信息安全防护技术及其在网络安全中的作用分析

刘天亮

北京启天安信科技有限公司，北京市，100000；

摘要：互联网快速演进使网络攻击手段愈加多样，数据泄漏、勒索软件与供应链渗透事件频发。密码技术、访问控制与智能检测构成了现代信息安全防护体系的核心支柱。本文首先阐述信息安全防护技术的概念与重要性，梳理当前主要威胁形态；随后结合数字签名、端到端加密、网络防火墙与多因素身份认证等关键技术，探讨密码学在网络安全中的典型应用；继而评估纵深防御对抵御攻击的综合成效，并分析资源受限场景、零日漏洞和政策合规带来的局限；最后总结研究发现，展望后量子密码与零信任自动化融合的未来发展方向。

关键词：信息安全；密码技术；纵深防御；零信任；后量子密码

DOI：10.69979/3060-8767.25.08.073

引言

数字经济时代，数据已成为驱动社会与产业迭代的核心资源。然而，黑客入侵、勒索软件、供应链渗透与物联网漏洞等威胁持续升级，传统单层防线屡屡失守。密码技术凭借机密性、完整性与身份鉴别优势，被视为构建纵深防御的基石。为了厘清其理论脉络与实际成效，本文以信息安全防护技术为切入点，先阐述基本概念与威胁格局，再聚焦密码学在加密通信、网络边界与身份管理中的典型应用，最后评估其对抗攻击的成效与局限，为后续架构优化与政策制定提供参考。

1 信息安全防护技术的基本理论

1.1 信息安全防护技术的定义及重要性

信息安全防护技术是指通过密码学原语、访问控制、入侵检测与日志审计等手段，对数据在采集、传输、存储与销毁各阶段进行系统性保护，以确保保密性、完整性、可用性和可审计性。龚健虎指出，伴随政务、金融与能源系统全面上云，网络边界日益模糊，单点失守可能引发级联故障；因此在系统规划之初即融入安全基线、落地差异化防护策略，已成为数字化转型的前置条件。尤其在关键基础设施领域，一次安全事件可能带来巨额损失甚至公共安全危机，提升防护技术水平不仅是企业合规需求，更是国家层面的战略任务。

1.2 信息安全威胁的主要表现形式

当前威胁形态呈现隐蔽化与产业化双重特征。恶意代码已由文件型病毒演变为无文件化脚本和内存马，逃逸传统杀毒引擎；勒索软件采用双重勒索策略，通过加密与泄密叠加提高受害方支付概率；供应链攻击则在第三方组件与自动化构建环节植入后门，绕过外围防御直达核心业务；物联网设备因固件老旧和加密算法弱化，成为僵尸网络与横向渗透的跳板；鱼叉式钓鱼结合深度伪造技术精准诱导关键岗位人员，为攻击奠定入口。冯国聪研究显示，5G 和大规模物联网部署极大扩展了攻击面；刘正阳则指出，技术人员安全意识不足与系统漏洞并行，使攻击更具隐蔽性。面对持续演化的威胁，防护体系正从签名比对转向基于威胁情报与行为分析的主动防御，并预留后量子密码升级通道，以应对量子计算对现有公钥体系的潜在冲击。

2 密码技术在网络信息安全中的具体应用

2.1 数据加密技术

在网络空间，数据加密是保证信息不被窃听、篡改的首要屏障。对称加密与非对称加密常以“混合模式”协同：会话数据以 AES、SM4 等对称算法高速加密，密钥交换与身份验证则借助 RSA、ECC 及国密 SM2 等非对称算法完成，从而兼顾效率与安全。为避免传输途中出现篡改或冒名，数字摘要会先对原始数据进行哈希计算，再将结果与原文一并加密，确保接收端可以通过比对哈希值验证完整性。由于移动端与云端数据流动频繁，现代加密系统普遍采用“分级密钥”管理：顶层根密钥只负责派生，会话密钥一次一换，从而降低长周期密钥泄露带来的风险。

2.1.1 数字签名技术

数字签名利用私钥加密哈希值，公钥负责解密并比对，达到身份鉴别与不可抵赖目的。在电子商务场景，买卖双方通过 CA 颁发的证书完成密钥绑定，再在合同文本上叠加签名；一旦发生纠纷，任何一方都无法否认已签署内容。冯国聪等人指出，随着区块链技术兴起，签名还被用于保护分布式账本的一致性，当节点收到新区块时，只需校验签名即可判断合法性，省去了繁琐的链下对账流程。

2.1.2 端到端加密技术

端到端加密通过在通信源端和目的端各自完成加解密，使中间路由器、服务器即便被攻陷也无法解读密文。即时通讯应用 Signal 和 WhatsApp 均采用“双棘轮”算法，为每条消息派生一次性会话密钥，从而提供前向与后向保密。刘正阳研究表明，引入端到端加密后，云协作平台的敏感文件在传输与存储阶段均保持加密状态，即便管理员权限被盗取，攻击者仍难以获得明文。需要注意的是，该机制会给审计与合规留取证据带来挑战，企业通常采用“客端加密+服务器检索密钥快照”的折中策略，既满足监管，又兼顾隐私。

