物联网环境下的网络安全挑战与对策

邱文强
西藏熙安信息技术有限责任公司　西藏自治区拉萨　850000

【摘　要】广泛的物联网设备应用带来了设备种类繁多、数据大规模流动、对持续连接的依赖以及系统高度整合等多重网络安全考验。本文深入剖析了物联网环境下的网络安全特性，并详细探讨了隐私泄露的潜在风险、系统安全漏洞、身份管理的复杂性，以及持续连接可能增加的攻击风险这四大核心挑战。并提出了相关应对措施，旨在针对物联网环境下的网络安全，提供一套全面、富有前瞻性且切实可行的解决方案，以确保物联网系统的安全与稳定运行。

【关键词】物联网；网络安全；隐私泄露；系统漏洞；身份管理

Network security challenges and countermeasures in the Internet of Things environment

Qiu Wenqiang
Xizang Xinan Information Technology Co.，LTD Lhasa City，Tibet Autonomous Region　850000

【Abstract】The wide range of Internet of Things device applications have brought multiple network security tests，such as a wide variety of devices，large-scale flow of data，dependence on continuous connection and high integration of the system. This paper deeply analyzes the characteristics of network security in the Internet of Things environment，and discusses in detail the potential risks of privacy leakage，system security vulnerabilities，the complexity of identity management，and the attack risk that may increase by continuous connection. And put forward the relevant countermeasures，aiming to provide a comprehensive，forward-looking and feasible solution for the network security in the Internet of Things environment，to ensure the security and stable operation of the Internet of Things system.

【Key words】Internet of Things；network security；privacy leakage；system vulnerability；identity management

引言

作为新一轮科技革命的关键一环，物联网（IoT）技术正深刻重塑着人类生活和生产方式。从智能家居、可穿戴科技，到工业控制系统乃至智能城市的基础设施，物联网设备已遍布每个角落，构建出一个宏大的网络生态。然而，物联网设备的迅速增长与应用领域的拓宽，也带来了日益严重的网络安全隐患。设备种类繁多、数据流动广泛、对持续连接的依赖，以及系统的高度整合，都使得物联网环境下的网络安全难题不断涌现。

一、物联网环境下的网络安全特点

（一）设备多样性与复杂性

在现今技术环境下，智能家居、可穿戴设备、工业控制系统以及智能城市基础设施的广泛应用，导致了网络架构的极端复杂性。这些由不同制造商生产的设备，在硬件、软件和通信协议方面差异显著，缺乏统一规范，从而加剧了兼容性和管理上的困扰。设备多样化所带来的挑战，关乎设备自身的管控，更延伸至设备间的互操作与互联互通。例如，某些低成本的物联网设备因计算资源有限，难以运行复杂的加密算法，使得它们在网络攻击面前显得异常脆弱。此外，设备的多样性也让网络管理员难以实施统一的监控与管理，进一步提升了维护和安全防护的难度。

（二）数据流动广泛性与敏感性

物联网设备遍布全球，涉及众多行业领域，数据交换范围极其广泛。以智能医疗设备为例，它们能够实时监控患者的生理数据，并迅速将这些信息传输至远程医疗中心以供深入分析和处理[1]。然而，这种跨越地域与行业的数据传输，亦伴随着多种风险，诸如数据泄露、非法访问以及数据篡改等安全隐患层出不穷。鉴于传输数据中包含着诸如健康档案、地理位置和金融资讯等大量个人隐私与敏感信息，其一旦外泄，将对个人隐私和安全构成严峻威胁。

（三）持续连接与实时性需求

现代物联网设备为保持数据的实时处理和传输，常需维持持续连接状态。这一特性确实提升了数据的实时性与系统的响应速度，但同时也显著加剧了设备遭受网络攻击的风险。黑客可借由持续在线的设备发起攻击，窃取机密信息或破坏系统功能。以智能交通系统为例，它需要不间断地监控交通流量并进行管理，网络攻击很可能引发交通紊乱，甚至对公共安全构成威胁。同时，为了满足物联网设备对实时性的高要求，网络系统应具备迅速响应的能力，还需高效处理数据流。

