基于人工智能的网络通信信息数据安全加密技术研究

李佳鹏

摘　要：随着网络技术的飞速发展，网络通信信息数据的安全问题日益凸显。人工智能（AI）技术以其强大的数据处理和智能分析能力，在网络通信信息数据安全加密领域展现出巨大潜力。本研究探讨了人工智能在网络通信信息数据安全加密中的应用，包括智能密钥管理、智能数据加密算法、数据隐私保护以及网络安全监测与防御等方面，并分析了面临的挑战与对策。

关键词：人工智能；网络通信；数据安全；加密技术；智能密钥管理

引言

在数字化时代，网络通信已成为人们日常生活和工作中不可或缺的一部分。然而，随着网络攻击手段的不断升级，网络通信信息数据的安全面临着前所未有的挑战。传统的加密技术虽然在一定程度上保障了数据的安全，但难以应对日益复杂的网络威胁。因此，研究基于人工智能的网络通信信息数据安全加密技术具有重要意义。

一、网络通信信息数据安全概述

1.网络通信的基本概念

网络通信是借助计算机网络实现信息高效传输与交换的复杂过程，它融合了多种技术与协议，构建起跨越地域界限的沟通桥梁。在这一过程中，数据以电信号、光信号或无线信号等形式，通过物理介质或空间传播，从发送端准确无误地传递至接收端。网络协议作为通信的“语言”，确保了不同设备间能够相互理解、协同工作，无论是TCP/IP协议簇的广泛应用，还是5G、物联网等新兴技术的兴起，都不断推动着网络通信的边界拓展与性能提升。此外，网络通信还涉及路由选择、流量控制、错误检测与纠正等多个关键环节，它们共同作用于数据传输的每一个环节，保障着信息的完整性、可用性与安全性，使得全球范围内的即时通讯、资源共享、在线服务等成为可能。（见图1）

2.数据安全的重要性

数据安全是网络通信的基石，关乎个人隐私、企业生存乃至国家安全。在数字化时代，数据已成为驱动社会运转的关键要素，从个人身份信息到企业商业机密，再到国家敏感数据，无一不牵动着各方神经。一旦数据泄露，不仅可能导致个人隐私曝光，引发诈骗、骚扰等风险，还可能使企业遭受重大经济损失，甚至影响国家主权、安全和发展利益。数据安全的重要性还体现在其对经济秩序和社会稳定的维护上，数据泄露事件可能引发公众恐慌，破坏市场信任，阻碍数字经济健康发展。因此，加强数据安全保护，不仅是技术层面的需求，更是法律、伦理和社会责任的体现，必须采取综合措施，确保数据在采集、存储、传输、使用等各环节的安全可控，为数字化时代的可持续发展筑牢屏障。

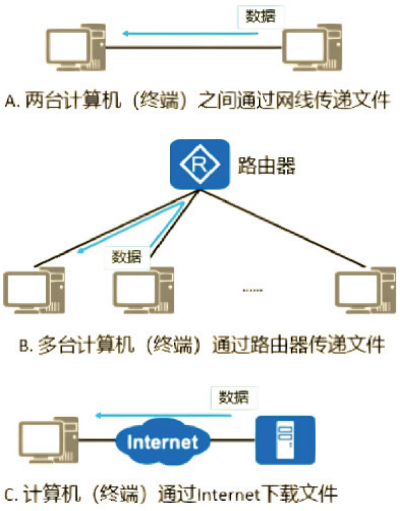

图1　网络通信的基本概念

3.传统加密技术的分类与特点

传统加密技术主要分为对称加密和非对称加密两大类，各具独特特点。对称加密采用单一密钥进行加密和解密，速度快、效率高，适合处理大量数据，但密钥管理复杂，一旦泄露将危及数据安全。非对称加密则使用

作者简介：李佳鹏（1994.03——）男，汉族，硕士研究生，中级工程师，主要从事通信工程项目方面的工作。

公钥和私钥对，公钥公开用于加密，私钥保密用于解密，安全性更高，尤其适用于数字签名和身份认证，但加密解密速度相对较慢。两类技术各有优劣，共同构成了传统加密技术的基石。

