

物联网在提升网络安全技术中应用

范建华

(福州墨尔本理工职业学院 福建福州 350000)

摘要: 随着物联网设备的广泛应用,从智能家居到工业自动化,网络安全成为了一个重要议题。本文主要讨论了物联网在网络安全技术中应用的价值,强调了其在保护敏感数据、提供动态安全管理、增强用户信任以及保护关键基础设施方面的重要性。并详细介绍了有效选择数据加密机制、积极完善入侵检测系统、强化认证和访问控制,以及促进区块链技术的应用等策略。以期提高物联网设备和数据的安全性,为现代社会提供更加稳定和可靠的技术基础。

关键词: 物联网; 提升; 网络安全技术; 应用

引言

随着物联网技术的迅速发展和普及,其在网络安全方面的应用变得越来越重要。物联网设备的广泛部署带来了新的安全挑战,如数据泄露、未授权访问和系统破坏等风险。因此,探索和实施有效的网络安全策略对于确保物联网环境的安全稳定运行十分重要。

一、物联网在提升网络安全技术中应用价值

物联网在提升网络安全技术中的应用具有多重价值,为保护日益扩展的互联设备网络提供了强有力的支撑。随着物联网设备的普及,从智能家居到工业自动化,大量敏感数据和关键操作开始依赖于这些设备。在这种背景下,物联网的安全性不仅关乎个人隐私保护,还涉及到整个社会和经济体的稳定运行。物联网技术在安全领域的应用能够确保数据在传输和存储过程中的安全性,防止数据泄露和未授权访问。同时,物联网的安全技术能够提供更加精细化和动态的安全管理,适应不断变化的网络环境和威胁。例如,通过实时监控和数据分析,可以及时识别和响应安全事件,防止潜在的攻击。物联网的安全技术还有助于增强用户信任,这对于物联网设备的广泛采用非常重要。用户只有在确信其数据和隐私得到妥善保护的情况下,才会更愿意接受和使用这些技术。在保护关键基础设施方面,物联网安全技术同样扮演着重要角色。例如,在电力网、交通控制系统等领域,物联网设备的安全运行对于确保这些基础设施的稳定非常重要。通过加强物联网安全技术,可以防止这些关键系统遭受破坏性攻击,保障社会运行的安全和效率。总体而言,物联网在网络安全技术中的应用提高了数据和设备的安全性,还为现代社会提供了更加稳定和可靠的技术基础,这对于促进科技创新和保障社会运行的安全性具有重要意义。并且随着物联网技术的不断进步和普及,其在网络安全领域的作用愈

发凸显,成为维护数字世界安全的关键力量。

二、物联网在提升网络安全技术中应用策略

(一) 有效选择数据加密机制

在提升网络安全技术的过程中,尤其在物联网的应用领域,选择合适的加密机制显得尤为关键。物联网设备通常涉及大量敏感数据的传输,这些数据包括个人信息、位置数据、环境监测数据等,因此确保这些信息的安全是至关重要的。有效的数据加密机制可以在数据传输过程中保护数据免受未经授权的访问和篡改。例如,对于智能家居系统,可以使用高级加密标准(AES)为家庭内部的通信网络提供坚固的加密保护。AES是一种广泛使用的加密技术,能够确保数据在从智能家居设备传输到控制中心的过程中保持加密和安全。此外,对于一些需要低功耗的物联网设备,如传感器网络,可以采用轻量级加密算法,这些算法能够在保证数据安全的同时,减少对设备处理能力和电池寿命的影响。除了选择恰当的加密算法外,还需要考虑到密钥管理机制。在物联网环境中,密钥管理尤为复杂,因为涉及到大量设备和用户,需要定期更新密钥、确保密钥的安全存储和传输,以及在设备生命周期结束时安全地废弃密钥。因此,在物联网环境中提升网络安全技术时,选择和实施合适的数据加密机制是基础且关键的步骤。其中不仅要涉及到选择适合的加密算法,还要包括密钥的安全管理和适应物联网特有的挑战,如设备的多样性、处理能力的限制和能耗问题。进而通过这些综合措施,大大提升物联网环境中的数据安全性,保护个人和组织免受网络威胁的侵害。

(二) 积极完善入侵检测系统

在物联网环境提升网络安全技术的过程中,需要积极完善入侵检测系统(IDS)。随着物联网设备数量的激增和应用范围的扩展,这些设备成为网络攻击的潜在目标。因此,有效的入

