计算机信息技术在互联网安全管理中的应用研究

常素丽
（河北政法职业学院，河北　石家庄　050000）

【摘　要】在当前的数字化时代，互联网已深度融入我们的社会生产与日常生活，成为不可或缺的一部分。网络科技的广泛应用极大地方便了人们的生活，然而，与此同时，网络安全问题也日益凸显，成为亟待解决的重要挑战。由于计算机网络本身的开放特性以及软硬件技术存在的某些不足，导致在实际应用中不可避免地潜藏着一些安全隐患。这些问题不仅对网络信息安全构成了严重威胁，而且也制约了互联网的持续发展。对此，本文就计算机信息技术在互联网安全管理中的应用进行探究，旨在通过具体的案例分析，探究计算机信息技术如何在互联网安全管理中发挥积极作用。

【关键词】计算机信息技术；互联网；安全管理；应用

前言

在信息化日益加速的今天，网络在人们的工作与生活中所扮演的角色愈发重要。为了确保网络安全，人们必须依赖电子信息技术来提供强大的技术支持。计算机信息技术的应用能够为计算机网络安全提供坚实的保障，有效解决网络使用过程中遇到的各种安全问题，进而显著提升网络系统的整体安全性。对此，需要结合当前的网络安全现状，积极探索如何利用计算机信息技术来制定有效的网络安全应对策略。通过这些研究，希望能够为提升互联网安全管理水平提供有益的参考与指导。

一、互联网安全管理中的主要问题

（一）网络系统漏洞

在数字化时代，计算机网络系统已成为我们日常生活和工作中不可或缺的一部分。然而，这些系统并非无懈可击，它们自带的漏洞为安全带来了不小的挑战。每当我们使用计算机进行办公、文档编辑或数据处理时，所依赖的软件系统都可能潜藏着安全风险。这些风险不仅源于软件本身的缺陷，还因为网络系统常常暴露在一个开放且多元的环境中。网络系统的这种开放性，虽然带来了便利，但同时也为不法分子提供了可乘之机。

他们可能会利用这些漏洞，尝试入侵他人的计算机系统，窃取数据，甚至破坏网络系统的正常运行。一旦成功，不仅可能导致个人信息的泄露，还可能造成整个系统的崩溃，给用户带来巨大损失。更为严重的是，当用户从非官方渠道下载并安装含有漏洞的软件时，这些漏洞可能会被放大，进而对信息安全构成更大的威胁。

（二）细致探讨信息安全隐患

随着大数据时代的推进，计算机网络中信息的产生和传输速度达到了前所未有的高度。这些信息的多样性、广泛性和海量化特点，使得信息安全问题愈发凸显。由于网络环境的开放性，一些掌握先进信息技术的不法分子开始蠢蠢欲动。他们利用技术手段，窃取用户的数据信息，使得信息在传输和存储过程中都面临着巨大的风险。

例如，近年来频发的电信诈骗案件，就是信息泄露导致的严重后果。诈骗分子通过盗取的个人信息，进行精准诈骗，导致许多无辜群众的资金被非法转移，银行卡、信用卡被盗刷，给受害者带来了巨大的经济损失和精神压力。此外，还有一些不法分子利用网络技术设置贷款陷阱，使许多人陷入困境。这些问题都尖锐地指出了当前计算机网络应用中的安全隐患，亟待我们寻求有效的解决方案。

（三）黑客攻击的威胁与应对

在计算机网络的使用过程中，黑客攻击是一个不容忽视的安全威胁。黑客利用高超的电脑技术，能够轻易入侵计算机系统，窃取或篡改重要信息。这种攻击对于拥有技术专利或敏感信息的公司和机构来说，尤为致命。黑客往往隐藏身份，悄无声息地进行网络入侵，给用户带来巨大损失。

面对黑客攻击，普通的计算机安全防护机制往往难以奏效。因此，需要采取更为先进和全面的安全措施，如加强网络监控、提升防火墙等级、定期更新安全补丁等，以应对这一严峻挑战。

