ISSN: 2661-3719(Print); 2661-3727(Online)

大数据时代计算机网络安全体系构建研究

王珉　司祯祯
中国电子科技集团公司第二十二研究所　河南省新乡市　453000

摘　要：大数据作为数字经济的核心驱动力，数据规模爆炸式增长、结构复杂度飙升，正使传统计算机网络安全架构面临前所未有的困境，亟需构建新型动态协同的网络安全体系，通过技术迭代与体系化防护应对数据洪流冲击，保障网络系统在大数据应用中的可靠安全运行。大数据的爆发式增长和传输效率的提升，为计算机网络安全带来了全新的问题。本文围绕在大数据背景下如何构建有效的网络安全架构，深度剖析网络安全的需求、难题以及核心科技，通过提出了一套综合性的安全策略，包括数据感知保护、即时反应机制、多元防护策略和智能安全解决方案，其目的就在于维护大数据环境下的网络系统安全稳定。对大数据方面的网络安全理论研究和工程实践具有较好指导意义。

关键词：大数据；信息安全；计算机网络安全；安全体系构建

引言

随着互联网技术的不断发展，大数据在各个行业的应用中也越来越广泛，大数据带来信息使用便捷的同时也埋下很多安全隐患，虽然大数据技术加快对数据信息 的处理和分析，但如没有足够安全的信息防护技术，很易出现数据的泄露，对用户隐私造成威胁。因此，要想进一步确保数据信息的准确性，制订切实有效的决策内容，在利用大数据对计算机网络信息的处理中，规范操作模式，确保操作手段的科学性。在当前大数据驱动的信息社会中，计算机网络安全体系的现状与大数据技术的飞速发展形成鲜明反差。网络安全技术的滞后性在大数据信息的广泛传播中日益显现，同时互联网安全保护工作中尚存诸多薄弱环节，这些缺陷反而加剧了网络信息的潜在风险。为了遏制进一步的数据泄露危机，提升计算机信息系统的防护能力，我们必须充分认识到在大数据时代背景下强化计算机网络安全配置的紧迫性和必要性。

1. 大数据时代计算机网络安全面临的挑战

1.1 数据量激增带来的存储和处理压力

在当前的信息洪流中，数据产量正以前所未有的速度急剧攀升。涵盖了从个人隐私到企业档案，再到政府文档的各类信息源源不断地涌现。为了挖掘这些海量数据中的潜在价值，有效管理和解析它们至关重要。然而，数据量的持续膨胀导致了存储和操作这些数据的硬件及软件资源需求同步增长，从而提升了企业的运营成本，并对网络安全保障提出了更为严苛的标准。传统的数据管理手段已无法适应这种变化，转而需要更为先进且稳定的数据存储解决方案。但这方面的投资和技术门槛对于部分中小型企业而言，无疑构成了严峻的考验。

大数据的处理则要求强大的计算实力以及优化的算法支持。尽管计算机处理性能已有显著提升，但面对大数据的挑战，仍显得力有未逮。同时，保证数据的即时性、精确性和可信度也是大数据处理环节不可忽视的部分，这些因素进一步加大了网络安全防护技术面临的压力。

1.2 多样化的网络攻击手段

步入信息爆炸的时代，网络犯罪手法也随之演变，呈现出前所未有的复杂性和多样性。罪犯巧妙地利用大数据技术的双重刃剑，编织出一套套精密的攻击策略。其中包括：

流量洪灾攻击（DoS 和 DDoS）：这是一种高明的战术，犯罪分子通过生成并投放海量无效数据，引发网络瓶颈，让目标服务器的资源被无情消耗，进而剥夺其正常服务的能力，使之无法顺畅地与外界沟通。

中间人拦截（MITM）：这种攻击方式如同隐形的窃听者，让攻击者得以在两个通信对象之间插入自己，从而可能窃取或篡改双方之间的私密信息。

钓鱼陷阱：犯罪者精心伪装成合法机构，以极具诱惑力的虚假邮件为饵，诱导受害者主动泄露关键信息，如账户密码或个人资料。

精准定向的网络钓鱼（如鲸鱼和鱼叉攻击）：这类攻击瞄准大型企业或特定个体，以其高度的定向性和欺骗性，

增加了防范的难度和影响的深度。

这些多样的网络攻击手法犹如暗夜中的阴影，对网络安全构成了严峻挑战。它们不仅可能窃取宝贵的数据，还可能导致系统瘫痪，对企业和个人的财产安全以及信任度造成不可估量的损害。

