 DOI: https://doi.org/10.12349/iser.v4i4.1670

Research on Security Technology Application in Electronic Information Engineering

Huina Zhang

Dongming County Emergency Management Guarantee and Technical Service Center, Heze, Shandong, 274500, China

Abstract

This paper studies the application of security technology in electronic information engineering technology, mainly discussing data security, network security, and Internet of Things security, and exploring relevant solutions. Through in-depth analysis, this paper aims to enhance readers' understanding of the field of electronic information engineering security and emphasize its importance in modern technology.

Keywords

electronic information engineering; information security technology; application

电子信息工程中的安全技术应用研究

张惠娜

东明县应急管理保障与技术服务中心，中国 · 山东 菏泽 274500

摘　要

论文研究了电子信息工程技术中的安全技术应用，主要讨论了数据安全、网络安全以及物联网安全，并探讨了相关的解决方法。通过深入分析，论文旨在提高读者对电子信息工程安全领域的理解，强调其在现代科技中的重要性。

关键词

电子信息工程；信息安全技术；应用

1 引言

电子信息工程技术作为现代科技领域的重要分支，已经深刻地改变了我们的生活和工作方式。随着信息化进程的不断推进，电子信息工程技术在各个领域的应用日益广泛。然而，这种广泛的应用也伴随着安全性挑战的不断增加。数据泄露、网络攻击和物联网漏洞等安全问题已成为电子信息工程技术领域的重要议题。因此，研究和应用安全技术以应对这些挑战至关重要。论文旨在深入探讨电子信息工程技术中的安全技术应用，以增进对该领域的理解，并提供解决方案来确保信息和系统的安全性。

2 电子信息工程技术概述

电子信息工程技术是一门多学科交叉的领域，它集成了电子工程、计算机科学、通信技术和信息处理等知识，旨在开发和维护各种信息系统和设备。这些系统和设备可以包括通信网络、嵌入式系统、传感器、计算机硬件和软件等。电子信息工程技术的应用领域多种多样，其影响几乎触及了每个行业和领域。通信与网络领域推动了移动通信、卫星通信和互联网的迅速发展。计算机与软件领域的创新推动了计算机科学的进步，催生了人工智能、大数据分析和云计算等领域的发展。物联网和嵌入式系统的应用改变了我们与设备和环境互动的方式。医疗与生命科学受益于生物医学工程和医疗信息技术的发展，提高了医疗诊断和治疗的效率。电子信息工程技术还在能源管理和环境保护方面发挥了积极作用。未来，电子信息工程技术将继续受益于新兴技术的涌现，如量子计算、边缘计算和区块链等。这些新技术将不断拓展其应用领域，进一步推动电子信息工程技术的发展。电子信息工程技术的核心原理包括数字信号处理、通信协议、嵌入式系统设计、大数据处理以及人工智能和机器学习等。这些原理和概念相互交织，构成了电子信息工程技术的技术基础，为其在各个应用领域中的成功发展提供了支撑 [1]。

3 电子信息工程中的安全问题

3.1 数据安全问题

数据安全一直是电子信息工程技术领域中的一个核心问题。随着信息技术的迅猛发展和数字化数据的广泛应用，数据的保护和安全性成为至关重要的挑战。首先，数据泄露威胁着个人隐私和企业机密。无论是由内部员工的不当行为

【作者简介】张惠娜（1984–），女，中国山东菏泽人，本科，工程师，从事信息工程研究。

还是外部黑客的恶意攻击，一旦敏感数据落入错误的手中，可能导致严重的隐私侵犯和机密信息泄露。其次，不适当的加密算法或密钥管理可能导致数据易受攻击。例如，如果使用弱密码或者未经充分测试的加密算法，黑客可能会轻松地解密受保护的数据，从而访问其内容。因此，数据加密技术的研究和实施至关紧迫，以确保数据在传输和存储过程中的安全性。再次，数据的访问控制也是数据安全的重要组成部分。不当的权限设置可能使未经授权的用户获得对敏感数据的访问权限，从而引发潜在的数据泄露风险。最后，有一个关键因素是数据备份和恢复策略。没有有效的数据备份和恢复策略可能导致数据丢失，无法恢复。在电子信息工程中，数据备份是一项关键的任务，必须定期进行备份，以确保在数据丢失或损坏的情况下能够迅速恢复到以前的状态。

