基于人工智能的移动互联网信息加密技术与网络安全技术

缪心飞　赵小叶
中国电信股份有限公司温州分公司

【摘　要】本文聚焦基于人工智能的移动互联网信息加密与网络安全技术，阐述了移动互联网、传统信息加密及人工智能相关理论与技术基础，指出传统技术在应对移动互联网安全挑战时存在局限。并深入探讨了人工智能在信息加密技术中的应用，包括加密算法设计、密钥管理和加密协议优化；同时分析其在网络安全技术方面的作用，涵盖网络入侵检测、恶意软件检测与防范、网络安全态势感知以及身份认证与访问控制。旨在为提升移动互联网信息安全提供理论支持与技术参考。

【关键词】人工智能；移动互联网；信息加密技术；网络安全技术

AI-Driven Mobile Internet Information Encryption and Cybersecurity Technology By

Miao Xinfeng　Zhao Xiaoye
China Telecom Corporation Limited Wenzhou Branch

【Abstract】This paper explores AI-powered encryption and cybersecurity solutions for mobile internet，examining the theoretical foundations of mobile internet，traditional encryption，and AI applications. It identifies limitations of conventional technologies in addressing mobile internet security challenges. The study further investigates AI's role in encryption technology，including algorithm design，key management，and protocol optimization，while analyzing its contributions to cybersecurity through intrusion detection，malware prevention，situational awareness，and authentication/access control. The research provides theoretical support and technical references for enhancing mobile internet information security.

【Key words】artificial intelligence；mobile internet；information encryption technology；network security technology

引言：

移动互联网的普及让信息交互愈发便捷，但开放性与移动性也使其面临诸多安全威胁，如数据泄露、网络攻击等。传统信息加密与网络安全技术在应对复杂多变的网络环境时，逐渐暴露出检测能力不足、适应性差等问题。人工智能凭借强大的数据分析、学习和预测能力，为解决这些问题带来了新的契机。深入研究基于人工智能的移动互联网信息加密技术与网络安全技术，对于保障用户信息安全、维护网络空间稳定具有重要意义。

1 移动互联网、传统信息加密及人工智能相关理论与技术基础

1.1 移动互联网技术概述

移动互联网作为移动通信技术与互联网技术深度交融的结晶，凭借移动终端这一灵活载体，为用户构建起信息快速获取与交互的便捷通道。其架构主要由移动终端、移动网络和移动应用三部分组成。移动终端包含智能手机、平板电脑等，硬件配置丰富多样，可满足不同用户的性能需求；操作系统方面，iOS 以流畅简洁著称，为用户带来顺滑体验，安卓则以开放多元见长，拥有海量个性化定制选项，它们都提供了拍照、视频播放、文件管理等丰富功能接口。移动网络发展迅猛，从 2G 时代到如今 5G 时代，传输速率实现指数级增长，网络覆盖范围也从城市逐步拓展至偏远乡村。此外，Wi-Fi 等无线接入技术凭借安装便捷、使用灵活的优势，在家庭、办公场所等场景广泛普及；移动应用领域极为广泛，社交应用打破时空限制，让人们随时随地畅快沟通；娱乐应用带来沉浸式视听盛宴，丰富人们的精神生活；办公应用则助力提升工作效率，实现便捷的移动办公。不过，移动互联网的开放性与移动性也带来诸多安全隐患，数据泄露易致个人隐私暴露，网络攻击可能造成系统瘫痪，因此，保障移动互联网的信息安全已成为亟待解决的重要问题。

1.2 传统信息加密技术与网络安全技术

传统信息加密技术主要分为对称加密算法和非对称加密算法。对称加密算法中，DES 和 AES 是典型代表，它们采用相同的密钥进行加密与解密操作。这种方式的加密效率颇高，能够在短时间内完成大量数据的加密处理。但由于加

密和解密使用同一密钥，密钥的管理难度较大，一旦密钥泄露，数据的安全性将受到严重威胁。非对称加密算法以 RSA 为例，它采用公钥和私钥配对的方式，公钥可公开分发，私钥则由用户妥善保管，有效解决了密钥分发问题。不过，其计算复杂度较高，在处理大规模数据时可能会影响系统性能。在网络安全技术方面，防火墙如同网络的第一道防线，通过设定访问规则过滤网络流量，阻止非法访问，保护内部网络的安全。入侵检测系统（IDS）则像敏锐的“哨兵”，实时监测网络和系统活动，识别潜在入侵行为。虚拟专用网络（VPN）利用加密和隧道技术在公共网络上建立安全通道，确保数据在传输过程中的保密性和完整性。然而，传统技术在应对复杂多变的网络攻击时，存在对未知攻击检测能力不足、难以适应移动互联网动态环境等局限性[1]。