（四）网络病毒的危害与防范

网络的开放性虽然带来了诸多便利，但也为网络病毒的传播提供了温床。一些恶意人士利用网络的这一特点，开发并传播病毒软件，窃取用户信息，破坏计算机系统。这些病毒不仅难以根除，还可能对计算机硬件造成长期损害。

为了防范网络病毒的侵害，需要提高警惕，不轻易点击不明链接或下载未知来源的软件。同时，定期使用专业的杀毒软件进行全盘扫描和清除病毒也是必不可少的措施。

二、计算机信息技术在互联网安全管理中的具体应用

（一）入侵检测与防御技术的深入应用

在计算机信息安全领域，入侵检测与防御技术扮演着举足轻重的角色。现今市场上已有众多入侵检测和防护应用，它们如同计算机系统的守门人，时刻警惕着任何异常进程的出现。这些程序能够敏锐地捕捉到计算机运行中的不寻常活动，并迅速发出警报，提醒用户及时应对。通过这种方式，它们有效地构筑起一道防线，对抗潜在的系统攻击，从而捍卫重要数据的安全。如下图 1 所示，为入侵检测防御系统架构：

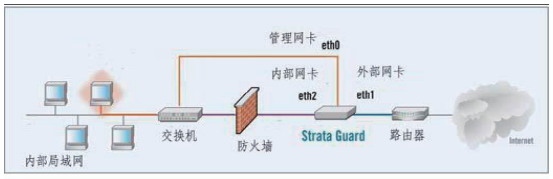

图 1　入侵检测防御系统架构

Strata Guard 还可以在标准模式下运行。在这种模式下，它主要作为 IDS 使用，专注于检测网络中的异常行为和潜在威胁。此外，它也可以与企业网络中已有的防火墙协同工作，通过联动机制实现 IPS 的功能。在这种配置下，Strata Guard 需要通过旁路方式接入目标网络，这样可以确保网络流量的全面监控而不会对主网络造成额外的负担。如，某大型企业网络为了保护其关键业务数据和客户信息，决定部署 Strata Guard 来增强其网络安全防护。在初期阶段，企业选择了标准模式，将 Strata Guard 作为 IDS 来使用，主要目的是监控网络中的异常流量和潜在攻击行为。随着安全需求的提升，企业决定进一步利用 Strata Guard 的功能。通过与现有防火墙的联动，Strata Guard 开始在检测到威胁时自动触发防火墙的防御机制，实现了 IPS 的功能。这种联动有效提高了威胁响应速度，还减少了潜在的安全风险。

入侵检测系统主要聚焦于监控网络流量，并分析其中可能存在的威胁。这种系统能够评估流经网络的数据，一旦发现可疑或恶意的活动迹象，便会立即触发警报系统。更为先进的是，一旦检测到恶意流量，入侵防御系统能够迅速作出反应，阻断相关请求或终止与恶意用户的会话连接，从而确保网络环境的安全稳定。

这些入侵检测与防御系统不仅功能强大，而且能够全天候运行，不间断地监控计算机的运行状态。它们能够实时提醒用户关于信息和流量的异常情况，为用户的网络应用提供坚实的安全保障。

（二）数据加密技术的多层次保护

数据加密技术是保护信息安全的重要手段。通过对信息、数据和相关文件进行加密处理，这一技术能够有效防止黑客的追踪和窃取行为，确保数据的整体安全。目前，DES 和 RAS 是两种广泛使用的数据加密方法。

首先是密钥加密算法，它通过复杂的置换和逆置换过程，将明文输入转换为加密输出，从而增加数据的保密性。这一过程包括将输入的 64 位数据块拆分为两个 32 位的数字块，并进行一系列的置换操作，最终生成加密后的数据。这种加密方法的复杂性使得黑客难以破解，从而极大增强了数据的安全性。如下图 2 所示，为基于区块链的数据加密技术系统：

