计算机技术在保障电子信息安全中的应用研究

武晓阳
保定市交通运输局满城区养路工区　河北　保定　071000

摘　要：数字化深度渗透下，电子信息安全至关重要，关乎国家、企业与个人权益及数字经济发展。然而，其面临黑客攻击、病毒恶意软件、网络钓鱼诈骗、内部威胁等挑战。计算机技术中，防火墙、加密、入侵检测与防御、访问控制等技术为信息安全提供保障。未来，人工智能与机器学习、量子加密、区块链技术将进一步发展，推动电子信息安全防护向主动智能、量子时代安全、多领域拓展方向转型。

关键词：计算机技术；电子信息安全；应用研究

引言：在数字化浪潮席卷全球的当下，电子信息技术深度融入社会各个层面，电子信息安全的重要性愈发凸显。从国家关键基础设施的稳定运行，到企业核心数据的资产安全，再到个人隐私与财产的切实保障，无一不依赖稳固的信息安全防线。然而，电子信息领域面临的威胁与挑战也日益复杂多样。在此背景下，深入探讨计算机技术在保障电子信息安全中的应用及未来发展趋势，具有重要的现实意义。

1 电子信息安全的重要性

在数字化深度发展的当下，电子信息安全至关重要，是保障社会、企业与个人权益的核心基石。国家层面，它是国家安全的关键部分，关乎国防、政务、金融等关键基础设施稳定运行。若核心信息系统遭攻击，会引发能源中断、金融混乱等危机，威胁国家主权安全。企业方面，客户数据、商业机密等核心信息是重要资产，良好的电子信息安全保障能防止数据泄露、机密被窃，维护企业信誉与竞争力，反之会给企业带来巨额损失甚至倒闭风险。个人角度，其关乎个人隐私与财产安全，个人信息泄露可能引发电信诈骗、身份冒用等问题。在数字经济蓬勃发展时，电子信息安全是推动新业态健康发展的前提，筑牢安全防线才能释放数字化红利，保障社会经济持续稳定发展[1]。

2 电子信息安全面临的威胁

2.1 黑客攻击

黑客攻击是电子信息安全领域的常见且具破坏性的威胁，手段随技术发展不断升级，目标广泛，涵盖个人、企业及国家关键信息系统，如今已形成专业化、产业化模式，部分黑客组建地下产业链。攻击手段多样，DDoS攻击通过控制僵尸网络发送海量请求，使服务器瘫痪，给电商平台等带来经济损失；渗透攻击利用系统漏洞植入恶意代码，窃取或篡改数据；高级持续性威胁（APT）攻击隐蔽性强，黑客长期潜伏在目标网络收集信息并攻击，常针对政府机构、企业等重要目标，危害难以估量。如部分企业因未及时更新系统补丁，导致客户信息被窃取并在暗网出售。

2.2 病毒与恶意软件

病毒与恶意软件是危害电子信息安全的载体，传播性强、隐蔽性高、破坏性大。计算机病毒可自我复制，通过邮件附件、移动存储设备等途径传播，侵入系统后破坏文件、占用资源甚至致系统崩溃。如“勒索病毒”加密用户文件索要赎金，影响众多企业、医院等。恶意软件种类丰富，间谍软件偷偷收集用户隐私数据；木马程序伪装合法软件，窃取敏感信息。移动互联网发展使手机等移动设备成恶意软件新目标，其伪装成正规APP传播，给用户带来隐私泄露和财产损失双重风险。

2.3 网络钓鱼与诈骗

网络钓鱼与诈骗以欺骗手段获取用户敏感信息，发案率高且手段不断翻新、更具迷惑性。网络钓鱼常伪造邮件、网站、短信等，冒充可信主体，以账户异常等名义诱骗用户点击链接或填写信息。如诈骗分子伪造银行短信，引导用户进入钓鱼网站窃取银行卡信息。社交媒体普及使钓鱼场景延伸，利用信任场景成功率提升。网络诈骗形式多样，结合虚假投资等形成复合型模式，不仅窃取信息还骗取资金。这类威胁针对民众防范弱点，利用心理诱导攻击，造成个人财产损失，破坏网络信任体系，影响数字经济健康发展。

2.4 内部威胁

内部威胁是电子信息安全中易被忽视却危害大的隐患，源于组织内部人员有意或无意行为，挑战组织核心信息安全。内部威胁分恶意和无意两类，恶意威胁由不满员工、商业间谍等实施，他们利用权限和信息优势，窃取商业机密、篡改数据、泄露客户信息。如员工离职

前恶意删除公司数据致项目停滞，商业间谍潜伏收集核心技术资料[2]。无意威胁是员工因安全意识薄弱或操作失误引发风险，如误点钓鱼邮件、使用弱密码等，虽非主观恶意，但也可能致系统入侵、数据泄露。

