基于人工智能的通信信息安全风险评估与防范

魏晓飞
西部机场集团宁夏机场有限公司　宁夏　银川　750000

摘　要：随着人工智能技术在通信领域的广泛应用，通信信息安全面临着新的机遇与挑战。本文首先探讨了人工智能在通信信息安全领域的应用现状，包括智能威胁检测、身份认证、数据加密等方面。接着，深入分析了基于人工智能的通信信息安全所面临的风险，如人工智能模型自身的安全漏洞、攻击者利用人工智能技术实施的新型攻击、数据隐私泄露等。然后，针对这些风险，从技术、管理和法律三个层面提出了相应的防范措施，技术层面包括加强人工智能模型的安全性、构建智能防御系统等；管理层面包括建立健全安全管理制度、加强人员培训等；法律层面包括完善相关法律法规、加强监管力度等。最后，对未来基于人工智能的通信信息安全风险评估与防范进行了展望，旨在为保障通信信息安全提供参考。

关键词：人工智能；通信信息安全；风险评估；防范措施

1 引言

在数字化时代，通信信息已成为社会发展和人们生活中不可或缺的重要组成部分。随着 5G、物联网、云计算等技术的飞速发展，通信信息的传输量和复杂度急剧增加，通信信息安全问题日益凸显。人工智能技术的出现为通信信息安全提供了新的解决思路和方法，它能够通过对海量数据的分析和学习，实现对安全威胁的智能检测、预警和响应。然而，人工智能技术本身也存在一定的安全风险，同时攻击者也可能利用人工智能技术实施更具隐蔽性和破坏性的攻击，这使得通信信息安全面临着前所未有的挑战。因此，开展基于人工智能的通信信息安全风险评估与防范研究具有重要的现实意义。

2 人工智能在通信信息安全领域的应用现状

2.1 智能威胁检测

传统的威胁检测方法主要基于特征匹配和规则库，对于新型的、未知的安全威胁往往难以有效检测。人工智能技术，尤其是机器学习和深度学习算法，能够通过对大量的网络流量数据、日志数据等进行分析和学习，挖掘出其中的异常模式和潜在威胁。例如，基于机器学习的入侵检测系统可以通过训练模型，识别出网络中的异常连接、恶意代码攻击等行为；深度学习算法可以对恶意软件的特征进行自动提取和分类，提高对新型恶意软件的检测率。

2.2 身份认证

身份认证是保障通信信息安全的第一道防线。传统的身份认证方法如密码认证、令牌认证等存在着易泄露、易被盗用等问题。人工智能技术可以通过生物特征识别如指纹识别、人脸识别、虹膜识别等实现更安全、便捷的身份认证。例如，人脸识别技术可以通过对人脸图像的特征提取和匹配，准确识别用户身份，避免了密码泄露等安全隐患；基于机器学习的行为认证技术可以通过分析用户的操作行为、登录时间、地点等信息，判断用户身份的合法性，提高身份认证的安全性。

2.3 数据加密

数据加密是保护通信信息隐私和安全的重要手段。人工智能技术可以为数据加密提供新的方法和思路。例如，基于神经网络的加密算法可以通过构建复杂的神经网络模型，生成加密密钥，提高加密的安全性；机器学习算法可以对加密算法的性能进行优化，提高加密和解密的效率。此外，人工智能技术还可以用于数据脱敏，通过对敏感数据进行处理，使其在不影响数据使用价值的前提下，保护数据隐私。

2.4 网络安全态势感知

网络安全态势感知是指对网络安全状态的整体把握和预测。人工智能技术可以通过对网络中的各种安全事件、漏洞信息、威胁情报等进行收集、分析和整合，构建网络安全态势模型，实时感知网络安全状态，并对可能出现的安全威胁进行预警。例如，基于深度学习的网络安全态势感知系统可以通过对大量的历史数据进行学习，预测网络安全事件的发生概率和影响范围，为网络安全决策提供支持。

3 基于人工智能的通信信息安全风险分析

3.1 模型投毒攻击：攻击者通过在训练数据中注入恶意样本，使模型在训练过程中学习到错误的特征和模式，从而导致模型在实际应用中出现误判或失效。例如，在入侵检测系统的训练数据中注入大量的正常流量

数据，使模型对恶意流量的检测率降低。

模型窃取攻击：攻击者通过对模型的输入和输出进行分析，窃取模型的结构、参数等信息，从而复制出与原模型功能相似的模型。这不仅会导致模型的知识产权受到侵犯，还可能使攻击者利用窃取的模型实施更具针对性的攻击。