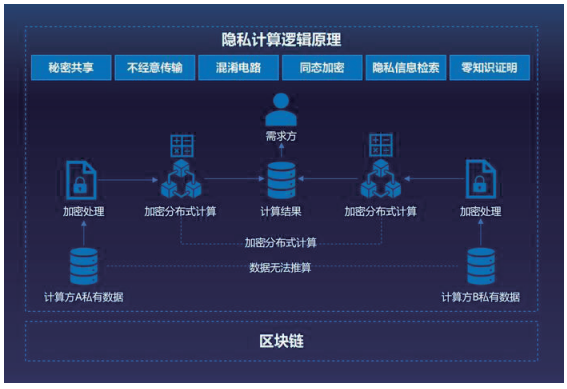

图 2　基于区块链的数据加密技术系统

零数科技倡议构建一个汽车大数据区块链交易平台，该平台将借助分布式的汽车数据共享交易网络，为数据提供者和需求者搭建起沟通的桥梁。为确保数据隐私和安全，平台还融合了先进的隐私计算技术，这种技术能够使得数据的所有权和使用权实现有效分离，仅通过输出计算结果来满足数据使用权的共享需求。

数据所有权与使用权的分离，其核心在于保障数据在不被直接查看的情况下仍能被有效利用。这意味着，其他方可以在不接触底层原始数据的前提下，利用这些数据得出所需的分析结果，实现了“数据可用但不可见”的理想状态。在此过程中，算法提供方无法窥视数据源，而数据源方也同样无法探知算法细节。双方将各自的算法和数据置于一个安全的“黑箱”环境中，共同进行模型训练。此外，在涉及跨境数据交互的场景中，隐私计算技术的重要性尤为突出。由于许多底层数据具有高度的敏感性，无法直接披露，因此需要通过隐私计算来确保数据的安全。这种技术不仅能够隐藏数据中的身份信息，还能对所有底层数据进行保护。在这种情况下，只有训练好的模型会被用于得出最终结果，从而确保了数据隐私的绝对安全。

此外，还有一种重要的加密方法是 RSA 公钥加密算法。它采用了公钥和私钥相结合的方式，使得加密和解密过程更加安全可靠。RSA 密钥的长度可根据需要进行调整，较长的密钥长度意味着更高的安全性。这种加密技术对于防范网络攻击和保护用户数据信息安全具有至关重要的作用。在大数据时代，数据加密技术还涵盖了端到端加密、对称加密和非对称加密

等多种方法。用户可以根据自身的实际需求选择合适的加密技术，以提升计算机网络的安全防护等级。

（三）电子取证技术在信息安全中的应用

随着大数据时代的到来，电子取证技术在计算机信息安全保护中发挥着越来越重要的作用。通过安装智能取证模块，用户可以监控每台主机的活动并对其进行深入分析。一旦检测到可疑信号或问题，系统会立即启动数据采集模块来收集相关数据。这些数据可以用于分析网络行为、获取关键信息以及进行广泛的取证工作。

电子取证技术不仅能够收集数据，还能对收集到的数据进行分类、加密签名并发送至专用服务器进行处理。服务器会对接收到的数据进行预处理并存储到数据库中，以便后续利用云计算技术进行分布式处理、检测和处理潜在的数据威胁源。这种技术的应用实现了对计算机网络的实时监控和动态信息捕捉，有助于及时发现风险因素并采取相应措施来确保网络安全。

（四）身份认证技术的强化与应用

在大数据时代背景下，黑客常常试图通过攻击漏洞来获取用户的账号和密码，进而窃取重要信息。因此，加强用户身份验证是保护数据信息安全的关键环节。为了实现这一目标，需要采取有效的身份认证技术来增加黑客盗取账号和密码的难度。