1.3 人工智能基础理论

人工智能是一门致力于使计算机模拟人类智能的学科，自诞生以来经历了多个发展阶段。其主要分支包括机器学习、深度学习和自然语言处理等。机器学习是人工智能的核心领域之一，它通过特定的算法从海量数据中学习模式和规律，进而实现分类、预测等任务。例如，在垃圾邮件识别中，机器学习算法可以分析邮件的文本内容、发送频率等特征，准确判断是否为垃圾邮件。深度学习基于神经网络架构，能够自动提取数据的复杂特征。在图像识别领域，深度学习模型可以对图像中的物体进行精准分类和识别，在语音识别方面，也能将语音准确转化为文字。自然语言处理则聚焦于实现计算机对人类语言的理解和处理，涵盖机器翻译、情感分析等多个方面。机器翻译可以打破语言障碍，实现不同语言之间的实时翻译；情感分析则能通过分析文本中的词汇、语气等，判断作者的情感倾向。在信息安全领域，人工智能技术凭借其强大的数据分析能力，可通过分析大量数据，发现潜在的安全威胁，为信息加密和网络安全防护提供有力支持。

2 基于人工智能的移动互联网信息加密技术

2.1 人工智能在加密算法设计中的应用

在传统加密算法设计里，往往依赖预先设定的规则与固定参数，难以灵活适应复杂多变的数据特性与安全需求。而人工智能的融入，为加密算法设计开辟了全新路径。机器学习算法具备强大的数据分析能力，它能够对海量数据的特征和分布进行自动剖析。通过对不同类型数据的深入学习，机器学习算法可以精准地优化加密参数，使加密算法能依据数据特点进行自适应调整。以神经网络设计加密模型为例，它就像一个智能的“加密工匠”，能根据数据类型（如文本、图像、音频等）以及具体的安全需求（如保密级别、传输环境等），动态地制定加密策略。深度学习算法更是厉害，它能挖掘数据中隐藏的潜在模式，利用这些模式生成更为复杂、难以破解的加密密钥。相较于传统加密算法，基于人工智能的加密算法如同拥有“智慧大脑”，能敏锐感知安全威胁的变化，及时调整加密方式，大大提高了信息加密的效率和可靠性，为数据安全筑牢坚实防线[2]。

2.2 人工智能辅助的密钥管理技术

密钥管理在信息加密中占据着核心地位，关乎着整个加密体系的安全。人工智能在密钥管理的各个环节都发挥着不可替代的作用。在密钥生成阶段，深度学习算法犹如一位高明的“密码制造师”，它能够生成高度随机且安全的密钥。这种密钥的随机性极强，极大地提高了密钥的抗攻击能力，让攻击者难以通过规律猜测等方式获取密钥。在密钥分发过程中，人工智能就像一位精明的“交通指挥官”，它会根据实时变化的网络环境和用户的个性化需求，动态地选择最优的密钥分发路径。这样可以确保密钥在传输过程中避开潜在的安全风险，安全、准确地到达目标用户手中。同时，人工智能还能实现密钥的智能存储和管理，它会持续分析密钥的使用情况和安全状态，一旦发现密钥存在泄露风险或已过期，就会及时更新或撤销密钥。此外，它还能敏锐检测密钥的异常使用行为，提前发现潜在的安全风险，为密钥安全保驾护航。

2.3 人工智能驱动的加密协议优化

加密协议是保障信息在网络中安全传输的关键保障。然而，传统的加密协议往往是静态的，难以适应不断变化的网络环境和安全威胁。人工智能的出现为加密协议的优化带来了新的契机。强化学习算法就像一位聪明的“策略调整师”，它能够让加密协议根据网络环境和安全威胁的动态变化，自动调整协议参数。例如，当遭遇不同类型的网络攻击时，加密协议可以迅速做出反应，动态调整加密算法和密钥长度。如果遇到高强度的暴力破解攻击，协议会自动选用更复杂的加密算法和更长的密钥，以提供更强的安全防护。而且，人工智能还能对加密协议进行全面的性能评估和优化。它会分析协议在运行过程中的计算开销和通信延迟，通过不断调整和改进，减少不必要的资源消耗，提高信息传输的效率，使加密协议在保障安全的同时，也能实现高效的信息传输。

3 基于人工智能的移动互联网网络安全技术

3.1 人工智能在网络入侵检测中的应用

网络入侵检测是维护移动互联网网络安全的关键防线。传统入侵检测系统在面对复杂多变的网络攻击时，暴露出检测准确率低、误报率高的弊端。而人工智能技术，尤其是机器学习和深度学习算法，为该领域带来了革新。以大量网络

