电子信息工程中的安全技术应用分析

李 扬
济宁市兖州区疾病预防控制中心 山东 济宁 272000

摘 要：电子信息工程领域，安全技术应用至关重要。当前主要安全技术涵盖防火墙，通过设置屏障阻挡内外非法访问；加密技术利用特殊算法保护数据；身份认证结合多因素验证，防止非法操作；入侵检测系统实时监控异常行为；区块链确保数据不可篡改。面对电磁泄漏、硬件篡改、网络攻击等威胁，这些技术通过物理、网络、数据等多层防护，为电子信息工程筑牢安全防线，保障信息系统的稳定运行。

关键词：电子信息工程；安全技术；应用

引言：在当今数字化高速发展的时代，电子信息工程作为关键领域，深度融入社会各行业的运转体系，深刻改变着人们的生活与工作方式。然而，伴随着信息技术的广泛应用，电子信息工程所面临的安全挑战愈发严峻，从物理设备的潜在破坏到网络空间的恶意攻击，再到数据信息的非法窃取与篡改，安全威胁无处不在。因此，深入分析并合理应用安全技术，构建全方位、多层次的电子信息工程安全防护体系，具有重要的现实意义。

1 电子信息工程中的安全威胁分析

1.1 物理层安全威胁

（1）电磁泄漏与侧信道攻击风险突出。电子设备运行时会产生电磁辐射，攻击者可通过专用设备捕获这些辐射信号，还原设备处理的敏感信息，如电脑键盘敲击时的电磁信号可能被破解，导致密码泄露；侧信道攻击还可通过分析设备功耗、运算时间差异，推断加密密钥，对加密设备构成严重威胁。（2）硬件篡改与供应链攻击隐患显著。攻击者可能在硬件生产、运输环节篡改设备组件，如在路由器中植入恶意芯片，实现对网络数据的窃听；供应链攻击则针对硬件供应链薄弱环节，如2018年某知名芯片厂商被曝硬件存在后门，导致大量使用该芯片的设备面临安全风险。

1.2 网络层安全威胁

（1）黑客攻击频发且破坏力强。DDoS攻击通过大量虚假流量淹没目标服务器，导致网站、平台瘫痪，如某电商平台曾遭DDoS攻击，造成交易中断数小时；中间人攻击则拦截网络通信，窃取或篡改数据，如公共Wi-Fi环境下，攻击者可能伪装成热点，窃取用户登录账号、支付信息[1]。（2）恶意软件与勒索软件传播迅速。恶意软件可通过邮件附件、恶意链接侵入设备，窃取数据或破坏系统；勒索软件则加密用户文件，索要赎金，如“WannaCry”勒索软件曾全球爆发，感染数百万台设备，影响医院、企业等多个领域。

1.3 数据层安全威胁

（1）数据泄露与隐私侵犯事件频发。企业内部人员可能因疏忽或恶意泄露用户数据，如某社交平台曾曝数千万用户信息被泄露；第三方数据处理机构也可能因防护不足导致数据外泄，严重侵犯用户隐私。（2）伪造数据与算法攻击影响深远。攻击者通过伪造虚假数据注入系统，干扰决策，如在AI训练数据中混入伪造数据，导致模型识别错误；AI模型投毒攻击则破坏模型完整性，使其输出错误结果，影响自动驾驶、医疗诊断等关键领域。

1.4 典型案例分析

（1）Stuxnet病毒攻击工业控制系统造成重大损失。该病毒针对伊朗核设施的ICS系统，通过U盘传播，破坏离心机控制程序，导致大量离心机故障，延缓核设施建设，展现了工业控制系统面临的严峻安全威胁。（2）智能IoT摄像头隐私泄露事件频发。部分低端IoT摄像头存在安全漏洞，攻击者可破解摄像头密码，远程查看摄像头画面，导致用户家庭隐私泄露，此类事件多次引发社会关注。

2 电子信息工程中的安全技术应用

2.1 加密技术

（1）对称加密与非对称加密算法是信息安全的核心支撑。对称加密算法（如AES）以单一密钥实现数据加密与解密，运算速度快，适用于大规模数据传输场景，如云计算平台中服务器与存储设备间的实时数据加密；非对称加密算法（如RSA）采用公钥与私钥配对机制，公钥可公开分发，私钥由用户独自保管，安全性更高，广泛应用于数字签名、密钥交换等场景，如网银交易中的身份验证与数据防篡改。（2）量子加密技术凭借量子力学特性开启安全新方向。其利用“量子不可克隆定理”与“测不准原理”，确保加密密钥在传输过程中一旦被

