证系统运行时可信。可信网关和安全管理中心双向身份认证，合法的网关才能接入安全中心获取安全策略。终端接入网关时，只有符合安全策略才能正确接入。网关与终端之间也是双向认证的，防范伪装网关的攻击。在终端进行访问时，可信网关除了对其行为进行管控和检测之外，对其访问行为还要实时审计，对不符合安全策略的行为进行上报安全管理中心，对于恶意的行为经分析后阻止其接入网络。

祁龙云等人提出了一种边缘设备远程证明和监控方案，边缘设备在TPM芯片的支持下，生成身份密钥AIK、TPM自身的EK公钥以及边缘设备的唯一标识符ID，与注册服务器建立验证关系，分发证明密钥以及AIK证书。基于证书AIK，远程证明协议可以验证边缘设备的身份信息以及确保边缘设备注册后到完整性监控协议启动前这段时间的可信性。边缘设备的远程证明和监控方案包括设备的注册协议、远程证明协议和完整性监控协议。该方案通过以上协议，完成了工业物联网新接入设备的注册、远程证明以及后续的完整性监控。

在注册工作开始前，要完成初始化工作，包括：生成TPM芯片制造商的EKpub、生成边缘设备的身份密钥对（AIKpub和AIKpri）以及生成边缘设备唯一标识ID（作用：表明身份“我是谁”，“谁“能证明”我是谁“）。在注册阶段，边缘设备将自身的ID、EKpub、AIKpub发送给注册服务器进行验证，验证有效后注册服务器生成边缘设备共享的证明密钥Katt，Katt加密后注册服务器还生成伪随机数生成器的种子Satt一起发回边缘设备，注册服务器还对边缘设备的AIKpub颁发AIKcert，为之后的远程证明协议的身份认证提供依据，边缘设备收到密文后进行解密获取证明密钥，再发送HMACKall(ID)给注册服务器，表明自己接收到了证明密钥。

验证服务器对新注册的边缘设备发起带有随机数nonce证明请求（随机数nonce确保信息不被重复使用，用以对抗重放攻击）。边缘设备接收到证明请求后,获取自身的软件度量值h,加上证明请求和自身的AIKcert，通过证明密钥Katt 生成证明响应的消息验证码μ，发送给验证服务器，验证服务器收到证明响应后,通过与注册服务器共享的会话密钥Kser建立安全的会话,从而获取对应边缘设备的证明密钥Katt以及证书AIKcert。最后,验证服务器验证证明响应μ的真实性和可信性,以及AIKcert的真实性。验证通过后,验证服务器保存边缘设备的证明密钥Katt,为非交互式的完整性监控协议提供对应的证明密钥,最后,将证明周期的生器种子Satt发送至边缘设备,为完整性监控协议提供随机性证明周期。

在验证边缘设备身份后，与验证服务器同步时钟，随机生成证明周期，到达证明周期时，边缘设备计算自身的软件度量值h，附加上证明周期，经证明密钥Katt加密后发送给验证服务器进行验证，验证服务器对一定时间内接收到的证明凭证认为有效。（验证服务器让边缘设备进行证明，边缘设备收到后生成一个接收时间，该接收时间随着证明信息一起打包，只有在规定时间内完成证明并发送证明凭证，该证明才被认为是有效的，否则，证明无效，认为该边缘设备是不可信的）

