网络安全与数据安全融合发展趋势研究

王鹏杰
中国电力科学研究院有限公司 北京 100192

摘　要：网络安全与数据安全作为信息时代的核心议题，其融合发展趋势已成为应对复杂安全挑战的必然选择。本文首先阐述了网络安全与数据安全的基本概念及现状，分析了二者融合的必要性和理论基础，探讨了融合的技术路径和实践案例。研究表明，融合不仅丰富信息安全理论体系，推动技术创新，还能提升企业和机构的安全防护能力。未来，融合将朝着技术融合、管理融合和政策融合方向发展，但需应对技术漏洞、管理协同难度、政策滞后及人才短缺等挑战。通过多方协同，构建科学的理论框架和高效的实践路径，将为构建更加安全可靠的信息环境提供有力支撑。

关键词：网络安全；数据安全；融合发展趋势；技术路径；管理融合

引言

网络安全与数据安全作为信息时代的核心议题，其基本概念和内涵具有显著的区别与联系。网络安全主要指网络系统的硬件、软件及其数据受到保护，不因偶然或恶意的原因而遭到破坏、更改或泄露，保障网络系统连续可靠地运行。数据安全则侧重于保护数据的完整性、可用性和保密性，防止数据在存储、传输和处理过程中被非法访问、篡改或泄露。当前，随着信息技术的迅猛发展，网络安全与数据安全的融合已成为必然趋势。

网络安全与数据安全融合的必要性体现在多个方面。首先，网络攻击手段日益复杂，单一的安全措施难以应对多样化的威胁，融合可以构建更为全面的安全防护体系。其次，数据作为网络系统的核心资产，其安全性直接关系到网络系统的稳定运行，融合有助于实现数据全生命周期的安全保护。此外，政策法规的不断完善也对网络安全与数据安全的融合提出了更高要求。

研究网络安全与数据安全融合的发展趋势具有重要意义。理论上，融合研究可以丰富信息安全理论体系，推动安全技术的创新与发展。实践上，融合应用能够提升企业和机构的安全防护能力，降低安全风险，保障信息系统的稳定运行。同时，融合研究还能为政策制定提供科学依据，推动信息安全法律法规的完善。通过深入探讨网络安全与数据安全的融合发展趋势，可以为构建更加安全可靠的信息环境提供有力支撑。

1 网络安全与数据安全的基本概念及现状

网络安全与数据安全作为信息时代的核心议题，其内涵和外延具有显著的区别与联系。网络安全主要指网络系统的硬件、软件及其数据受到保护，不因偶然或恶意的原因而遭到破坏、更改或泄露，保障网络系统连续可靠地运行。其外延涵盖网络架构的安全性、网络服务的稳定性以及网络传输的保密性。数据安全则侧重于保护数据的完整性、可用性和保密性，防止数据在存储、传输和处理过程中被非法访问、篡改或泄露。其外延包括数据加密、访问控制、数据备份与恢复等技术手段。

当前，网络安全与数据安全的发展现状呈现出多维度、多层次的特征。技术层面，防火墙、入侵检测系统、数据加密技术等不断升级，人工智能和大数据分析技术的引入显著提升了安全防护能力。政策层面，各国政府纷纷出台相关法律法规，如欧盟的《通用数据保护条例》（GDPR）、中国的《网络安全法》等，构建了较为完善的法律框架。市场层面，网络安全与数据安全市场需求持续增长，相关企业和产品层出不穷，形成了多元化的市场竞争格局。

然而，网络安全与数据安全的发展仍面临诸多挑战和问题。首先，技术漏洞和攻击手段的多样化使得安全防护难度加大，零日漏洞、高级持续性威胁（APT）等新型攻击手段层出不穷。其次，政策执行力度不足，部分法律法规在实际操作中难以落实，导致安全防护存在盲区。再者，市场资源配置不均，中小企业在安全投入上捉襟见肘，安全防护能力薄弱。此外，跨界数据流动带来的隐私保护问题、国际合