1.3 网络安全防护技术的滞后性

尽管计算机网络安全防御体系在当今已展现出显著的进步，但在迎接大数据挑战时，却暴露出了明显的滞后效应。首要的是，尽管防护技术在持续进化，但其与瞬息万变的网络生态和层出不穷的攻击策略之间的同步性问题日益凸显。技术革新步伐往往落后于攻击手法的迭代，形成了某种程度的技术滞后。其次，现有的防护措施在应对大数据特性上显得捉襟见肘，如数据的巨量、多样性和实时性要求。它们往往无法充分契合这些特性，从而在大数据的浪潮中遗留下潜在的安全缺口和风险。

1.4 网络安全管理制度的不完善

在大数据时代的计算机网络安全困境中，制度层面的问题同样关键。首要的，健全的网络安全管理体系应明确规定所有成员的角色和权限边界，以保障数据的绝对安全和完整性。然而，现实中的执行常常偏离理想，角色混淆和权限模糊的情况屡见不鲜，这无疑为数据保护设置了无形的隐患。其次，制度应当构建强大的危机应对框架，包括预先制定的应急预案，以迅速、有效地应对任何突发网络安全危机。遗憾的是，由于缺失这样的响应体系，我们往往在事件爆发后才手忙脚乱，使得损失进一步加剧。

2. 计算机网络安全体系构建的理论基础

2.1 计算机网络安全的基本概念

计算机网络环境的保障机制着重于多元化的保护策略，旨在维护网络系统及其包含的硬件、软件和宝贵信息免受各类潜在威胁。它关注的核心在于开放网络空间中，如何实现信息的严格保密、完整性不受侵犯以及服务的持续可用性，同时确保系统的稳定运行。这一领域的需求促使我们必须对网络保护进行全方位的深入洞察，涵盖从实体设备防护、系统架构防御、网络层面防护、应用程序安全到数据隐私维护等多个关键环节。

2.2 计算机网络安全体系构建的原则

构建计算机网络安全框架的核心理念在于全方位且高效地守护网络系统的完整性。这个框架需涵盖网络系统的各个维度，从基础的硬件设施到复杂的软件程序，再到数据存储和通信规程，务求无一遗漏地消除潜在的威胁。它提倡实施分层次的安全策略，包括物理防护、网络保护、系统防护和应用防护等多个层面，以满足多元化的安全需求和差异化的安全等级要求。网络安全框架应具备动态适应性，能随着网络环境变迁和新出现的安全挑战自我调整，始终保持对新兴安全需求的高度响应。在追求绝对安全的同时，它寻求在保障网络安全与维护网络效能之间找到微妙的平衡，防止过于严格的防护手段干扰到正常的网络服务运行。这种平衡策略旨在实现网络安全与使用效率的双赢。

2.3 计算机网络安全体系构建的关键技术

在构建数字化环境下的安全保障架构中，核心技术扮演着基石般的角色。首先，边界防护墙如同一道坚固的闸门，高效地划定了内部与外部网络的界限，严格拦截未经许可的访问和潜在的侵袭行为。与此同时，实时监控系统犹如敏锐的眼睛，持续扫描网络动态，迅速察觉并预警可能存在的安全隐患。其次，数据加密算法犹如无形的铠甲，确保信息在流转和存储备份阶段的绝对保密性和完整性，抵御数据泄露或篡改的风险。身份验证技术、详尽的日志审计策略以及严谨的安全通信协议，这些多元化的技术手段交织成一个强大的安全网，为数字系统的平稳运行提供了坚实的防护盾牌。

3. 大数据时代计算机网络安全体系构建策略

3.1 数据安全控制策略

数据保护在数字世界的基石中占据核心地位，它涵盖了数据的隐私性、完整性和功能性。在当今的大数据洪流中，海量数据的管理带来了前所未有的挑战，对数据安全的保障显得尤为关键。为抵禦潜在威胁，一套全面的数据安全管控策略必不可少。首先，通过先进的加密技术，如同态加密和异态加密，我们能在数据传输和存储过程中构筑一道坚不可摧的防护墙，阻止未经授权的获取或篡改。同时，严谨的密钥管理机制，包括密钥生成、存储、分配和使用流程的严密监督，确保了加密技术的有效运用。

大数据的价值不容忽视，任何数据丢失或损坏都可能造成无法弥补的经济损失。因此，建立高效的数据备份和恢复系统至关重要，定期备份重要信息，并确保备份数据的完整性和可恢复性，以降低潜在风险。对于数据的访问，严格的权限控制系统应运而生，只有获得授权的个体才能触及数据，确保信息的专属性。此外，实施数据使用追踪审计，实

时监控并记录数据操作行为，犹如一双无形的眼睛，能及时预警并解决任何潜在的数据安全隐患。总的来说，数据安全控制是一项系统的工程，需要全方位、多层次的防护措施共同构建起坚固的数据防护网。

