物联网背景下计算机网络安全技术分析

林余义
平阳县职业中等专业学校　浙江　温州　325400

摘　要：文章在物联网快速发展的背景下，深入探讨计算机网络安全技术的现状与发展趋势。通过分析物联网环境下网络架构的复杂性及潜在的安全威胁，重点研究了数据加密、身份认证、访问控制、入侵检测与防御等关键技术。同时还强调终端设备安全、隐私保护及综合监测在物联网安全体系中的重要性。通过综合应用这些安全技术，本文旨在为物联网的健康发展提供坚实的安全保障，促进其在智慧城市、智能制造、智能家居等领域的广泛应用。

关键词：物联网；计算机；网络安全

1 物联网技术概念

物联网是以互联网为载体，实现物品之间交流沟通技术的总称。随着现代科技进步，互联网已经成为了人们生产和生活的重要技术。通过对互联网技术的延伸和创新，物联网能够达到技术水平上的更高级别，物联网的持续创新也给各行各业的发展创造了更大的前景。例如，在现代社会的汽车保有量快速增加的今天，城市在停车方面越来越困难，利用物联网技术可以对区域内的车库进行全面监测，达到智能停车目的，也使城市在智慧泊车系统的构建方面拥有更大的可能性。使用物联网技术，可以将不同的物体连接在一起，实现系统之间的信息交流，也可以使数据的通信更加方便快捷，形成一个集认证、采集、分析、定位以及管理为一体的多功能性系统。利用物联网体系，可以使信息传递和处理更加方便快捷。

2 分析计算机网络安全现状

2.1 计算机网络数据安全问题

随着信息技术的飞速发展，计算机网络已成为现代社会不可或缺的基础设施，极大地促进了信息的交流与共享，与此同时，计算机网络安全问题也日益凸显，成为制约网络健康发展的关键因素。当前，计算机网络安全面临诸多挑战，主要包括几个方面；（1）威胁多样化：随着技术的发展，网络攻击手段和威胁方式不断演变，恶意软件、钓鱼攻击、勒索软件等层出不穷，给网络安全带来了巨大挑战。（2）防御手段有限：传统的防御手段如防火墙、入侵检测系统等在面对复杂多变的网络攻击时显得力不从心，难以有效应对新型威胁[1]。（3）数据安全意识提升：随着数据价值的提升，企业和个人对数据安全的重视程度逐渐提高，但安全意识与防护能力之间仍存在较大差距。计算机网络数据安全问题主要体现在几个方面：黑客通过技术手段非法侵入系统，窃取敏感数据，如用户信息、企业机密等，导致数据泄露，给企业和个人带来巨大损失。攻击者可能通过注入恶意代码、发起DDoS攻击等方式，篡改或破坏网络中的数据，影响数据的完整性和可用性。勒索软件已成为一种常见的网络攻击手段，攻击者通过加密用户数据并要求支付赎金来解锁数据，严重威胁用户的数据安全。随着物联网设备的普及，其安全性问题也日益突出。物联网设备往往存在安全漏洞，容易被攻击者利用，进而威胁整个网络的数据安全。在全球化背景下，数据跨境流动成为常态，但不同国家和地区的数据保护法规存在差异，导致数据跨境流动面临合规性挑战。

2.2 计算机网络通信安全问题

在当今数字化时代，计算机网络不仅是信息传递的基石，也是支撑各行各业运行的重要基础设施，随着网络技术的飞速发展，计算机网络安全问题日益复杂，尤其是网络通信安全，成为了亟待解决的关键议题。当前，计算机网络安全面临着一系列严峻挑战。首先，网络攻击手段不断更新换代，从传统的病毒、木马等恶意软件，发展到更为复杂的钓鱼攻击、勒索软件、高级持续性威胁（APT）等，这些攻击方式隐蔽性强、破坏力大，给网络安全防护带来了巨大压力。随着物联网、云计算、大数据等新兴技术的广泛应用，网络边界日益模糊，安全威胁也呈现出多样化的趋势。物联网设备的海量接入增加了网络攻击面，云计算的资源共享特性则使得数据泄露风险加大，大数据的集中存储和处理则成为黑客攻击的重点目标。网络安全意识的不足也是当前网络安全现状中的一个突出问题。许多用户和管理员对网络安全的重视程度不够，缺乏必要的安全知识和技能，容易成为网络攻击的突破口。网络通信作为计算机网络的核心功能之一，其安全性直接关系到信息的传输质量和系统的稳定运行。当前，计算机网络通信安全面临的