作不足等也是当前亟待解决的难题。

为更直观地展示网络安全与数据安全的关系，图 1（见下）通过 Mermaid 生成的流程图或关系图，揭示了二者在技术、政策和市场等方面的交织与互动。

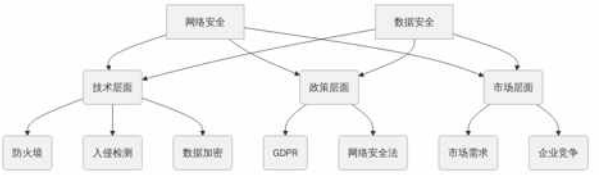

图 1 网络安全与数据安全在各个层面的紧密联

图 1 展示了网络安全与数据安全在各个层面的紧密联系，凸显了二者融合发展的必要性。通过技术、政策和市场的协同推进，有望构建更为坚实的网络安全与数据安全防护体系。

2 网络安全与数据安全融合的理论基础

网络安全与数据安全融合的理论依据可从系统论（强调整体关联）与信息论（关注信息安全传输处理）视角探讨，二者结合可构建兼顾网络整体稳定与数据全环节安全的综合框架。

具体理论模型包括层次化安全模型（如 OSI 架构，分层融合安全需求）和风险管理模型（如 NIST 框架，统一风险管控过程）。融合需遵循整体性（统筹协同）、动态性（随威胁更新策略）、均衡性（优化资源配置）、合规性（符合法规）原则。

理论意义在于形成全面安全防护体系，提升效能；实践价值体现为优化资源、提高管理效率、促进技术创新。实践中需技术（研发跨领域应用）、政策（完善法规）、市场（引导企业投入）协同，推动融合创新。

综上，融合是理论必然与实践需求，科学框架与原则可助力构建更安全的信息环境。

3 网络安全与数据安全融合的技术实践

当前，网络安全与数据安全的融合技术已成为保障信息安全的重要手段。主流的融合技术包括加密技术、访问控制、态势感知等，这些技术在不同的应用场景中展现出显著的效果。

加密技术作为基础性安全手段，广泛应用于数据传输和存储过程中。对称加密和非对称加密是两种主要的加密方式。对称加密算法如 AES（高级加密标准），具有加解密速度快、效率高的特点，适用于大规模数据加密。非对称加密算法如 RSA（Rivest–Shamir–Adleman），则通过公钥和私钥的分离，提供了更高的安全性，常用于数字签名和密钥交换。加密技术在金融、医疗等敏感数据保护领域发挥了重要作用，有效防止数据泄露和篡改。

访问控制技术通过限制用户对资源的访问权限，确保数据的安全性和完整性。基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）是两种常见的访问控制模型。RBAC 通过角色分配权限，简化了权限管理过程，适用于大型组织的管理。ABAC 则根据用户的属性动态分配权限，灵活性更高，适用于复杂多变的环境。访问控制在企业内部系统和云计算平台中得到广泛应用，有效防止未授权访问和数据滥用。

态势感知技术通过实时监测和分析网络环境中的安全态势，提供动态的安全防护。态势感知系统通常包括数据采集、态势理解和态势预测三个环节。数据采集环节通过传感器和网络设备收集各类安全数据；态势理解环节对数据进行综合分析，识别潜在威胁；态势预测环节则基于历史数据和当前态势，预测未来可能的安全风险。态势感知技术在网络安全监控和应急响应中发挥了关键作用，提升了系统的主动防御能力。

为了更清晰地对比这些技术的特点和应用效果，表 1 展示了网络安全与数据安全融合技术的对比情况。

表 1 网络安全与数据安全融合技术的对比情况

技术	特点	应用场景	效果
加密技术	对称加密速度快，非对称加密安全性高	数据传输、存储	防止数据泄露和篡改
访问控制	RBAC 简化管理，ABAC 灵活度高	企业内部系统、云计算平台	防止未授权访问和数据滥用
态势感知	实时监测、动态防护	网络安全监控、应急响应	提升主动防御能力