对抗性攻击：攻击者通过对输入数据进行微小的、有针对性的修改，使模型做出错误的判断。例如，在图像识别中，攻击者可以对图像进行微小的扰动，使人脸识别系统将一个人识别为另一个人；在恶意软件检测中，攻击者可以对恶意软件的代码进行修改，使检测模型将其误认为正常软件。

3.2 攻击者利用人工智能技术实施的新型攻击

智能钓鱼攻击：攻击者利用人工智能技术制作高度逼真的钓鱼邮件、网站等，诱骗用户泄露个人信息和账号密码。例如，通过自然语言处理技术生成与正常邮件相似的钓鱼邮件，提高钓鱼攻击的成功率；利用深度学习技术生成与目标人物相似的语音和视频，实施语音钓鱼和视频钓鱼攻击。

自动化攻击：攻击者利用人工智能技术实现攻击的自动化和智能化，提高攻击的效率和范围。例如，通过机器学习算法自动生成攻击脚本和 payload，对目标系统进行批量扫描和攻击；利用强化学习技术优化攻击策略，提高攻击的成功率。

隐私数据挖掘：攻击者利用人工智能技术对大量的公开数据和半公开数据进行分析和挖掘，提取出用户的隐私信息。例如，通过对社交媒体上的用户数据进行分析，挖掘出用户的兴趣爱好、人际关系、地理位置等隐私信息；利用机器学习算法对医疗数据、金融数据等进行分析，获取用户的敏感信息。

3.3 数据隐私泄露风险

人工智能技术的应用需要大量的数据支持，这些数据中往往包含着用户的隐私信息。在数据收集、存储、处理和传输过程中，存在着数据隐私泄露的风险。例如，在数据收集过程中，如果对数据的来源和合法性审核不严，可能会收集到大量的个人隐私数据；在数据存储过程中，如果存储设备的安全防护措施不到位，可能会导致数据被非法访问和窃取；在数据处理过程中，如果对数据的处理方式不当，可能会导致数据隐私信息的泄露。此外，人工智能模型在训练过程中可能会记住训练数据中的隐私信息，当模型被部署和使用时，这些隐私信息可能会被泄露。

3.4 算法偏见导致的安全风险

人工智能算法的训练数据往往来自于现实世界，而现实世界中存在着各种偏见和歧视。如果训练数据中存在偏见，那么训练出来的人工智能算法也会存在偏见。这种算法偏见可能会导致通信信息安全领域出现不公平的现象。例如，在身份认证中，如果人脸识别算法对某些种族或年龄段的人群存在识别偏见，可能会导致这些人群的身份认证失败，影响其正常的通信和使用；在风险评估中，如果算法对某些用户群体存在偏见，可能会导致对这些用户的安全风险评估不准确，增加安全事故的发生概率。

4 基于人工智能的通信信息安全风险防范措施

4.1 技术层面

采用安全的模型训练方法：在模型训练过程中，采用数据清洗、数据增强等技术，减少训练数据中的恶意样本和噪声，提高模型的鲁棒性。同时，采用联邦学习、差分隐私等技术，保护训练数据的隐私安全，避免数据泄露。

开展模型安全测试：在模型部署前，对模型进行全面的安全测试，包括模型投毒攻击测试、模型窃取攻击测试、对抗性攻击测试等，及时发现模型存在的安全漏洞，并进行修复。

采用模型加密技术：对人工智能模型的结构和参数进行加密处理，防止模型被窃取和滥用。例如，采用同态加密技术，使模型在加密状态下能够进行计算和推理，保证模型的安全性。

融合多种安全技术：将人工智能技术与传统的安全技术如防火墙、入侵检测系统、 antivirus 等相结合，构建多层次、全方位的智能防御系统。通过人工智能技术对网络流量、日志数据等进行实时分析和监测，及时发现和预警安全威胁，并利用传统安全技术进行快速响应和处置。

实现动态防御：利用人工智能技术实现防御策略的动态调整。根据网络安全态势的变化和攻击者的攻击手段，自动调整防御策略，提高防御系统的适应性和有效性。例如，当发现新的攻击模式时，智能防御系统可以自动更新入侵检测规则，提高对新型攻击的检测率。

数据加密：对通信信息数据进行加密处理，包括数据传输加密和数据存储加密。采用先进的加密算法如 AES、RSA 等，确保数据在传输和存储过程中的安全性。同时，加强密钥管理，定期更换密钥，防止密钥泄露。

