电子信息技术在网络安全保障中的应用研究

陈　光　赵　旭
天津理工大学中环信息学院　天津　300000

摘　要：本文深入探讨了电子信息技术在网络安全保障领域的应用。首先对电子信息技术进行了概述，阐述了其基本概念与特点。接着分析了电子信息技术与网络安全保障之间的紧密关系，强调了电子信息技术在维护网络安全中的重要性。随后详细介绍了电子信息技术在网络安全保障中的关键技术应用，包括加密技术、防火墙技术、入侵检测与防御技术、身份认证与访问控制技术以及安全审计与监控技术，并对每种技术的应用原理、优势及局限性进行了分析。最后对电子信息技术在网络安全保障中的应用进行了总结与展望，为进一步推动网络安全保障技术的发展提供了参考。

关键词：电子信息技术；网络安全保障；加密技术；防火墙技术；入侵检测与防御

引言

在信息技术高速发展的今天，网络已渗透到了人们生活与工作中的每一个领域，是现代社会中不可缺少的组成部分。但是网络的开放性与共享性同时带来许多安全隐患，例如黑客攻击，病毒传播，数据泄露等等，这些都严重威胁到个人，企业以及国家的安全。电子信息技术是信息技术的一个重要部分，对于网络安全保障起到了至关重要的作用。通过先进电子信息技术的应用，能够对各类网络安全威胁进行有效的防范，探测与处理，确保网络系统正常工作以及数据安全。所以，对电子信息技术应用于网络安全保障进行深入的研究是非常有实际意义的。

一、电子信息技术概述

电子信息技术融合了电子技术、信息技术和计算机技术等多个学科的知识，它是推动现代科技进步的关键因素之一。它是利用电子设备作为载体，在电子元件、电路和系统等辅助下，达到精准处理和高效传输电信号。信息处理环节中，电子信息技术凭借计算机运算能力强的特点，实现了大量数据的快速获取，存储，分析和挖掘，使数据由无序走向有序，并从中挖掘出有价值的信息。就通信领域而言，其建设了一个巨大且复杂的网络，不管是光纤通信、移动通信或者卫星通信都需要电子信息技术作为支持，使信息瞬间穿越万水千山，全球实时沟通。与此同时，电子信息技术也促进了智能化发展，人们通过在电子设备中集成传感器，人工智能算法等来使之具有感知，思维与决策能力，实现智能家居和智能交通、智能医疗及其他应用的出现在很大程度上改变着人们生活与工作的方式。另外，电子信息技术在工业生产，金融服务以及国防军事各领域都有着广泛的应用，已经成为社会进步，经济发展以及国家安全的主要驱动力，它的不断发展与创新，将会继续给人类社会提供更大的方便与改变。

二、电子信息技术与网络安全保障的关系

电子信息技术为网络安全保障奠定了稳固的基石，也为安全网络环境建设提供了大量技术手段。在数据层面上，它具有较强的数据处理能力，能够实时监控和分析流转在网络上的大量信息，准确识别出异常数据流，从而为及时发现潜在的安全威胁提供了可能性；通信技术确保了安全命令和防护信息能够迅速且准确地传达，从而使安全防护措施能够迅速响应并部署到适当的位置。与此同时，电子信息技术智能化的发展也催生出智能防火墙和入侵检测系统这类借助于机器学习和深度学习算法的高级工具，能够自主地学习网络行为模式、自动地调整防护策略、有效地应对网络攻击手段的变化。

网络安全保障的要求反过来也反向促进了电子信息技术不断革新。面对越来越严重的网络安全挑战，例如黑客攻击的复杂性和病毒变种的多样性，电子信息技术正在努力突破技术的限制，以研发更为高效和安全的加密算法和身份验证技术。网络安全保障对于数据隐私保护和系统稳定运行提出的更高需求也刺激了电子信息技术从数据加密强度和系统容错能力两个方面进行持续优

化升级。可以说电子信息技术对网络安全保障起到了强有力的支持作用，网络安全保障工作的需要也给电子信息技术指出了前进的道路，两者共同促进网络空间向更安全，更稳定，更可靠的方向迈进。

三、电子信息技术在网络安全保障中的关键技术应用

（一）加密技术

加密技术是保障网络安全的核心手段之一，它如同给数据穿上了一层“隐形衣”，让未经授权者难以窥探数据内容。其核心原理是运用特定算法将明文数据转换为密文，只有掌握正确密钥的接收方才能将其还原为明文。对称加密算法中，加密和解密使用同一密钥，就好比用同一把钥匙开锁，像AES算法，凭借其高效的加密速度和较高的安全性，广泛应用于大量数据的快速加密场景，如文件传输、数据库加密等，能在短时间内完成大量数据的加密处理。非对称加密算法则使用一对密钥，公钥用于加密，私钥用于解密，如同一个公开的信箱和一把专属的钥匙，只有持有私钥的人才能打开信箱取出信件，RSA算法就是典型代表，常用于数字签名、密钥交换等关键环节，确保数据来源的真实性和完整性。此外，哈希算法虽不属于传统加密，但能将数据生成固定长度的哈希值，用于数据完整性校验，一旦数据被篡改，哈希值就会改变，就像给数据打上了一个独特的“指纹”，可及时发现数据是否被恶意修改，为网络安全筑牢防线。