窃取，就会因量子状态改变被即时察觉，从根本上杜绝密钥泄露风险。目前，我国已建成“京沪干线”量子保密通信骨干网络，在政务、金融等领域开展试点应用，未来有望成为应对量子计算威胁的核心技术。（3）在通信数据加密与区块链安全领域应用广泛。通信层面，5G网络通过加密技术对用户面与控制面数据进行保护，防止通信内容被窃听或篡改；区块链领域，加密算法保障区块数据的完整性与不可篡改性，如比特币采用SHA-256哈希算法生成区块标识，确保每一笔交易记录都可追溯且无法被恶意篡改[2]。

2.2 身份认证与访问控制

（1）多因素认证（MFA）技术大幅提升身份验证安全性。其结合“用户知道的信息”（如密码）、“用户拥有的设备”（如手机验证码）、“用户自身特征”（如指纹）等多种验证因子，即使单一因子泄露，攻击者也无法通过认证。目前，MFA已在金融APP、企业办公系统中普及，如支付宝登录需同时验证密码与手机短信验证码。（2）零信任架构（ZeroTrust）重塑电子信息工程安全防护理念。该架构遵循“永不信任，始终验证”原则，不再依赖传统网络边界防护，而是对每一次访问请求进行身份认证、权限管控与行为审计。例如，企业通过零信任架构，实现员工在远程办公时，需经过多轮验证才能访问内部核心数据，有效防范内部泄露与外部攻击。（3）生物特征识别技术凭借唯一性与便捷性广泛应用。指纹识别通过采集手指纹路特征进行身份验证，已集成于智能手机、笔记本电脑等设备；虹膜识别则利用眼球虹膜的独特纹理信息，因安全性更高，被应用于金融押运、边境安检等高端安全场景。

2.3 入侵检测与防御系统（IDS/IPS）

（1）基于机器学习的异常检测技术提升威胁识别能力。该技术通过对正常网络行为数据进行训练，建立行为模型，当检测到偏离模型的异常行为时，及时发出警报。例如，在企业网络中，机器学习算法可识别出“异常流量峰值”“陌生IP频繁访问”等攻击前兆，提前阻断潜在威胁。（2）软件定义网络（SDN）中的安全策略部署增强防护灵活性。SDN通过将网络控制层与数据转发层分离，可动态调整安全策略，实现对不同区域、不同业务的精准防护。例如，当某一服务器遭遇DDoS攻击时，SDN可快速调整网络路由，将攻击流量引流至清洗中心，保障其他服务器正常运行。（3）在工业互联网平台入侵防御实践中成效显著。例如，某汽车制造企业的工业互联网平台部署IDS/IPS系统后，成功拦截针对生产设备的恶意代码攻击，避免生产线停工；系统还能实时监控设备通信数据，识别出非法修改生产参数的行为，保障产品质量与生产安全[3]。

2.4 区块链与分布式安全

（1）区块链在数据不可篡改性中的应用解决信任难题。区块链将数据以区块形式按时间顺序链接存储，每个区块都包含前一区块的哈希值，若修改某一区块数据，需同时篡改后续所有区块，难度极大。例如，在农产品溯源领域，区块链记录种子采购、种植、加工、运输等全流程数据，消费者可扫码查询，确保信息真实可信。（2）智能合约安全漏洞防护成为区块链安全重点。智能合约因代码漏洞可能被攻击者利用，如“重入攻击”“整数溢出”等漏洞曾导致大量数字资产被盗。目前，通过代码审计、形式化验证等技术，可提前发现智能合约漏洞；部分区块链平台还推出漏洞赏金计划，鼓励白帽黑客挖掘漏洞并修复。（3）分布式存储系统的去中心化安全机制降低单点故障风险。传统集中式存储一旦服务器宕机，数据将面临丢失风险，而分布式存储将数据分割为多个片段，存储于不同节点，即使部分节点故障，也可通过其他节点恢复数据。例如，IPFS（星际文件系统）采用分布式存储架构，保障数据在去中心化网络中安全存储与快速访问。

2.5 人工智能安全技术

（1）对抗样本攻击与防御技术保障AI系统安全。对抗样本通过在正常数据中添加微小干扰，使AI模型误判，如在交通标志图像中添加细微噪点，导致自动驾驶系统将“停止标志”识别为“直行标志”。防御方面，可通过数据增强、对抗训练等方式提升AI模型的鲁棒性，减少对抗样本的影响。（2）AI驱动的威胁情报分析与响应提升安全处置效率。AI技术可实时采集全球范围内的威胁情报数据，快速分析攻击趋势、攻击手段与攻击源，生成防御策略。例如，安全厂商利用AI分析海量日志数据，可在几分钟内定位勒索软件的传播路径，并推送解密工具与防护方案给受影响用户。（3）联邦学习中的隐私保护技术解决数据共享与隐私矛盾。联邦学习让多个参与方在不共享原始数据的情况下，共同训练AI模型，仅传输模型参数，避免数据泄露。例如，多家医院通过联邦学习联合训练疾病诊断模型，既利用了多机构的数据优势提升模型准确率，又保护了患者隐私[4]。