流量数据和系统日志为“教材”，人工智能模型展开深度学习，精准掌握正常网络行为模式。一旦出现偏离正常模式的行为，即可判定为异常入侵。卷积神经网络（CNN）便是其中的佼佼者，它能对网络流量进行细致的特征提取与分类。面对 DDoS 攻击时，CNN 可快速识别出异常的流量模式，准确判断攻击类型；对于端口扫描，也能精准捕捉异常的端口访问行为[3]。不仅如此，人工智能具备实时监测和预警能力，如同一位时刻警惕的“网络卫士”，能及时发现网络入侵事件，并迅速发出警报，为安全人员争取应对时间，有效降低网络攻击带来的损失，全方位保障移动互联网网络的安全稳定运行。

3.2 人工智能在恶意软件检测与防范中的应用

恶意软件犹如隐藏在网络中的“定时炸弹”，是网络安全的主要威胁。传统基于特征码匹配的检测方法，在应对不断变形和加密的恶意软件时，显得力不从心。人工智能技术则凭借强大的分析和学习能力，为恶意软件检测与防范开辟新路径。深度学习算法如同一位“代码侦探”，能深入分析恶意软件的行为特征和代码结构。即便恶意软件经过精心伪装和加密，也能从其行为模式中找出破绽，实现准确分类和识别。同时，人工智能可实时监测系统运行状态，如同一个“智能监控器”，一旦发现恶意软件试图安装或运行，立即发出警报并阻止其行动。这种实时、精准的检测与防范机制，能有效保护系统免受恶意软件的侵害，确保移动互联网环境的纯净与安全，为用户的信息和隐私提供可靠保障。

3.3 人工智能辅助的网络安全态势感知

网络安全态势感知是对网络安全状况的全面“体检”和精准评估。在移动互联网复杂的环境下，人工智能技术发挥着关键作用。它如同一个“数据整合大师”，能够整合来自网络流量、系统日志、安全事件等多个来源的安全数据。通过数据分析和挖掘，实时感知网络安全态势。机器学习算法则像一位“预测专家”，基于历史安全数据，预测网络安全事件的发生概率和发展趋势。例如，通过分析过往数据，能识别出网络安全的高风险时段和区域，提前部署防范措施。此外，人工智能还可实现安全态势的可视化展示，将复杂的网络安全状况以直观的图表和图像呈现出来，让安全管理人员一目了然，如同拥有了一双“透视眼”，能清晰了解网络安全状况，从而做出科学合理的决策，有效提升网络安全防护水平[4]。

3.4 人工智能在身份认证与访问控制中的应用

身份认证和访问控制是保障移动互联网网络安全至关重要的“大门”，直接决定着网络资源的安全访问。传统基于密码和令牌的身份认证方法，虽然在一定程度上能起到安全防护作用，但存在诸多安全隐患。密码可能因用户疏忽而被泄露，令牌也可能因丢失或被盗用而导致安全风险，给不法分子可乘之机。人工智能技术的引入，为身份认证和访问控制带来了全新的变革。生物特征识别技术宛如给这道“大门”加上了一把独特的“生物锁”，其中人脸识别、指纹识别等应用广泛。每个人的生物特征都是独一无二的，具有极高的唯一性和稳定性，能够准确验证用户身份，大大提高了身份认证的安全性。例如，在金融交易场景中，通过人脸识别可以确保是用户本人进行操作，有效防止他人冒用身份进行非法交易；行为特征识别则通过分析用户的键盘敲击模式、鼠标移动轨迹、操作习惯等行为特征，实现动态的访问控制。它就像一位“智能守门人”，根据用户的身份和行为实时调整访问权限。同时，人工智能具备强大的检测能力，能够敏锐地发现身份冒用和异常访问行为。一旦检测到可疑情况，如异常的登录地点、频繁的错误尝试等，系统会立即发出警报并阻止访问，有效防止安全威胁的侵入，为移动互联网网络安全构建起一道坚不可摧的防线。

结束语

随着移动互联网的持续发展，信息安全问题愈发关键。人工智能在信息加密与网络安全领域的应用，为解决传统技术难题提供了有效途径。通过在加密算法设计、密钥管理、入侵检测等多方面的创新应用，显著提升了信息加密的效率和可靠性，增强了网络安全的防护能力。未来，应进一步深化人工智能技术在信息安全领域的研究与应用，不断完善相关技术体系，以更好地应对日益复杂的网络安全挑战，为移动互联网的健康发展保驾护航。

参考文献

[1]刘冬晖，谢佳睿.基于人工智能的移动互联网信息加密技术与网络安全技术[J].信息记录材料，2025，26（8）：166–168.
[2]钟再淳.基于人工智能的网络入侵检测与防御技术[J].网络安全技术与应用，2022（12）：6–8.
[3]吴雄杰.基于竖屏剧建设移动互联网媒介平台的思考[J].中国广播电视学刊，2023（8）：49 – 51.
[4]裴雅，李亚珂.数据加密技术在计算机网络通信安全中的应用探究[J].信息记录材料，2025，26（4）：87–89.