二、人工智能在网络通信信息数据安全加密中的应用

1.智能密钥管理

智能密钥管理作为人工智能在网络通信信息数据安全加密中的关键应用，正逐步重塑传统密钥管理体系。通过深度融合机器学习算法与密钥生命周期管理，系统能够动态感知网络环境变化，智能预测密钥使用模式，实现密钥的自动化生成、分发与轮换。这一过程不仅显著降低了人为干预带来的安全风险，还通过精准控制密钥暴露面，有效抵御了量子计算等新兴技术对传统加密体系的潜在威胁。深度学习模型在密钥材料处理中展现出独特优势，其非线性映射能力可构建复杂且难以逆向的密钥空间结构，使得密钥破解难度呈指数级增长。同时，强化学习机制的引入进一步优化了密钥策略决策过程，系统能够在实时攻防对抗中自主调整密钥强度与分布策略，确保加密通信的灵活性与安全性达到动态平衡。这种智能化密钥管理模式还促进了跨域密钥协同，通过联邦学习等技术实现多机构间密钥信息的隐私保护共享，为构建去中心化、抗攻击的网络通信安全架构提供了创新思路，标志着数据加密技术向更高级别的自适应、自防御阶段迈进。

2.智能数据加密算法

智能数据加密算法在人工智能的赋能下，正突破传统加密技术的边界，构建起更为坚韧的数据安全屏障。通过神经网络与加密逻辑的深度融合，算法能够自主学习数据特征，动态调整加密参数，使加密过程不再拘泥于固定模式，而是根据数据内容、传输环境及潜在威胁实时演化，形成千变万化的加密策略。这种自适应加密机制不仅极大提升了加密强度，还巧妙规避了单一算法易被针对性破解的风险。深度学习模型的引入，更是让加密算法具备了预测攻击模式的能力，能够在加密过程中预设防御陷阱，使攻击者在破解时陷入层层迷局。同时，智能数据加密算法还注重效率与安全的平衡，通过优化计算路径与资源分配，在保障加密效果的前提下，显著降低了加密解密的计算开销，使得高强度加密不再以牺牲系统性能为代价。这种智能化的加密变革，不仅为网络通信数据提供了前所未有的安全保障，更为数据加密技术的发展开辟了新的路径，预示着未来数据安全领域将迈向更加智能、灵活与高效的全新阶段。

3.数据隐私保护

数据隐私保护在人工智能的浪潮中迎来了革新，通过差分隐私、联邦学习等前沿技术，为敏感数据构筑起坚不可摧的防护网。差分隐私技术通过精心调控噪声参数，如拉普拉斯噪声的尺度，确保在数据发布或共享时，单个数据点的信息被有效隐藏于统计噪声之中，即便攻击者获取了数据集，也难以推断出具体个体的敏感信息，从而在数据可用性与隐私保护间找到了精妙平衡。联邦学习则打破了数据孤岛，允许多个参与方在不共享原始数据的前提下，通过交换模型参数或梯度更新，共同训练出精准的预测模型，这一过程中，数据始终保留在本地，仅有模型知识在参与方间流动，极大地降低了数据泄露风险。这些技术不仅遵循了严格的数据最小化原则，还通过动态调整隐私预算、加密强度等参数，适应不同场景下的隐私保护需求，使得数据在流动中既能发挥最大价值，又能确保个人隐私不被侵犯，为构建安全可信的数字生态奠定了坚实基础。

4.网络安全监测与防御

网络安全监测与防御在人工智能的加持下，已演变为一场智能与威胁的实时博弈。深度学习模型如同敏锐的猎手，潜伏于海量网络流量之中，通过不断分析数据包的特征、频率及异常模式，精准识别出隐藏在正常通信下的恶意攻击，如DDoS攻击的流量峰值、恶意软件的隐蔽通信等。这些模型不仅具备自我学习能力，还能根据新出现的威胁特征动态调整检测策略，确保防御机制始终领先一步。同时，强化学习技术被引入安全决策系统，模拟攻防对抗场景，让防御系统在不断试错中优化响应策略，自动选择最优的阻断、隔离或反击措施，实现从被动防御到主动出击的转变。自然语言处理技术的融入，则让安全日志分析更加高效，系统能够自动解析日志中的安全事件，提取关键信息，辅助安全专家快速定位问题根源。在这场没有硝烟的战争中，人工智能驱动的网络安全监测与防御体系，正以前所未有的智能与速度，守护着数字世界的安宁，构建起坚不可摧的安全屏障。