2.6 物理层安全技术

（1）电磁屏蔽与抗干扰设计防范物理层信息泄露与干扰。通过在电子设备外壳采用金属屏蔽材料、内部线路布置电磁屏蔽层，可减少设备电磁辐射，防止攻击者通过电磁泄漏窃取信息；同时，抗干扰设计可降低外部

电磁信号对设备的影响，如在工业控制系统中，通过加装滤波器，避免电网波动对设备运行的干扰。（2）可信计算基（TCB）与硬件安全模块（HSM）筑牢物理安全防线。TCB是计算机系统中保障安全的核心组件，通过对TCB的完整性验证，确保系统未被篡改；HSM则是一种专用硬件设备，用于安全存储加密密钥、执行加密运算，如银行ATM机中的HSM模块，可保障交易过程中密钥的安全，防止密钥被窃取。

3 电子信息工程安全技术的挑战与未来发展趋势

3.1 当前安全技术面临的挑战

（1）算法复杂度与计算资源矛盾日益凸显。为提升安全防护能力，加密、检测等安全算法不断升级，复杂度持续增加，对设备的计算性能、存储容量要求也随之提高。例如，高精度的AI入侵检测算法需大量算力支撑，在普通物联网设备、边缘终端等资源受限场景中，难以高效运行，导致防护效果与设备性能难以兼顾。（2）跨平台安全协同的复杂性阻碍防护效能提升。当前电子信息系统涵盖云计算、物联网、工业互联网等多平台，不同平台的架构、协议、安全标准存在差异。如企业同时使用云端服务器、本地工控系统、员工移动终端，各平台的安全系统往往独立运行，数据难以互通、策略无法同步，当遭遇跨平台攻击时，无法快速联动响应，形成安全防护“孤岛”。（3）新兴技术（如量子计算）对现有加密体系构成严重威胁。现有主流加密算法（如RSA、ECC）的安全性依赖于“大整数分解”“离散对数”等传统数学难题，而量子计算凭借超强算力，可在短时间内破解这些难题。一旦量子计算技术成熟并普及，当前广泛应用于金融、政务、通信等领域的加密体系将面临失效风险，数据安全防线岌岌可危。

3.2 未来发展方向

（1）人工智能与安全技术的深度融合成为核心趋势。AI技术将全面赋能安全防护全流程：在威胁检测环节，通过深度学习分析海量数据，精准识别未知攻击模式；在响应处置环节，借助强化学习自动生成最优防御策略，实现攻击的实时阻断与系统修复。例如，AI驱动的自适应防火墙可根据网络环境变化动态调整防护规则，大幅提升安全防护的智能化与自动化水平。（2）轻量化安全协议在边缘设备的应用加速推进。针对物联网终端、边缘计算设备等资源受限场景，轻量化安全协议通过简化算法流程、减少数据交互量，在降低资源消耗的同时保障安全。如轻量级加密算法AES-128精简版、CoAPs安全协议，可在低算力、低带宽的边缘设备上高效运行，满足智慧家居、工业传感器等场景的安全需求。（3）国际标准与合规性（如GDPR、等保2.0）的适应成为企业安全建设重点。随着数据跨境流动频繁，各国对数据安全的监管日益严格。企业需在安全技术研发与应用中，主动适配GDPR的数据隐私保护要求、等保2.0的分级防护标准，通过建立合规的安全管理体系、部署符合标准的技术方案，确保业务运营合法合规，规避数据泄露引发的法律风险与声誉损失。

结束语

电子信息工程领域安全技术的研究与应用是一场持续的“攻防战”。随着技术迭代，安全威胁不断演变，这要求我们时刻保持警惕，紧跟技术发展趋势，不断创新与完善安全防护体系。未来，人工智能、量子计算等前沿技术既带来挑战，也提供了新的安全解决方案。我们需积极探索，将新技术融入安全体系，提升防护能力，为电子信息工程营造安全稳定的环境，保障其在各行业持续发挥关键作用，推动社会数字化发展。

参考文献

[1]刘梦轩.电子信息工程技术的应用和安全管理浅析[J].房地产世界,2020,(10):123-125.

[2]梁靖昕.电子信息工程技术应用中的问题与对策分析[J].中国战略新兴产业,2024,(11):60-62.

[3]王芳.智能技术在电子信息工程自动化设计中的应用分析[J].信息系统工程,2024,(06):58-60.

[4]王良敏.电子信息工程中的安全技术应用研究[J].大众标准化,2023,(13):171-173.