3.2 网络安全问题

在电子信息工程技术的广泛应用中，网络安全问题与数据安全问题密切相关，是一个不可忽视的重要方面。首先，网络作为数据传输和通信的主要媒介，容易成为黑客和恶意软件的目标。恶意软件，如病毒、间谍软件和勒索软件，可能感染计算机系统，损害网络安全。这些威胁可能通过恶意附件、恶意链接或未经授权的下载进入网络，因此需要有效的反恶意软件措施。其次，拒绝服务攻击（DDoS）也是网络安全问题的一部分。攻击者可能发起 DDoS 攻击，通过洪水般的流量使网络服务不可用，从而影响正常业务运行。这种攻击可能导致企业服务中断，损害声誉，甚至造成财务损失。最后，网络漏洞是网络安全的关键问题之一。未修补的网络漏洞可能被黑客利用，导致入侵和数据泄露。因此，网络管理员必须及时识别和修复潜在的漏洞，以确保网络的安全性 [2]。

3.3 物联网中的安全挑战

物联网的崛起为电子信息工程领域带来了革命性的变化，然而它也引入了一系列复杂的安全挑战，需要认真研究和解决。首先，物联网设备通常分布在各种环境中，包括户外、工厂和医院等。这些设备容易受到物理访问和恶意干预的威胁。攻击者可能试图篡改或禁用设备，对设备进行未经授权的修改，或者窃取设备中的敏感信息。因此，确保物联网设备的物理安全性至关重要。这包括采取适当的访问控制、设备封装和加密技术，以保护设备免受未经授权的访问和物理攻击。其次，物联网设备之间的通信也面临着安全挑战。设备之间的数据传输需要进行加密以保护数据的机密性，以防止数据截获和篡改。物联网通信通常是异构的，涉及多种通信协议和技术，这增加了管理和维护安全性的复杂性。最后，物联网设备通常运行特定的固件和软件，这些软件需要定期更新以修复安全漏洞和提高安全性。但是，在大规模物联网环境中，设备的管理和维护变得更加复杂。设备可能分布在不同的地理位置，而且更新可能需要考虑设备的能耗和计算能力。所以，确保设备的固件和软件安全性，包括及时的漏洞修复和安全更新，是一项重要任务。

4 数据安全技术应用

在电子信息工程中，数据安全技术的应用至关重要。以下将探讨数据安全技术在电子信息工程中的广泛应用，包括数据加密、访问控制和身份认证以及数据备份和灾难恢复策略。首先，数据加密技术在电子信息工程中的应用是为了确保数据的保密性。无论数据在传输过程中还是储存在数据库或云存储中，数据加密都可以有效地防止未经授权的访问。通过使用复杂的加密算法，数据在被传送或存储时会被转化为一种非常难以理解的形式，只有具备解密密钥的授权用户才能还原其原始内容。这种方法不仅适用于网络传输，还适用于本地数据存储，即使攻击者物理获得访问权限也无法轻易解密数据，因为他们没有解密密钥。其次，访问控制和身份认证在数据安全中的作用非常重要。它们旨在确保只有授权用户能够访问系统和数据资源。身份认证是第一道防线，要求用户提供有效的身份验证信息，例如用户名和密码、生物识别数据或者多因素认证。一旦用户身份得到确认，访问控制策略会确定该用户可以执行哪些操作，并限制对敏感数据的访问。最后，数据备份和灾难恢复策略是在数据丢失或系统崩溃时保护数据的关键措施。定期备份是将敏感数据复制到安全存储介质的过程，以防止数据丢失。备份应具有版本控制，以便在需要时还原到先前的状态。同时，制定灾难恢复计划是至关重要的，它详细说明了如何在灾难事件发生时恢复数据、重新构建系统和确保业务连续性 [3]。