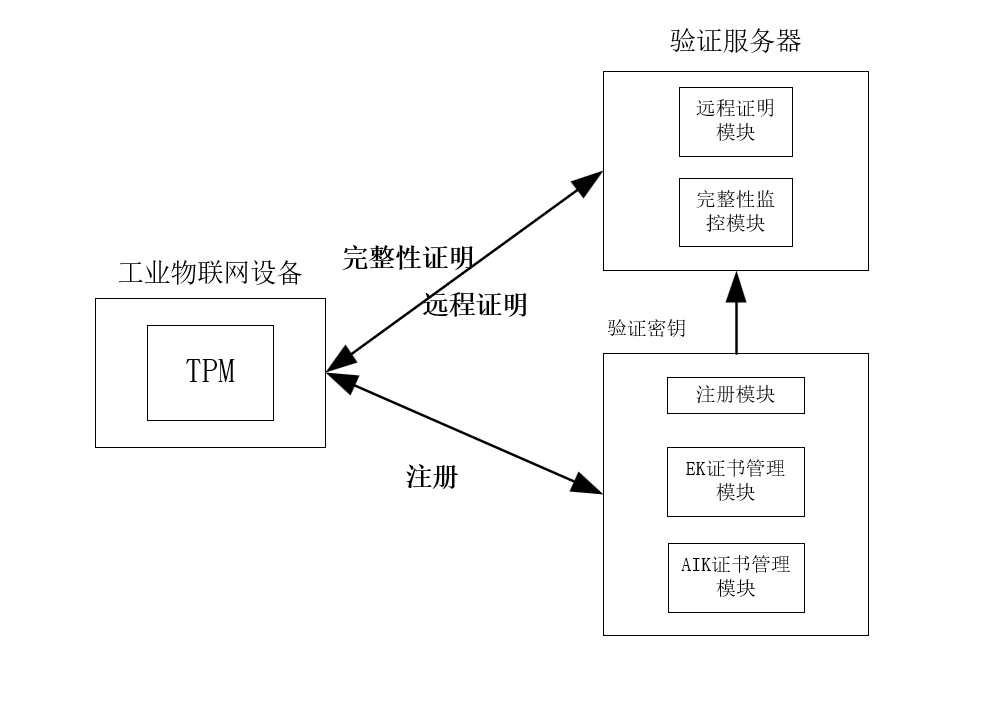


图3-2 系统实现框架图

邵诚等人设计了一种基于可信连接的安全工业控制系统设计框架，用户通过TNC客户端向PEP设备请求接入，并提交客户端的完整性状态和用户授权信息，PEP向TNC转发客户端信息，TNC通过了用户身份和平台完整性验证，以相应的请求角色向客户端授权，通知PEP可以接入。TNC通过IF-MAP协议向MAP服务器发布客户端完整性状态、用户授权信息。TNC服务器验证客户端完整性状态、用户授权信息。内部防火墙检测到终端的访问请求，由防火墙通过IF-MAP协议向MAP服务器进行搜索。通过搜索，发现接入客户端设备当前的用户的授权，来判断设备状态是否可信，如果搜索不到防火墙则拒绝连接处理。防火墙通过添加动态策略允许该客户端请求访问。内部网络行为监控节点和防火墙检测到攻击之后，立即向MAP服务器报告，并通过IF-MAP协议通知PDP有安全事件发生，PDP通过判断立即修改终端的可信状态，通知PEP对连接终端进行隔离处理，删除终端的访问授权，并将新的状态和授权信息发布到MAP服务器。如图3-3所示。

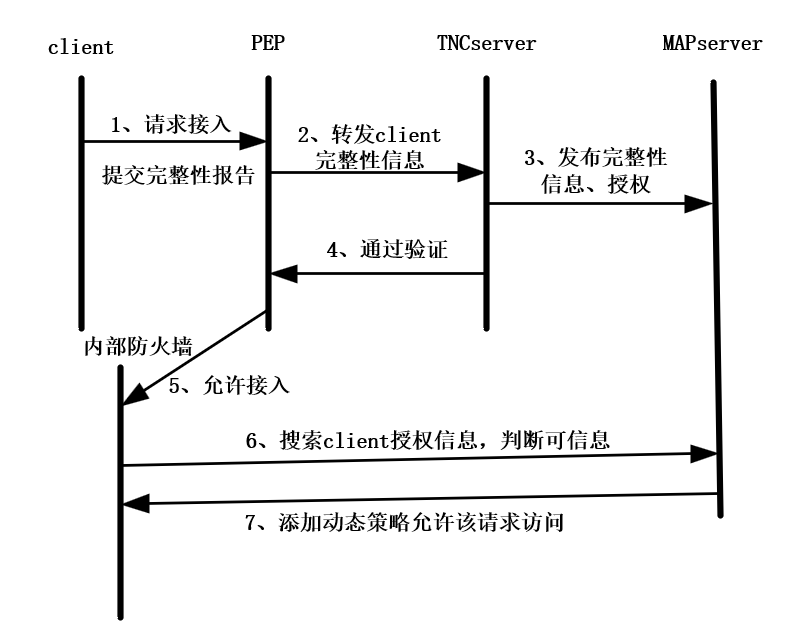


图3-3 远程终端访问机制

**4. 结束语**

可信计算作为构建积极防御网络安全保障体系的核心技术，其理念能覆盖工业互联网多种设备和网络环境，满足工业互联网业务和应用相对稳定的运行特点，在工业互联网安全建设中的应用具有重要的意义。

好的解决方案离不开严格的规范和管理，制定相应的安全标准、指南、管理要求对工业物联网信息安全显得尤为重要，同时，研究具有自主知识产权的控制器、操作系统、软硬件设施才是从国家安全层面上保证工业物联网信息安全的关键。

**参考文献**

[1]刘思尧.可信计算在物联网感知层安全中的应用研究[J].信息与电脑(理论版)，2022,34(19),213-216

[2]杨 宏、王晓春、林冠辰、郭雄.可信物联网技术与标准化研究[J].物联网标准化专题，2023,(05),10-15+20

[3]何申等.基于可信计算构建物联网安全边界[J].电信工程技术与标准化，2019,32(12),7-11,DOI:10.13992/j.cnki.tetas.2019.12.002

[4]楚兵.工业嵌入式控制系统可信计算技术应用研究[J].自动化博览，2023,40(01),27-31

[5]刘思尧、贾博等.基于可信计算的物联网设备安全研究[J].信息与电脑(理论版)，2022,34(17)

[6]邵诚、钟梁高.一种基于可信计算的工业控制系统信息安全解决方案[J].信息与控制，2015,44(05)，DOI:10.13976/j.cnki.xk.2015.0628

[7]祁龙云、刘苇、张晓、赵保华、李科、李向南、林江南. 电力边缘设备远程证明和监控方案[J/OL].计算机应用与软件，http://link.cnki.net/urlid/31.1260.TP.20240607.1628.002