主要问题包括：在通信过程中，敏感信息如用户密码、交易数据等可能被非法截获或窃取，导致个人隐私泄露或经济损失。攻击者可能通过篡改通信数据来破坏信息的完整性和真实性，影响数据的正确解读和使用。通过发起拒绝服务（DoS）或分布式拒绝服务（DDoS）攻击，攻击者可以使得目标网络服务无法正常访问，造成业务中断或瘫痪。攻击者可能伪装成通信双方之间的中继站，窃取或篡改传输的信息，严重威胁通信安全。网络通信协议中可能存在安全漏洞，攻击者可以利用这些漏洞发起攻击，绕过安全防护措施。

2.3 终端节点安全问题

在计算机网络体系中，终端节点作为用户直接交互的设备，如个人电脑、智能手机、物联网设备等，扮演着至关重要的角色。然而，随着网络应用的广泛普及和技术的快速发展，终端节点安全问题日益凸显，成为网络安全领域的一个重要关注点。终端节点安全问题主要涉及几个方面；（1）恶意软件感染：终端节点容易受到病毒、木马、勒索软件等恶意软件的攻击。这些恶意软件可能通过网络下载、电子邮件附件、恶意网站链接等途径传播，一旦感染，将严重威胁终端节点的安全，导致数据泄露、系统崩溃等后果。（2）漏洞利用：终端节点上运行的操作系统、应用程序等往往存在安全漏洞，攻击者可以利用这些漏洞进行渗透攻击，获取系统控制权，进而执行恶意操作，如窃取敏感信息、破坏数据等[2]。（3）弱密码与认证问题：许多用户在使用终端节点时，习惯使用简单密码或默认密码，且缺乏多因素认证等安全措施，这使得攻击者容易通过暴力破解或社会工程学手段获取用户凭证，进而入侵终端节点。（4）物理安全威胁：对于某些可移动的终端节点（如笔记本电脑、平板电脑等），物理安全威胁也是一个不容忽视的问题。设备丢失、被盗或被非法访问都可能导致数据泄露或系统被篡改。（5）隐私泄露：随着大数据和人工智能技术的发展，终端节点上的用户行为数据被大量收集和分析。如果这些数据没有得到妥善保护，就可能被不法分子利用，导致用户隐私泄露。

3 制定基于物联网的计算机网络安全防护措施

3.1 强化用户个人网络安全意识

在物联网（IoT）日益融入我们日常生活的今天，强化用户个人网络安全意识成为了构建基于物联网的计算机网络安全防护措施的首要任务。物联网设备，如智能家居系统、可穿戴设备、智能家电等，虽然为用户带来了前所未有的便捷与智能化体验，但同时也成为了黑客攻击的新入口，提升用户的网络安全素养，使其具备识别和防范网络威胁的能力，是保障物联网环境安全的关键。首先，应加大对公众的网络安全教育力度，通过媒体宣传、社区讲座、在线课程等多种形式，普及物联网安全知识，包括但不限于密码安全、隐私保护、恶意软件识别等方面。教育内容应贴近日常生活，用通俗易懂的语言解释复杂的安全概念，使普通用户也能轻松掌握。其次，鼓励用户形成良好的网络安全习惯。比如，定期更换密码，避免使用简单或容易猜测的密码；不随意点击来源不明的链接或下载未知来源的应用程序；对于重要的物联网设备，应设置复杂的访问权限，避免他人轻易接入。用户还应学会识别并防范钓鱼攻击、社会工程学等常见网络威胁手段。为了激发用户参与网络安全防护的积极性，可以建立反馈与激励机制。例如，设立网络安全奖励计划，对及时发现并报告安全漏洞的用户给予奖励；同时，建立用户安全行为评分系统，根据用户的安全操作习惯给予相应的评价，鼓励用户不断提升自身的网络安全意识。

3.2 构建物联网隐私保障体系

物联网环境下，数据的海量生成与共享使得隐私保护成为了一个亟待解决的问题。构建物联网隐私保障体系，旨在确保用户数据在采集、处理、存储、传输等各个环节中的安全性与隐私性。应坚持数据最小化原则，即仅在必要的情况下收集用户数据，并尽可能减少数据的收集范围和存储时间。物联网设备在设计和使用过程中，应明确界定数据收集的目的和范围，避免过度收集用户隐私信息。对敏感数据进行加密处理，确保数据在传输过程中的机密性，对于需要共享的数据，应进行匿名化处理，以去除个人身份信息，降低数据泄露的风险，还应建立严格的数据访问控制机制，确保只有经过授权的用户才能访问相关数据。物联网企业应制定明确的隐私政策，明确告知用户数据的收集、使用、共享和存储方式，以及用户享有的权利和责任。企业应积极遵守相关法律法规，确保数据处理的合法合规性。对于跨国企业而言，还需关注不同国家和地区的数据保护法规差异，确保全球范围内的隐私保护标准一致[3]。