5 网络安全技术应用

网络安全技术在电子信息工程中的角色举足轻重，在当今数字化时代，信息系统和网络面临着日益复杂和多样化的威胁。为了维护信息的机密性、完整性和可用性，电子信息工程领域必须采用创新的安全技术来保护其资产和用户的数据免受攻击。首先，防火墙技术作为网络安全的第一道防线，旨在监控、过滤和控制进出网络的数据流量。防火墙可以根据事先定义的规则，阻止未经授权的访问和恶意流量进入网络。它可以实施不同层次的保护，包括网络层、传输层和应用层。网络层防火墙通常基于 IP 地址和端口号来控制流量，而应用层防火墙可以深入检查数据包中的内容，以识别潜在的威胁和恶意行为。防火墙技术的应用有助于减轻网络攻击的风险，保护敏感信息免受未经授权的访问。其次，入侵检测系统（IDS）和入侵防御系统（IPS）是关键的网络安全组件，用于监测和应对网络中的威胁。IDS 负责实时监测网络流量和系统活动，以检测异常行为和潜在的入侵。一旦发现异常，IDS 会触发警报并记录事件，以供后续分析。IPS 进一步增强了网络安全，它可以主动响应威胁，例如自动阻止具有恶意特征的流量或封锁潜在的攻击者。这些系统可以基于特征、行为和统计信息来检测威胁，提供了多层次的威胁防护。最后，安全审计和监控是维护网络和系统安全

性的重要组成部分。安全审计涉及记录和分析用户和系统活动的日志，以识别潜在的安全问题和威胁。监控系统实时监视网络和服务器的性能和安全状态以及异常活动的出现。通过分析审计日志和监控数据，安全专业人员可以及时识别安全事件并采取必要的措施，以降低潜在的风险概率。

6 物联网安全技术应用

首先，在物联网中，海量的数据不断从各种传感器和设备中产生和传输，这些数据可能包含敏感信息，如个人健康数据、商业机密和安全指标。因此，数据保护在物联网中至关重要。安全技术应用包括数据加密、数据隐私保护和访问控制。数据加密确保数据在传输和存储过程中得到保护，只有经过授权的用户才能解密和访问数据。其次，数据隐私保护技术可以对数据进行匿名化处理，以保护用户的隐私。访问控制技术则确保只有授权的设备和用户可以访问物联网数据资源。再次，物联网的网络拓扑复杂，涉及各种设备之间的通信，包括传感器、嵌入式系统和云端服务器。网络安全技术在物联网中起着关键作用，以防止未经授权的访问、数据篡改和拒绝服务等网络威胁。技术应用包括网络分段、入侵检测系统和网络隔离。网络分段将物联网划分为不同的网络区域，以减少攻击面。入侵检测系统监视网络流量，及时发现异常行为。网络隔离技术可确保在网络中的某个部分受到攻击时，不会影响整个系统的运行。最后，物联网安全监控和事件响应是保持系统的连续性和完整性的重要组成部分。安全监控系统持续监测物联网的状态和数据流量，以便及时发现潜在的威胁和漏洞。一旦发现异常情况，事件响应团队将采取适当的措施来隔离威胁、恢复系统并进行事后分析。这包括制定紧急计划、修补漏洞、加强访问控制和改进安全策略。

7 结论

论文深入探讨了电子信息工程中的安全技术应用，聚焦于数据安全、网络安全以及物联网中的安全问题。在不断发展的技术背景下，保护信息资产和系统安全性变得至关重要。数据加密、访问控制、防火墙等安全技术在电子信息工程中的应用具有重要意义。随着技术的不断进步，电子信息工程领域的安全需求也在不断演变。数据的价值愈发重要，网络的复杂性不断增加，物联网的普及程度也在上升。因此，必须保持警惕，不断改进和加强安全技术的应用，以确保信息的机密性、完整性和可用性。

参考文献

[1] 李冬辰.计算机电子信息工程技术的应用和安全研究[J].环球市场,2021(8):385-386.

[2] 陈春至,阎玲.电子信息工程中的安全技术应用[J].集成电路应用,2022(5):39.

[3] 齐邦强.信息安全技术在电子信息工程中的应用与解析[J].信息与电脑,2019,31(19):3.