2.2 网络防火墙技术

传统防火墙依赖端口与协议特征进行过滤，难以处理日益增多的 TLS 加密流量。下一代防火墙则在零信任接入点实现被动解密，再结合深度包检测与威胁情报，识别 SQL 注入、跨站脚本和命令执行等高危行为。虞凤娟指出，将人工智能模型嵌入检测链后，可以基于语义特征发现未知攻击，拦截率较静态特征方法提升近二成。在大流量 DDoS 攻击场景，云清洗中心通过 BGP 牵引将可疑流量导入高带宽清洗池，利用速率限制与协议一致性校验在秒级内剥离垃圾报文，保证核心链路畅通。

2.3 身份认证技术

身份认证是防止非法访问和权限滥用的最后一道关口。多因素认证结合口令、动态令牌与生物特征，可以显著降低撞库与社工成功率。近年来，无密码登录框架 FIDO2 在主流浏览器中落地，用户凭借本地可信平台模块生成的私钥完成签名，服务器仅保存公钥，彻底消除了密码泄露风险。对于分布式环境，属性基加密将解密权限与用户属性绑定，数据持有者可灵活定义“部门+级别+时间”等复杂策略，符合条件者才能解密。零信任模型进一步将身份验证从登录前置到每一次请求，结合设备健康度与行为基线实时计算信任分，当分值低于阈值即触发动态二次认证或直接阻断，极大抑制了横向移动的可能性。

3 信息安全防护技术在网络安全中的作用与局限性

3.1 防护技术对网络攻击的防范作用

密码学主导的多层防御体系已在金融、电力与工业互联网场景经过验证并显示出显著成效。大型商业银行将硬件防火墙、Web 应用防火墙、入侵检测系统与自动化编排平台串联，在网络、系统与应用三层实现“实时监测—关联分析—闭环处置”流程。试运行一年，重大入侵的平均发现时间由两个多小时缩短至不足十五分钟，业务中断率下降近九成。电网调度中心在现有 TLS 隧道外叠加 Kyber 密钥交换与 Dilithium 数字签名，形成“经典算法+后量子算法”的双层密钥体系，实测链路完整性提升七个百分点，时延仅增加百分之十二，可满足对实时性的严格要求。工业控制网络引入零信任网关，所有南北向与东西向流量均需通过动态信任评估，微分段策略让未经授权的扫描流量直接在边界被阻断，平台监控数据显示横向渗透事件同比减少七十八百分点。面对 Tbps 级 DDoS 攻击，云清洗中心基于 BGP 牵引在三秒内完成流量切换，并利用 AI 引擎进行协议一致性校验和速率限制，使业务可用性维持在百分之九十九点九九。综上，纵深协同的密码与检测机制不仅压缩了攻击面，也显著提高了应对高强度敌对活动的韧性和恢复速度。

3.2 当前信息安全防护技术的局限性分析

尽管综合防护能力已显著增强，现阶段仍存在四方面瓶颈。第一，未知漏洞与对抗样本可精准逃避基于特征与统计的检测模型。机器学习引擎一旦训练集不平衡或被污染，漏报与误报率会骤升，高级持续性威胁仍可能在低噪声状态下潜伏数周才被发现。第二，资源受限的物联网终端无法承载复杂椭圆曲线或同态运算，厂商往往被迫采用弱加密或干脆明文传输，从而为攻击者提供踏板。第三，零信任落地需要对资产、身份和策略持续细化。老旧系统接口难以标准化，策略失配易导致合

法业务中断；同时动态评估带来的额外认证流量使边缘节点延迟抬升，对实时控制场景构成挑战。第四，合规与运营短板限制了技术效能。跨境数据流动需同时满足多地法规，日志留存、密钥托管与脱敏标准各异，集成与运维成本高昂。中小企业即便采购了先进安全产品，也因缺乏专业人才无法持续调优，形成“买而不用”的尴尬。未来需要在三个维度持续发力：一是引入可解释人工智能与威胁情报，共同提升未知攻击识别率；二是推动轻量级加密与后量子算法并行标准化，为低功耗设备提供安全与性能兼顾的方案；三是通过自动化策略编排平台与统一合规框架，降低零信任维护与跨域数据治理成本，最终弥补当前防护体系的空隙。

参考文献

[1]李宪伟,陈静.基于计算机网络技术的网络信息安全防护体系建设[J].长江信息通信,2025,38(04):144-146.

[2]钟巧燕.计算机网络信息安全及其防护对策研究[J].石河子科技,2024,(05):39-40.

[3]冯国聪,王健,付志博.5G 网络信息安全的威胁及防护技术探讨[J].工程技术研究,2023,8(01):226-228.

[4]刘正阳.大数据时代计算机网络信息安全及防护技术研究[J].中国新通信,2022,24(08):113-115.

[5]董洪蒙.计算机网络信息安全中的数据加密技术应用及防护策略[J].造纸装备及材料,2024,53(10):130-132.