未来，随着技术的不断进步，网络安全与数据安全融合将涌现出更多新技术和新方法。量子加密技术有望突破传统加密算法的局限性，提供更为可靠的数据保护。基于人工智能的访问控制技术将通过机器学习算法，实现更精准的权限分配和动态调整。此外，区块链技术在数据溯源和防篡改方面的应用，也将为网络安全与数据安全的融合提供新的解

决方案。

综上所述，当前主流的网络安全与数据安全融合技术在保障信息安全方面发挥了重要作用，未来新技术的涌现将进一步推动融合的深度和广度。通过不断探索和实践，网络安全与数据安全的融合将构建更加坚实的信息安全防线。

4 网络安全与数据安全融合的应用案例分析

在金融领域，网络安全与数据安全融合成效显著。某大型商业银行综合运用加密技术（AES 与 RSA 结合）、基于角色的访问控制（RBAC）及态势感知技术，构建多层次防护体系，使安全事件发生率显著下降，客户数据安全得到有效保障。

医疗领域，某三甲医院通过高强度加密保护患者数据，应用基于属性的访问控制（ABAC）并引入态势感知技术，在保障患者隐私的同时，提升了医疗信息系统安全性与医疗服务可靠性。

政务领域，某市政府推进智慧城市建设时，采用数据分类分级加密、RBAC 与 ABAC 结合的访问控制及态势感知技术，有效提升了政务信息系统安全性，保障了政务数据的完整性和保密性。

这些案例虽各有侧重，但均通过融合网络与数据安全技术取得显著成效，为其他领域提供了借鉴。

5 网络安全与数据安全融合的发展趋势

网络安全与数据安全融合发展将体现在三方面：技术融合上，人工智能、区块链等技术深化应用，提升防护智能化与数据安全性；管理融合中，企业构建统一安全管理平台，优化资源配置与协同效率；政策融合则推动法律法规完善，促进标准化。

融合面临技术漏洞、跨部门协同难、法规滞后及人才短缺等挑战，但也带来防护能力提升、企业竞争力增强及安全产业发展的机遇。

应对需企业加大研发、优化管理平台，政府加快法规制定、统一标准并加强人才培养，多方协同推进融合。

6 结论

网络安全与数据安全融合不仅是应对当前复杂安全挑战的必然选择，更是信息安全领域发展的关键趋势。融合的必要性在于单一安全措施难以应对多样化威胁，数据作为核心资产其安全性直接影响网络系统的稳定运行，且政策法规的不断完善也提出了更高要求。理论上，融合研究丰富信息安全理论体系，推动技术创新；实践上，提升安全防护能力，降低风险，保障信息系统稳定运行，并为政策制定提供科学依据。未来，融合将朝着技术融合、管理融合和政策融合方向发展，但也面临技术漏洞、管理协同难度、政策滞后及人才短缺等挑战。为此，企业需加大技术研发投入，优化管理流程，政府应加快法律法规制定，推动标准化建设，加强人才培养，以构建更加安全可靠的信息环境。

参考文献：

[1] 李小华 . 混合加密算法在计算机网络数据传输安全技术中的应用 [J]. 百科知识 ,2025,(18):14-16.

[2] 张晓鲁 . 大数据环境下网络信息安全漏洞检测技术研究 [J]. 信息与电脑 ,2025,37(12):72-74.

[3] 彭海信 . 基于网络大数据分析的校园安全风险智能预测与防范策略研究 [J]. 中国宽带 ,2025,21(07):49-51.

[4] 何贞昱 , 黄安 .5G 网络数据治理安全风险评估与动态防控构建 [J]. 中国宽带 ,2025,21(07):28-30.

[5] 范宇 , 郭豪伟 . 基于数据挖掘的网络安全监测方法研究 [J]. 中国宽带 ,2025,21(07):58-60.

作者简介：王鹏杰（1993—），男，汉，山西朔州，中国电力科学研究院有限公司，大学专科，无，网络安全。