（四）系统整合与协同防御需求

在当下物联网技术环境中，多层次、多组件融合的系统里，各环节间的整合与协同工作至关重要。但此整合过程中

易产生安全漏洞，从而成为攻击焦点。以智能家居系统为例，它融合了众多传感器、控制器及网络设备，任何一个环节的漏洞都可能使整个系统陷入被攻击的风险。因此，需构建一个全方位的协同防御机制，以实现各层次间的信息共享与联合防护。在这一体系中，边缘计算设备负责在数据接入初期进行基础的安全筛选，而云端系统则肩负更复杂的安全分析及策略制定任务。同时，提升不同设备和系统间的互操作性与兼容性，也是协同防御中待解决的问题。

二、物联网环境下的网络安全挑战

（一）隐私泄露风险

在物联网环境中，隐私泄露风险显得尤为严峻。物联网设备在日常运作中会大量收集个人信息，涵盖地理位置、健康数据及行为习惯等诸多方面。由于这些数据需频繁传输至云端进行处理与存储，在任一传输环节中，安全漏洞均可能成为不法分子的攻击点，进而引发隐私泄露[2]。例如，黑客可能截获未加密数据，窃取用户的敏感信息。另外，部分物联网设备在设计与制造时安全性考虑不足，存在潜在漏洞，为黑客提供了入侵的机会。一旦遭受攻击，黑客便可盗取隐私数据，甚至利用这些数据进行身份盗用、金融欺诈等非法行为。隐私泄露对个人及社会均造成深远影响，如泄露的健康数据可能助长医疗欺诈，地理位置的泄露更可能危及用户安全。

（二）系统安全漏洞

物联网设备种类繁杂，且由多家制造商出品，其硬件、软件和通信标准各异，这种多样性与复杂性直接加剧了系统安全漏洞的风险。层出不穷的漏洞为黑客提供了可乘之机，使其能够发动各类网络攻击。例如，黑客可利用设备固件漏洞，植入恶意代码以操控设备，扰乱系统正常运行。部分物联网设备更新及维护机制不足，难以及时应对新型攻击，修复漏洞，使设备长期暴露于风险中。此外，物联网设备间的互联互通使得单一设备的安全漏洞可能危及整个网络。如黑客可通过攻击一个不安全的智能家居设备，进而控制整个家庭网络及其连接设备。这些系统安全漏洞不仅危及设备自身，更可能导致关键数据泄露或被损坏，对用户的生活与工作造成深远影响。

（三）身份管理难题

身份管理的不完善可能引发未授权访问，进而危及整个物联网系统的安全。例如，若设备身份认证机制存在缺陷，黑客便能轻易伪造或窃取合法设备身份，进而渗透系统并发动攻击。同时，物联网设备的动态特性和移动性也为身份管理带来了额外难度。设备在不同网络环境间的频繁切换，使得在高效管理的同时确保安全变得极具挑战性。此外，用户身份管理亦不容忽视，因物联网设备常涉及大量用户数据的收集与处理。若无法妥善管理和保护用户身份信息，便可能引发数据泄露与隐私侵犯风险。值得一提的是，身份管理问题不仅包含技术层面的挑战，还牵涉到政策法规的复杂性，进一步加剧了物联网身份管理的难度。