入侵检测系统对于预防和识别潜在的网络威胁十分重要。入侵检测系统在物联网环境中的作用可以通过几个方面来体现。首先,监测网络流量,识别异常模式或行为,从而及时发现和响应潜在的入侵活动。例如,在智能城市的物联网应用中,可以利用一个有效的IDS监测和分析城市交通管理系统、公共安全监控等多个系统的数据流,以便于及时检测和阻止任何异常或恶意的网络活动。其次,入侵检测系统需要能够适应物联网的特殊性,如设备多样性和网络结构的复杂性。这需要IDS不仅要能够处理传统网络攻击,如DDoS(分布式拒绝服务攻击)和恶意软件,还要能够识别针对物联网特有协议和设备的攻击。例如,IDS需要针对智能家居系统的攻击会尝试利用无线通信协议的漏洞,识别这类特殊的攻击模式。最后,随着人工智能和机器学习技术的发展,将这些技术应用于入侵检测系统能显著提高其效率和准确性。AI驱动的IDS通过学习正常的网络流量模式,能够更精确地识别异常行为,减少误报率。同时,还能够适应新型攻击策略,持续改进检测能力。

(三) 强化认证和访问的控制

随着物联网设备数量的增加,确保只有授权的用户和设备能够访问网络资源变得尤为重要。这关系到个人隐私的保护,也关系到整个网络系统的安全性。强化认证和访问控制主要涉及到两个方面:一是确保用户身份的准确验证,二是控制用户对网络资源的访问权限。在物联网环境中,需要实施更加复杂和安全的认证机制。例如,在智能家居系统中,除了传统的密码认证外,还可以实施生物识别技术,如指纹或面部识别,以提高认证的安全性。另外,物联网设备本身也需要进行严格的认证,以确保它们是网络中可信的实体。例如,智能工厂中的传感器和控制器需要通过安全协议来验证它们的身份,从而确保数据的安全传输。在访问控制方面,需要细致地定义和管理用户和设备对网络资源的访问权限。这需要不同的用户和设备根据其角色和需求被授予不同级别的访问权限。例如,在医疗健康监控系统中,患者的个人健康数据应该严格控制访问权限,只有授权的医护人员和患者本人能够访问。对于企业级的物联网应用,如工业控制系统,访问控制策略应该能够管理员工对关键系统的访问,防止未经授权的操作导致的安全风险。从而通过这些措施共同作用,大大降低物联网设备被未经授权访问或恶意操作的风险,保护整个网络系统的安全与稳定。并通过实施严格的认证和访问控制,使物联网的应用更加安全,更好地服务于人们的生活和工作。

(四) 促进区块链技术的应用

为了提升网络安全技术,需要促进区块链技术的应用。区块链技术以其去中心化、不可篡改和透明性的特点,为物联网环境中的数据安全和设备管理提供了新的解决方案。通过区块链技术,可以在物联网设备之间建立一个安全、可信的通信网络,有效防止数据被未经授权的修改和访问。例如,在供应链管理中,区块链可以用来跟踪商品从生产到消费的整个过程。物联网设备如传感器可以实时收集商品的状态信息,如温度、位置和运输环境,并将这些数据记录在区块链上。由于区块链的数据不可篡改性,所以确保了数据的真实性和完整性,使得供应链过程更加透明和安全。同样,在智能家居系统中,区块链技术也可以用来确保设备间的安全通信。在这样的系统中,每个设备的身份和交易(如数据传输和控制命令)都可以通过区块链来验证和记录。这提高了系统的安全性,还增加了用户对智能家居设备使用数据的信任度。

结语

总而言之,物联网在提升网络安全技术中的应用展现了其在现代社会中的重要作用。通过实施先进的数据加密、入侵检测、认证控制以及区块链技术,能够使物联网更好保护自身系统的安全,还能为用户提供更加安全、可信的服务。并且能够加强物联网的安全基础,也能够推动整个网络安全技术的发展,为物联网技术的未来应用奠定坚实的基础。

参考文献

- [1]苏虞磊,薛方,曲蕴慧. 计算机网络安全技术在网络安全维护中实际应用探讨 [J]. 公关世界, 2023, (19): 93-95.
- [2]解晓盈. 基于物联网技术的数字化校园网络安全防御系统设计 [J]. 自动化与仪器仪表, 2023, (09): 151-155.
- [3]金超. 物联网环境中计算机网络安全技术影响因素及防范研究 [J]. 中国新通信, 2023, 25 (18): 125-128.
- [4]张咏梅,王萍,卞薇薇等. 基于 5G 物联网技术构建患者安全智能预警系统在整复外科护理工作中的应用 [J]. 组织工程与重建外科, 2023, 19 (04): 402-407.
- [5]李毅超,高毅,刘辛彤等. 基于域信任管理的配电物联网通信与网络安全防护技术架构研究 [J]. 电气时代, 2023, (06): 48-51.

范建华,男,汉族,1989-03,福建闽清人,州墨尔本理工大学职业学院,助理工程师,现代教育技术中心科员,本科学历,学士学位,研究方向:计算机网络技术。