三、基于人工智能的数据加密技术面临的挑战与对策

1.面临的挑战

人工智能在网络通信信息数据安全加密领域的应用

虽展现出巨大潜力，却也不得不直面多重复杂挑战。算法复杂度与计算资源消耗成为首要难题，深度学习模型动辄涉及海量参数与复杂计算，导致加密解密过程耗时久、能耗高，难以在资源受限的设备上高效运行，严重制约了其实际应用范围。数据隐私与合规性风险如影随形，在利用敏感数据进行模型训练时，稍有不慎便可能触犯数据保护法规，引发法律纠纷与信任危机，如何在保障数据可用性的同时确保隐私不被泄露，成为亟待解决的关键问题。对抗性攻击的威胁更是日益严峻，攻击者通过精心设计的扰动数据或模型投毒等手段，试图绕过智能加密系统的检测，破坏其安全性与稳定性，这对加密算法的鲁棒性提出了极高要求。此外，人工智能技术的快速迭代与加密标准的相对滞后性之间的矛盾逐渐凸显，如何确保新技术在符合现有安全框架的前提下实现创新突破，成为推动该领域持续发展的又一重要课题。

2.对策与建议

面对人工智能在网络通信信息数据安全加密中遭遇的挑战，需构建多层次、多维度的应对策略。针对算法复杂度与计算资源瓶颈，应着力研发轻量化模型架构与高效算法优化技术，通过模型剪枝、量化及知识蒸馏等手段，在保持加密效能的同时显著降低计算开销，使智能加密技术能够灵活部署于各类资源受限场景。为化解数据隐私与合规性风险，需建立严格的数据治理体系，采用差分隐私、同态加密等先进技术，确保数据在训练与使用过程中全程匿名化、去标识化，同时加强法律法规的遵循与监管，构建数据全生命周期的安全防护网。对于对抗性攻击，应强化加密算法的鲁棒性设计，引入对抗训练机制，提升模型对恶意扰动的识别与抵御能力，并构建实时监测与应急响应系统，实现对潜在威胁的快速捕捉与有效应对。此外，还需推动加密标准的动态更新与技术创新同步，鼓励产学研用深度融合，加速新技术在合规框架内的转化应用，为网络通信信息数据安全加密的可持续发展奠定坚实基础。

结论

人工智能在网络通信信息数据安全加密领域的深度应用，正引领着数据安全防护的革新与突破。通过智能密钥管理、加密算法优化、隐私保护强化及安全监测防御等多元手段，不仅显著提升了数据加密的效能与灵活性，更为构建坚不可摧的网络安全屏障提供了有力支撑。尽管面临算法复杂度、隐私合规、对抗攻击等重重挑战，但通过轻量化模型设计、严格数据治理、鲁棒性增强及标准动态更新等策略，我们能够有效化解风险，推动技术持续演进。展望未来，随着人工智能技术的不断成熟与创新，其在数据安全加密领域的应用将更加广泛而深入，为数字经济的蓬勃发展保驾护航，助力构建一个更加安全、可信、智能的网络空间新生态，让信息在流动中绽放价值，而安全则成为这一进程的永恒基石。

参考文献

[1]王杰.基于人工智能的高校体育俱乐部会员信息安全加密算法[J].赤峰学院学报（自然科学版），2024，40（10）：11-16.

[2]冯文果.基于人工智能的光通信网络加密方式设计研究[J].通信电源技术，2023，40（8）：172-174.

[3]张海涛.智能网联汽车网络安全关键技术研究与应用[D].电子科技大学，2023.

[4]韩艳.基于数据加密技术的计算机网络通信安全防御研究[J].信息与电脑，2022（011）：034.

[5]孙强，尹琴，李宁，等.人工智能技术与网络信息安全分析[J].集成电路应用，2023，40（6）：351-353.