（四）持续连接与攻击风险

物联网设备因需持续连接以支持实时数据处理与传输，而设备长期在线使其始终暴露在网络攻击的风险之下，随时可能成为被攻击目标。黑客可利用此特点发动持续性攻击，如分布式拒绝服务（DDoS）攻击，通过海量请求耗尽设备资源，致其瘫痪。同时，持续联网也为攻击者提供了更多时间与机会来探测并利用设备漏洞，进行长期渗透与数据窃取[3]。另外，物联网设备需快速响应并处理数据以满足实时性要求，这对系统稳定性与安全性提出了更高要求。但过分追求实时性可能削弱安全措施，增加设备脆弱性。在持续的数据收发过程中，任何安全漏洞都可能被攻击者利用，造成严重后果。持续连接与实时性需求的双重压力使物联网设备面临的安全风险更加复杂难测，成为物联网网络安全的一大挑战。

三、物联网环境下的网络安全对策

（一）数据加密与认证

在物联网环境中，加密算法能有效防范数据窃取与篡改，保障数据的机密性和完整性。其中，对称加密算法如 AES，以高效著称，适用于大规模数据加密；而非对称加密算法如 RSA，虽速度稍慢，却在身份认证和密钥交换中表现出色。结合运用这两种算法，能够在维持高效加密的同时，大幅提升安全性。身份验证同样是物联网安全不可或缺的一环，它通过核实通信实体的身份，有效防止未授权访问。目前，主流的身份验证方式包括密码验证、双因素认证及生物特征认证。特别是双因素认证，它通过结合密码与物理设备，显著增强了安全性。而生物特征认证，如指纹识别和面部识别，则因其独特性和防伪性备受青睐。为进一步提升系统安全性，公钥基础设施（PKI）的身份认证管理发挥着关键作用。PKI 利用数字证书和公钥加密，为物联网提供稳健可靠的身份认证。这些数字证书由权威认证机构颁发，确保了身份的真实性。在通信中，物联网设备可利用数字证书实现双向身份验证，有效抵御中间人攻击和身份伪造。此外，分布式身份（DID）技术在物联网安全领域也展现出巨大潜力。DID 通过区块链实现去中心化身份管理，增强了身份数据存储和管理的安全性与透明度。每个设备或用户都拥有唯一的 DID，通过区块链进行身份验证，为物联网环境的安全性提供了坚实保障。

（二）固件更新与漏洞管理

物联网设备在使用过程中可能会暴露多种安全漏洞，一旦被黑客利用，后果不堪设想。因此，迅速应对和修复这些已知漏洞、持续更新设备固件，成为预防安全风险的重中之重。固件更新是消除已知漏洞的关键途径。制造商应定期推出固件更新，以强化设备的安全性能。用户也需及时安装这

些更新，确保设备免受攻击。但考虑到物联网设备的多样性，更新过程可能面临挑战。例如，部分设备缺乏自动更新功能，需要用户手动操作，这无疑增加了用户的负担[4]。同时，网络不稳定等因素也可能导致更新失败，延误安全补丁的应用。因此，制造商在设计设备时，必须着重考虑固件更新的便捷与可靠，以便用户能轻松、安全地完成更新。另一方面，完善的漏洞管理流程也是保障设备安全的关键环节。制造商应建立涵盖漏洞发现、修复和通报等全面的管理机制。利用自动化扫描与人工检测相结合的方式，定期对设备进行漏洞排查。一旦发现漏洞，应立即采取修复措施，并通过固件更新将安全补丁推送给用户。对于严重漏洞，还需及时向用户发出警告，并提供紧急应对方案，防止黑客利用。此外，与第三方安全机构的紧密合作也不可或缺。这些机构的专业经验和先进工具，可以提升制造商在漏洞检测和修复方面的能力。