数据脱敏：对敏感数据进行脱敏处理，去除或替换数据中的敏感信息，如姓名、身份证号、银行卡号等。在数据共享和使用过程中，只提供脱敏后的数据，保护用户的隐私安全。

数据访问控制：建立严格的数据访问控制机制，对数据的访问进行授权和管理。根据用户的角色和权限，限制用户对数据的访问范围和操作权限，防止数据被非法访问和滥用。

4.2 管理层面

制定完善的安全管理规范：明确通信信息安全管理的目标、职责、流程和要求，建立健全安全事件响应机制、风险评估机制、安全审计机制等，确保通信信息安全管理工作的规范化和制度化。

加强人员管理：加强对员工的安全意识培训和教育，提高员工的安全意识和防范能力。建立员工安全行为规范，对员工的操作行为进行监督和管理，防止因员工操作不当导致的安全事故。

定期开展安全检查和评估：定期对通信信息系统和网络进行安全检查和风险评估，及时发现和消除安全隐患。根据安全评估结果，制定相应的整改措施，不断完善安全管理体系。

对供应商进行严格审核：在选择人工智能技术和产品供应商时，对供应商的资质、信誉、安全能力等进行严格审核，选择具有良好安全记录和较强安全实力的供应商。

签订安全协议：与供应商签订详细的安全协议，明确双方的安全责任和义务，要求供应商采取必要的安全措施，保障其提供的技术和产品的安全性。

加强对供应链的监督和管理：定期对供应商的安全状况进行监督和检查，及时发现和解决供应链中存在的安全问题。建立供应链安全事件应急响应机制，当发生供应链安全事件时，能够及时采取措施进行处置。

4.3 法律层面

制定专门的人工智能安全法律法规：针对人工智能技术在通信信息安全领域的应用，制定专门的法律法规，明确人工智能技术的应用范围、安全要求、责任划分等，为人工智能技术的安全应用提供法律保障。

加强数据隐私保护立法：进一步完善数据隐私保护法律法规，明确数据收集、存储、处理、传输等环节的隐私保护要求，加大对数据隐私泄露行为的处罚力度，保护用户的隐私安全。

建立健全监管机制：建立由政府部门、行业协会、企业等多方参与的监管机制，加强对人工智能技术在通信信息安全领域应用的监管。明确各监管主体的职责和权限，形成监管合力。

加强对人工智能产品和服务的监管：对人工智能产品和服务进行严格的安全审查和认证，确保其符合安全标准和要求。对不符合安全要求的产品和服务，禁止其进入市场。

加大对违法行为的处罚力度：对利用人工智能技术实施通信信息安全违法行为的，依法予以严厉处罚，追究其法律责任。通过严厉的处罚措施，威慑潜在的违法者，维护通信信息安全秩序。

5 结论与展望

5.1 结论

人工智能技术在通信信息安全领域的应用为保障通信信息安全带来了新的机遇，但同时也带来了一系列的安全风险。本文通过对人工智能在通信信息安全领域的应用现状进行分析，指出了基于人工智能的通信信息安全所面临的模型安全漏洞、新型攻击、数据隐私泄露、算法偏见等风险，并从技术、管理和法律三个层面提出了相应的防范措施。通过加强人工智能模型的安全性、构建智能防御系统、加强数据安全管理、建立健全安全管理制度、完善相关法律法规等措施，可以有效降低基于人工智能的通信信息安全风险，保障通信信息的安全。

5.2 展望

随着人工智能技术的不断发展和进步，基于人工智能的通信信息安全风险评估与防范将面临新的挑战和机遇。未来，人工智能技术将在通信信息安全领域发挥更加重要的作用，如基于量子计算的人工智能安全技术、基于区块链的人工智能安全管理等将成为研究的热点。同时，随着法律法规的不断完善和监管力度的不断加强，人工智能技术在通信信息安全领域的应用将更加规范和安全。我们需要不断加强对人工智能技术的研究和探索，提高通信信息安全风险评估与防范的能力，为数字化时代的通信信息安全提供坚实的保障。

参考文献

[1]王允昕. 基于人工智能的网络通信信息数据安全加密技术[J].互联网周刊,2025,(14):35-37.

[2]徐焕. 基于人工智能的网络通信信息数据安全加密技术研究[J].中国高新科技,2025,(12):109-111.DOI:10.13535/j.cnki.10-1507/n.2025.12.33.

[3]杨嘉. 基于人工智能的网络通信信息数据安全加密技术研究[J].信息记录材料,2025,26(03):120-122.DOI:10.16009/j.cnki.cn13-1295/tq.2025.03.022.

[4]朱杰. 基于人工智能的网络通信信息数据安全加密技术研究[J].信息记录材料,2025,26(02):144-146.DOI:10.16009/j.cnki.cn13-1295/tq.2025.02.036.