3 计算机技术在保障电子信息安全中的应用原理

3.1 防火墙技术

防火墙技术是保障网络边界安全的核心，能构建网络访问的“安全关卡”，依据预设规则控制进出网络的数据流，初步拦截网络攻击。其核心工作原理基于访问控制策略，隔离内部与外部不安全网络（如互联网），仅允许符合规则的数据流通过。防火墙主要依靠包过滤、状态检测、应用代理三种核心技术防护。包过滤是基础方式，检查数据包头的源IP、目标IP、端口号等信息，与预设规则匹配，允许符合规则的数据包通过，拒绝不符合的。状态检测更智能，不仅检查数据包静态信息，还跟踪连接状态，如建立、传输、断开连接等，只允许合法状态下的数据包通过，可有效防范伪造数据包攻击。应用代理技术在内外网络间建代理服务器，内外网络通信都经其中转，代理服务器对应用层数据检测过滤，提升防护精度，不过对网络性能影响较大。三种技术结合，防火墙构建起多层次的网络边界防护体系，为电子信息安全提供有力保障。

3.2 加密技术

加密技术是保护信息机密性的关键技术，通过特定的算法将原始明文信息转换为不可直接读取的密文，只有拥有合法密钥的接收者才能将密文解密为明文，从而防止信息在传输和存储过程中被窃取或篡改。加密技术主要分为对称加密和非对称加密两大类，两者各有特点并常结合使用。对称加密技术的核心是加密密钥和解密密钥相同或可相互推导，其优势是加密和解密速度快、效率高，适合对大量数据进行加密处理，常见的算法有DES、AES等。在实际应用中，对称加密常用于本地数据存储加密或高速数据传输加密，如对数据库中的敏感数据进行加密存储，确保即使数据库被入侵，攻击者也无法直接获取明文信息。非对称加密技术则采用一对密钥，即公钥和私钥，公钥可公开传播，私钥由用户自行保管，用公钥加密的信息只能用对应的私钥解密，反之亦然。其优势是解决了对称加密中密钥传输的安全问题，常见的算法有RSA、ECC等。在数据传输场景中，通常先通过非对称加密方式传递对称加密的密钥，再使用对称加密技术对实际数据进行加密传输，既保证了密钥传输的安全性，又兼顾了数据传输的效率。加密技术还与数字签名、数字证书等技术结合，实现对信息完整性和发送者身份的验证，进一步提升信息安全保障能力。

3.3 入侵检测与防御技术

入侵检测与防御技术（IDS/IPS）是网络安全防护的“监控与反击系统”，通过实时监测网络或系统中的行为，及时发现并处置入侵行为，弥补防火墙仅防范边界攻击的不足，形成纵深防御体系。入侵检测技术（IDS）主要负责“检测”，其工作原理是通过收集网络中的数据流、系统日志、应用日志等信息，运用特征检测、异常检测等方法对这些信息进行分析，识别是否存在违反安全策略的入侵行为。特征检测方法基于已知的攻击特征库，将收集到的信息与特征库中的攻击模式进行匹配，一旦匹配成功则发出告警，这种方法准确率高，但对未知攻击的检测能力较弱[3]。异常检测方法则先建立系统或网络的正常行为模型，如正常的流量分布、用户操作习惯等，当监测到的行为偏离正常模型且超过预设阈值时，即判定为异常行为并发出告警，这种方法能检测到未知攻击，但误报率相对较高。入侵防御技术（IPS）是在IDS基础上发展而来，除了具备检测功能外，还能在发现入侵行为时主动采取防御措施，如阻断攻击连接、丢弃恶意数据包、修改防火墙规则等，实现对入侵行为的实时拦截。IPS通常部署在网络关键节点，如防火墙之后、核心服务器之前，对进出核心区域的数据流进行实时监测和处置，与防火墙形成互补，构建起“边界防护+内部监控”的多层次安全防护体系。

3.4 访问控制技术

访问控制技术是保障信息系统安全的基础技术，通过对用户或终端的访问权限进行严格管理，确保只有授权主体才能访问特定资源，防止未授权访问导致的信息泄露或破坏。其核心原理是遵循“最小权限原则”，即给用户分配完成工作所需的最小权限，避免权限过大带来的安全风险。访问控制技术主要包括自主访问控制、强制访问控制、基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）等类型。自主访问控制由资源所有者决定谁能访问资源及访问权限，灵活性较高，但安全性依赖于所有者的安全意识，适用于对安全性要求不高的场景。强制访问控制则由系统根据资源和主体的安全级别强制分配访问权限，主体只能访问安全级别匹配的资源，安全性高，适用于政府等对安全性要求极高的领域。基于角色的访问控制是目前应用最广泛的方式，先根据组织的业务需求定义不同角色，如管理员、普通员工、客户等，为每个角色分配相应的访问权限，再将用户分配到对应角色，用户通过角色获得访问权限，这种方式简化了权限管理，便于批量调整权限，适合企业