（三）网络监控与行为分析

网络监控通过实时监测网络流量及设备行为，能迅速发现异常，从而遏制潜在威胁的扩散。行为分析则通过学习设备和用户的常规行为模式，精准识别异常举止，实现对攻击的迅速应对。网络监控工具为管理者提供了网络运行状态的实时视图，助力检测异常流量及未授权访问。例如，入侵检测与防御系统能深入剖析网络流量，及时识别和阻断恶意活动，从而在攻击初期就构筑起有效的防御，降低损害。同时，网络监控还能揭露网络漏洞和弱点，为安全策略的调整提供有力依据。行为分析在网络安全中也占据着举足轻重的地位。它通过学习建立正常行为的基准模型，一旦监测到偏离此基准的行为，即刻发出警报。比如，若智能家居设备异常地向未知外部服务器大量发送数据，可能意味着设备已遭黑客操控，而行为分析能敏锐捕捉并阻断此类攻击。此外，它还能用于发现内部威胁，如员工未经授权的数据访问或敏感信息泄露，行为分析系统能即刻识别并作出反应。网络监控与行为分析的结合，构成了一个完备的安全防护体系。前者提供实时的流量与事件监测，后者则进行深入的行为模式剖析，二者相得益彰，共同增强物联网系统的安全性。管理者应定期审视这些监控与分析成果，并根据最新的威胁情报调整防御策略，确保系统始终得到最佳保护。同时，随着人工智能与机器学习技术的进步，更加智能化的监控与分析工具正逐渐融入物联网安全领域，它们能更精确地识别复杂攻击模式，并提供自动化响应，从而进一步提升安全防护的效能。

（四）标准化与多方合作

物联网安全标准化意味着建立统一的安全准则与要求，以确保不同设备与系统间的相容性与互操作性。借由设定及推广通用的安全标准，我们可减少设备间的兼容问题，进而增强整体安全。例如，国际标准化组织（ISO）和国际电信联盟（ITU）等机构已颁布一系列物联网安全标准，覆盖设备认证、数据加密、漏洞管控等层面。这些标准为制造商提供了清晰的安全指引，便于在产品设计中融入安全要素。多方合作对于提升物联网安全同样至关重要。政府、企业、学术界及民间组织各有独特资源与优势，唯有通过协同合作，方能更有效地应对物联网安全挑战[5]。政府可制定政策法规，推动安全标准的落实，并鼓励企业与研究机构投身安全技术的研发应用。企业则可通过技术创新与市场驱动，提升产品安全性能，满足用户需求。学术界可深入研究与实验，探索物联网安全的新理念与新方法，为实际应用提供科学支撑。而民间组织如行业协会和安全联盟，可通过组织培训、交流与协作，提升整个行业的安全认知与防护能力。合作形式可多样化，如公私合作模式（PPP）在物联网安全领域正日益受到重视。通过 PPP，政府与企业可共同投资运营物联网安全项目，共担风险与收益，从而提升项目的成功率与可持续性。此外，鉴于物联网设备与数据传输的全球化特点，单一国家的努力往往难以应对跨国安全威胁。国际合作能实现信息共享与资源互补，共同抵御全球范围内的物联网安全风险。

结语

物联网技术的广泛运用便利了人类生活，推动了创新，同时也带来了错综复杂的网络安全难题。为应对这些挑战，本文提出数据加密与身份认证机制、固件定期更新与漏洞及时管理、全面的网络监控与深入的行为分析、推动标准化进程并强化多方协同合作等措施，为物联网环境下的网络安全构筑了坚实的屏障。未来，必须不断完善物联网安全规范，深化各方之间的协作，携手提升物联网系统的整体安全防护能力。

参考文献

[1]孙英梅.物联网技术下的计算机网络安全问题探讨[J].网络安全技术与应用，2024，（06）：144-146.
[2]王承悦.网络安全与隐私保护技术在物联网环境中的应用研究[J].信息与电脑（理论版），2024，36（08）：210-212.
[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]宋博.基于物联网技术的网络安全问题及应对策略研究[J].网络安全技术与应用，2023，（09）：160-161.
[5]赵哲锋，梁雄伟，王涵群，等.基于云计算和物联网技术的网络安全架构[J].中国宽带，2023，19（08）：28-30.
作者简介：邱文强，男，汉族，1997 年 12 月，四川泸州人，专科学历，西藏熙安信息技术有限责任公司等保测评师，研究方向为网络安全。