通过利用先进的身份认证技术，可以更加谨慎地验证用户身份，并确保只有合法用户才能访问敏感信息和执行关键操作。此外，借助虚拟技术来安全地存储用户的身份信息，并对网络身份盗用行为进行精准监测和识别，也是提升操作安全性的重要手段。系统还可以记录并存储用户的相关信息和操作历史，以便在必要时进行追溯和分析。这些措施共同构成了保护计算机信息安全的坚固防线。如，佛罗里达州的 First Citrus Bank 为个人、专业人士、高管和企业家提供一流的独立社区银行服务。First Citrus 力求改变现状，不再将密码作为员工在共享 Windows 工作站上系统登录的主要验证手段。考虑到密码重置的高昂成本和其对员工工作效率的负面影响，公司旨在消除密码输入的必要，同时确保用户身份验证的安全性。

该银行曾探索多种桌面身份验证方式，例如智能卡和基于时间的一次性密码（TOTP）。然而，这些方法不仅增加了员工登录的复杂性，降低了用户体验，而且并未提供充分的安全增强。更重要的是，这些方法仍然需要密码输入。

因此，First Citrus 开始考虑采用 FIDO 身份验证，这是一种标准化的强身份验证方法。其标准化带来的互操作性非常符合 First Citrus 广泛的安全策略需求。FIDO 标准利用设备上的公钥加密技术，提供了比密码和其他身份验证方式更强大的安全性。它保证用户凭据绝不会被共享，也绝不会离开用户设备。这些协议从设计之初就致力于保护用户隐私，不会提供可用于跨服务协作和追踪用户的信息，同时生物识别信息也始终保存在用户设备上。所有这些特性都与简洁的用户体验相结合，满足了在用户设备上使用本地生物识别技术的无密码需求。

总结：

计算机信息技术众多，在互联网安全管理中，根据现有的主要网络安全威胁因素，可以借助计算机信息技术为安全管理提供有效的技术支撑，减少和消除安全隐患，促进互联网安全管理提质增效。本文通过对计算机信息技术在互联网安全管理中的实际应用方面和方法，结合部分案例分析，指出相关技术对于提升互联网安全管理的效益，具有一定的参考价值。

参考文献：

[1] 章建忠 . 计算机信息技术在互联网安全管理中的应用 [J]. 信息与电脑（理论版），2024，36（03）：186-188.

[2] 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]. 科技资讯，2024，22（01）：30-33.

[3] 李欣 .“互联网 +”背景下计算机技术应用模式分析 [J]. 信息记录材料，2024，25（01）：136-138.

[4] 单薇 . 基于信息技术和互联网发展的计算机网络安全发展现状 [J]. 黑龙江科学，2023，14（17）：146-148.

[5] 王宇 . 计算机信息技术数据的安全漏洞及加密技术 [J]. 数字技术与应用，2023，41（09）：234-236.

[6] 王国平 . 计算机信息技术在互联网安全管理中的应用 [J]. 数字技术与应用，2023，41（04）：234-236.

[7] 刘威，李江丰 . 人工智能技术在互联网信息服务安全评估中的应用研究 [J]. 通信管理与技术，2023，（01）：46-47.

[8] 丁园园 . 人工智能在当代计算机信息技术中的应用研究 [J]. 信息记录材料，2023，24（01）：66-68.

[9] 桂月亮 . 数字经济背景下互联网企业爬虫技术专项合规制度建构——基于 82 篇刑事裁判文书的实证分析 [A] 人民法院服务中国特色社会主义法治体系建设与刑事法律适用问题研究——全国法院第 34 届学术讨论会获奖论文集（下）[C]. 最高人民法院，国家法官学院科研部，2022：16.

[10] 王国勇 . 计算机信息技术应用安全隐患与防护策略研究 [J]. 电脑知识与技术，2021，17（15）：65-66.

作者简介：

常素丽（1982.04—），女，汉族，河北石家庄人，硕士研究生，讲师，研究方向：计算机应用技术。