（二）防火墙技术

防火墙技术是网络安全的核心防线，通过在网络边界部署硬件或软件系统，对进出网络的数据包进行深度检查与过滤。它依据预设的安全策略，基于源IP地址、目的IP地址、端口号及协议类型等参数，决定是否允许数据包通过。包过滤防火墙通过逐包检查数据包头部信息，快速筛选出符合规则的数据包，虽效率较高，但对应用层攻击的防御能力有限。状态检测防火墙则在此基础上，跟踪网络连接的状态信息，确保只有符合状态要求的数据包能够通过，有效抵御如IP欺骗等攻击。应用层防火墙深入解析应用层协议，对数据包内容进行细致审查，能精准识别并阻止恶意流量，但可能影响网络性能。防火墙还具备网络地址转换功能，将内部私有IP地址转换为公共IP地址，隐藏内部网络结构，提升安全性。同时，它支持虚拟专用网络技术，为远程用户提供安全的加密通信通道。此外，防火墙能记录网络流量和安全事件的日志，为安全审计和事件追溯提供依据。随着技术发展，防火墙不断融合深度包检测、入侵防御等高级功能，形成更全面的安全防护体系，在保护企业和个人网络安全方面发挥着不可替代的作用。

（三）入侵检测与防御技术

入侵检测技术通过实时监控网络流量、系统日志与用户行为，运用特征比对或异常分析识别潜在攻击。特征检测依赖已知攻击模式数据库，将当前活动与特征库对比匹配，可精准识别已知威胁；异常检测则通过建立正常行为基线模型，当系统检测到显著偏离基线的行为时，判定为异常并触发警报。入侵防御技术在此基础上进一步升级，不仅能实时检测攻击，还能主动采取措施阻止恶意行为。入侵防御系统部署在网络关键节点，采用深度包检测技术，深入分析数据包内容，发现隐藏在加密流量或复杂协议中的恶意活动。一旦检测到潜在威胁，系统会立即采取行动，如丢弃可疑数据包、阻断攻击者IP地址等，从源头上阻止攻击。此外，入侵防御系统具备自我学习与自适应能力，能通过抓取网络数据流中的规则库，挖掘有效数据信息建立新的安全策略模型，不断优化防御机制。同时，入侵防御系统还能与其他安全工具集成，实现自动化响应，减少人工干预需求，提高应急响应速度，为网络安全提供全方位、多层次的保障。

（四）身份认证与访问控制技术

身份认证是验证用户身份的过程，其技术涵盖生物认证与非生物认证两大类。生物认证利用用户独有的生物特征，如指纹、虹膜、语音等，具有高安全性与准确性，但实现成本较高，像指纹认证通过比对皮肤纹路特征确认身份，应用于门禁系统等场景；非生物认证则依赖用户所知信息或所持物品，如密码、智能卡等，密码认证虽基础但易被破解，智能卡认证通过存储密钥或证书来验证身份。访问控制旨在限制用户对系统资源的访问权限，确保资源安全完整。自主访问控制允许资源所有者自主决定访问权限，通过访问控制列表记录权限，灵活性高但可能导致管理混乱；强制访问控制由系统策略决定权限，使用安全标签标识资源和实体，严格且一致，但灵活性欠佳；基于角色的访问控制将权限与角色关联，用户通过成为角色成员获得权限，利于权限管理与职责分离，适用于复杂权限需求场景。在实际应用中，应结合具体场景和需求选择合适的身份认证和访问控制技术，并采用多因素认证、定期更新凭证、实施最

小权限原则等最佳实践，以增强系统安全，防范未授权访问。

（五）安全审计与监控技术

安全审计聚焦于对网络活动、系统操作和用户行为的全面记录与分析，它收集各类日志信息，涵盖操作系统日志、应用程序日志、网络设备日志等，通过深度挖掘这些日志数据，能发现潜在的安全风险与违规操作。例如，审计人员可分析用户登录记录，识别异常的登录时间、地点或频繁的登录失败尝试，以此判断是否存在账号被盗用的风险。安全监控则侧重于实时追踪网络状态与系统运行情况，借助流量监测工具，可实时掌握网络带宽使用情况、数据传输流向，及时发现异常流量峰值，这可能预示着网络攻击，如分布式拒绝服务攻击（DDoS）。同时，监控系统能对关键业务系统进行性能监测，当系统响应时间过长或出现故障时，迅速发出警报。此外，安全审计与监控技术还能相互协同，审计结果为监控策略的调整提供依据，而监控数据又丰富了审计分析的内容。通过对审计与监控数据的综合分析，安全团队能够构建全面的安全态势感知，快速定位安全事件源头，评估事件影响范围，并采取针对性的应对措施，有效降低安全事件带来的损失，确保网络系统的稳定、安全运行。

结论

综上，电子信息技术对网络安全保障起到关键作用，加密技术、防火墙技术、入侵检测与防御技术、身份认证与访问控制技术和安全审计与监控技术这几个关键技术的运用对网络安全起到多层次保护作用。但随着网络技术的发展，网络安全威胁变得越来越复杂，电子信息技术对网络安全保障提出了许多挑战。在今后的发展中，必须要进一步强化电子信息技术研究与创新，在增强网络安全防护能力的前提下，强化网络安全管理、建立与完善网络安全制度、共同建设安全、可靠的网络环境。

参考文献

[1]吴建军.信息安全技术在计算机网络中的应用[J].集成电路应用，2023，40（2）：258-259.

[2]代兵.电子信息技术在网络安全中的应用研究[J].信息记录材料，2025，26（2）：126-128.

[3]冯云婷，李攀，李景景，等.电子信息工程中网络安全技术应用研究[J].软件，2025（2）.

[4]贾美明.大数据背景下计算机信息技术在网络安全中的运用[J].2024.

[5]肖习江，刘涛.网络信息安全技术在高校信息化建设中的应用[J].通讯世界，2024，31（3）：36-38.