3.3 构建安全可靠的加密体制

加密技术是保障物联网通信安全的重要手段。构建安全可靠的加密体制，可以有效防止数据在传输过程中被窃取或篡改，确保通信的机密性、完整性和可用性。应根据应用场景和安全需求选择合适的加密算法，对于敏感数据的传输，应采用高强度的加密算法，如AES（高级加密标准）等，还应关注加密算法的兼容性和性能表现，确保在保障安全性的同时不影响系统的正常运行。

密钥管理是加密体制中的关键环节，应建立完善的密钥管理系统，确保密钥的生成、存储、分发和销毁等各个环节的安全性。对于物联网设备而言，由于设备数量庞大且分布广泛，密钥的分发和管理尤为复杂，可以采用基于公钥基础设施（PKI）的密钥分发机制，实现密钥的安全分发和更新。还应遵循国际通用的加密协议和标准，如TLS（传输层安全协议）、DTLS（数据报传输层安全协议）等。这些协议和标准经过长时间的实践检验，具有较高的安全性和可靠性。通过遵循这些协议和标准，可以确保物联网设备之间的通信过程更加安全可信。强化用户个人网络安全意识、构建物联网隐私保障体系以及构建安全可靠的加密体制是制定基于物联网的计算机网络安全防护措施的重要方面。

3.4 强化终端设备的综合监测

随着物联网技术的不断发展，终端设备作为数据收集与交互的关键节点，其安全性直接关系到整个物联网系统的稳定运行。强化终端设备的综合监测是制定基于物联网的计算机网络安全防护措施的重要一环。这包括但不限于对设备的运行状态、网络连接、安全漏洞等进行全面、持续的监测。通过部署专业的监测工具和系统，可以及时发现并响应设备异常，防止潜在的安全威胁扩散。在综合监测过程中，应重点关注几个方面：一是设备的物理安全，防止设备被盗、损坏或非法篡改；二是设备的网络安全，确保设备在接入网络时不会成为攻击入口或传播恶意代码；三是设备的数据安全，保护设备生成和存储的数据不被非法获取或滥用。为了实现这些目标，可以引入智能监测技术，如机器学习、大数据分析等，对终端设备进行智能化的风险评估和预警。

3.5 采取多种措施实时监控终端设备

实时监控终端设备是保障物联网系统安全的重要手段之一。通过采取多种措施对终端设备进行实时监控，可以及时发现并应对潜在的安全威胁，确保系统的稳定运行。具体措施包括但不限于几个方面：（1）网络流量监控：利用网络流量分析工具对终端设备的网络流量进行实时监控，识别并阻止异常流量和潜在的网络攻击。（2）日志审计与分析：对终端设备的操作日志进行收集、存储和分析，通过日志审计发现潜在的安全问题，并追溯攻击源头[4]。（3）入侵检测与防御系统（IDS/IPS）：部署入侵检测与防御系统，对终端设备上的恶意行为进行检测和防御，及时阻断攻击行为。（4）远程管理与控制：建立远程管理和控制机制，允许管理员远程监控和管理终端设备，包括查看设备状态、更新固件、配置安全策略等。（5）安全事件响应机制：建立完善的安全事件响应机制，一旦发现安全事件立即启动应急预案，组织专业团队进行处置和恢复工作。通过采取这些多种措施对终端设备进行实时监控，可以显著提高物联网系统的安全性，降低安全风险，保障用户数据的安全与隐私，这也要求物联网企业和用户具备高度的安全意识和专业的技术能力，共同构建安全可信的物联网生态环境。

结束语

物联网背景下计算机网络安全技术的研究与应用对于保障物联网系统的安全稳定运行具有重要意义。随着技术的不断进步和应用场景的日益丰富，物联网安全面临的挑战也将更加复杂多变。需要持续关注安全技术的发展动态，加强技术创新与合作，构建更加完善的安全防护体系。提高用户的安全意识，加强安全管理和培训也是不可或缺的一环。只有这样，才能更好地应对物联网安全挑战，推动物联网技术的持续健康发展。

参考文献

[1]刘畅.物联网计算机网络安全与控制策略分析[J].无线互联科技,2022,19(03):11-12.

[2]王坚.网络安全技术在计算机维护中的运用[J].电脑知识与技术,2021,17(19):36-37+49.

[3]王超.物联网计算机网络安全与远程控制技术初探[J].信息记录材料,2020,21(10):176-177.

[4]王志强.物联网计算机网络安全与远程控制技术初探[J].电子测试,2020(13):96-97.