3.2 网络安全防护策略

网络安全保障构成了计算机网络安全架构的关键环节，它直接影响到网络系统的稳定运行和信任度。在当前大数据背景下，网络攻击技术的持续演进增加了网络安全保障的复杂性和挑战性。因此，实施多元化的网络安全保障策略显得至关重要，以保证网络系统的安全性。防火墙作为一道屏障，隔绝内外网络，防止未授权的侵入和攻击。我们应建立健全的防火墙管理规则，定期审查和升级防火墙设置和策略，以保证其对抗网络攻击的有效性。入侵检测系统能实时监控网络活动，快速识别并通报可能的安全风险。我们需要构建一套完整的入侵检测流程，定期审核和更新检测系统的配置和响应策略，确保其能精确识别并应对网络攻击。此外，安全漏洞管理同样是不可忽视的一环。需确立完善的安全漏洞管理政策，定期扫描和修补系统内的漏洞，避免攻击者利用这些弱点发动攻击。同时，设立安全漏洞报告机制，激励用户即时上报发现的问题，便于我们及时解决，增强整体网络的安全韧性。

3.3 应用安全策略

计算机网络安全架构中，应用安全占据了至关重要的地位，其关乎着应用系统的可靠性和持久性。尤其是在大数据环境下，应用系统的错综复杂和异质性使得应用安全问题显得尤为棘手且艰巨。因此，实施全面的应用安全措施显得刻不容缓。需对应用系统的源代码进行详尽的审查和测试，以消除任何可能的安全薄弱环节和潜在威胁。应构建严谨的代码管理规则，对代码的改动和发布施加严密管控，避免出现未授权的改动和发布行为。确立牢固的身份验证和访问控制政策，通过验证用户身份并授予相应权限，保证只有合法用户能接入应用系统。同时，设立用户活动审计系统，对用户的操作和访问行为进行实时监控和记录，以便尽早察觉并应对可能出现的安全隐患。此外，安全漏洞的扫描和修补同样是应用安全的关键环节。需定期对应用系统进行全面的安全漏洞扫描，并迅速修补，以防攻击者利用这些漏洞发动攻击。最后，建立安全漏洞上报机制，激励用户一旦发现安全漏洞能立即上报，以便我们能及时采取修复行动。

3.4 安全管理策略

在计算机网络的保护伞下，安全管理扮演着至关重要的角色，它涵盖了政策、教育以及意识等多个层面。进入大数据时代，这一领域的价值更是不容忽视，我们需要制定一系列行之有效的安全管理策略以保证网络安全体系的高效运行。首要任务是建立健全的安全管理制度，清晰界定安全管理的职责与权力，以促进安全管理活动的有条不紊。此外，设立快速反应的应急预案，对任何安全威胁做出即时应对，避免对网络系统的正常运行产生干扰。

持续进行安全培训是不可或缺的一环，旨在提升员工对网络安全的理解和重视，促使他们自觉遵循安全规程和操作步骤。通过持续的宣传教育，进一步增强员工的网络安全意识，让他们始终保持警觉，有效预防潜在的网络风险。总结而言，在大数据环境下构建网络安全架构，需从数据管控、网络防御、应用安全以及全面管理等多个角度出发，实施多样化的策略和手段，以维护网络系统的安全与稳定。

5. 结语

综上所述，大数据时代的网络安全是贯穿数据全生命周期的持久保卫战。它要求我们在实践中融合科技手法和治理策略，持续强化安全防护体系，以维持网络生态的稳固与高效。如何应对不断涌现的网络安全风险，是确保数字经济稳健增长的必要前提。只有通过这样的系统性努力，我们方能从容面对未来的挑战，为数字时代的信息安全筑起坚固的堡垒。

参考文献：

[1] 周志强 . 大数据时代计算机网络安全维护与管理措施研究 [J]. 大众标准化 , 2023(12):161–163.

[2] 郑碧虹 . 浅谈大数据时代背景下的计算机网络安全防范策略 [J]. 网络安全和信息化 , 2023(4):124–127.

[3] 代丰 . 大数据时代医院计算机网络信息系统的安全试析 [J]. 移动信息 , 2023, 45(1):133–135.

[4] 陈文涛 . 大数据时代计算机网络安全技术的优化策略 [J]. 网络安全技术与应用 , 2023(11):157–158.

[5] 李华龙 , 陈力超 . 大数据时代的计算机网络信息安全问题及防范策略 [J]. 中文科技期刊数据库《工程技术》, 2023.

作者简介： 王珉 (1974 —), 男, 河南新乡, 高级工程师, 1997 年毕业于西安电子科技大学电子工程专业，现就职于中国电子科技集团公司第二十二研究所，从事电子信息工程方面研究工作。