级信息系统。基于属性的访问控制则更灵活，通过综合考虑主体属性（如用户身份、职位）、资源属性（如资源类型、敏感级别）、环境属性（如访问时间、地点）等多方面因素，动态判断是否授予访问权限，适用于复杂的云计算、物联网等场景。

4 计算机技术在保障电子信息安全中的未来发展趋势

4.1 人工智能与机器学习在信息安全中的应用

人工智能与机器学习凭借强大的数据处理和模式识别能力，成为电子信息安全领域核心驱动力，推动安全防护从“被动”向“主动智能防御”转型。传统安全防护依赖人工规则应对已知威胁，难以应对复杂未知威胁，而人工智能与机器学习通过学习海量安全数据，实现威胁智能识别、预测和处置。在威胁检测上，机器学习模型学习历史攻击和正常网络行为数据，构建精准检测模型，能发现未知攻击和零日漏洞攻击，降低误报和漏报率。恶意软件分析中，人工智能自动对可疑文件进行静态和动态行为分析，判断是否为恶意软件，分析攻击路径和破坏方式，辅助应急响应。安全运维方面，人工智能驱动的自动化运维平台实时监控系统，自动发现并修复隐患，减轻运维负担。另外，它还可用于钓鱼邮件识别、身份认证等场景，如通过分析用户行为生物特征进行智能身份验证，未来大模型技术将使其在更复杂场景发挥作用，构建智能安全防护体系。

4.2 量子加密技术的发展前景

量子加密技术基于量子力学原理，具有“不可破解”的安全优势，是应对量子计算时代密码破解威胁的核心技术，前景广阔。传统加密依赖数学难题复杂性，而量子计算机强大的并行计算能力可短时间内破解RSA等传统算法，给信息安全带来挑战，量子加密技术能解决这一问题。其核心技术是量子密钥分发（QKD），利用量子态叠加性和测量扰动原理实现密钥安全传输。发送方通过量子信道向接收方发送量子态载体，因量子态不可克隆，窃听会改变其特性，双方检测可发现窃听，确保密钥安全。目前，量子加密技术进入实用化初期，国内外建成多条量子通信骨干网，如“京沪干线”，在金融、政务等领域试点应用[4]。未来，量子通信技术将成熟，传输距离延长、速率提升、成本降低，实现全面覆盖，量子加密与经典通信融合技术将突破，推动其在个人通信等多领域广泛应用，构建量子时代安全信息传输体系。

4.3 区块链技术增强信息安全

区块链技术以去中心化、不可篡改、透明可追溯等特性，为解决信息安全信任问题提供新思路，在增强信息安全方面潜力巨大，应用场景将不断拓展。去中心化是核心优势，传统信息系统依赖中心服务器，一旦被攻击或篡改，系统安全性受威胁，而区块链将数据存储在多个节点，无单一中心控制点，部分节点被攻击不影响整体数据安全。不可篡改通过密码学算法和共识机制实现，数据记录到区块链上后，修改难度极大，有效防止恶意篡改。透明可追溯使区块链上交易和数据操作可实时查看和追溯，便于责任认定和审计监管。未来，随着与隐私计算、智能合约等技术深度融合，将解决数据透明与隐私保护的矛盾，拓展在医疗数据共享、金融交易安全等敏感领域的应用，为信息安全提供更全面保障。

结束语

电子信息安全是数字化时代的关键防线，关乎社会稳定、企业兴衰与个人权益。当前，计算机技术虽为保障信息安全筑牢根基，但威胁不断演变升级。未来，人工智能与机器学习、量子加密、区块链等新兴技术将带来新契机。我们应紧跟技术发展趋势，持续创新安全防护手段，构建更稳固、智能、全面的信息安全体系，为数字经济发展与社会稳定保驾护航。

参考文献

[1]黄建剑.浅谈电子信息技术在电力自动化系统中的应用[J].电脑知识与技术,2021,17(14):204-205+212.

[2]李秋昊.电子信息技术的应用特点及发展探索[J].信息记录材料，2021，22(06):209-210.

[3]赵永金.电子信息科学在计算机技术中的应用分析[J].科技经济导刊，2020，28(29):23+22.

[4]杨仕牧.基于互联网的电子信息科学技术创新分析[J].电子技术，2023，52(6):360-361.