AI驱动的移动通信网用户行为分析技术研究

Research on AI-Driven User Behavior Analysis Technology for Mobile Communication Network

谢中怀，张曼君，谢泽铖（中国联通研究院，北京，100048）
Xie Zhonghuai，Zhang Manjun，Xie Zecheng（China Unicom Research Institute，Beijing 100048，China）

摘　要：
随着移动通信网技术的不断发展，网络边界趋于消失，接入方式日益复杂，网络用户行为监管和内部安全管控的难度显著增加。通过引入AI驱动的用户与实体行为分析（UEBA）技术，可以有效应对这一安全挑战。介绍了UEBA技术的基本概念与技术流程，分析了UEBA技术在移动通信领域应用的可行性，并对其未来发展趋势作出展望。

关键词：
移动通信网络安全；用户行为分析；人工智能；内部威胁
doi：10.12045/j.issn.1007-3043.2025.09.008
文章编号：1007-3043（2025）09-0043-04
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
With the continuous development of mobile telecommunication network technology, network boundaries are gradually vanishing, access methods are becoming increasingly complex, and the difficulty of regulating user behavior and controlling internal security has significantly increased. The introduction of AI-driven User and Entity Behavior Analytics (UEBA) technology can effectively address the security challenge. It introduces the basic concepts and technical processes of UEBA technology, analyzes the feasibility of applying UEBA technology in the field of mobile telecommunication, and provides an outlook on the future development trends.

Keywords：
Mobile telecommunication network security; User behavior analysis; Artificial intelligence (AI); Internal threats

引用格式：谢中怀，张曼君，谢泽铖. AI驱动的移动通信网用户行为分析技术研究[J]. 邮电设计技术，2025(9)：43-46.

1 概述

随着移动通信技术的不断演进、物联网的爆发式增长以及边缘计算的深度部署，移动通信网已经成为国家关键信息基础设施和社会经济运行的核心载体。海量用户数据（包括身份信息、位置轨迹、通信内容、业务偏好等）在网内产生、传输与处理，其价值与敏感性日益凸显。同时，网络架构的云化、虚拟化、服务化使得传统网络边界趋于消失，接入方式更加复杂多元，极大地增加了网络内部安全管控与用户行为监管的难度。而随着网络运营商、设备商等企业数字化转型的不断推进，企业员工接入方式日益复杂，企业内部的安全管控也越来越困难。Ponemon在2022年发布的《全球内部威胁成本报告》显示，内部威胁给企业带

收稿日期：2025-07-25

来的安全风险正在大幅度增加。2021年全球60%的公司面临超过20次的内部攻击,比2018年增加了53%[1]。一方面,网络攻击者可以伪装成合法用户来入侵网络边界,从而侵入组织网络制造安全事故,借机窃取网络中的重要信息;或者在内网安装恶意软件,影响企业网络的正常运行,危害企业正常的生产经营活动。另一方面,随着定向社工等威胁技术的不断发展,被勒索的用户、安全意识淡薄的用户成为了企业网络的新型漏洞。一些掌握着涉密、敏感信息的高权限用户一旦被此类攻击渗透,就会成为隐形的攻击点位,导致大规模用户隐私泄露、关键业务中断、网络资源被恶意占用,甚至导致国家级通信基础设施遭受破坏[2-3]。

因此,移动通信网亟需引入有效的内部威胁分析与检测机制,来满足日益增长的网络用户行为监管和内部安全管控需求。用户与实体行为分析(User and Entity Behavior Analytics,UEBA)[4]技术最早起源于用户行为分析(User Behavior Analytics,UBA)技术。2014年,Gartner发布了UBA市场指南,并在2015年将实体行为与用户行为进行了关联,逐步由最初应用的经营销售领域转向网络及数据安全领域[5]。其中,新增加的实体(Entity)概念强调了设备行为在网络攻击与威胁检测中的重要作用[6]。而随着AI与大数据的不断发展,机器学习、深度学习、联邦学习等技术逐步被引入到UEBA系统之中。通过抓取海量、多维的移动网络数据,UEBA系统可以自动化地学习用户与实体的正常行为模式,并建立动态演进的行为基线。通过实时比对实际行为与基线模型的偏差,结合如时间、位置、业务类型、网络状态等的上下文信息,UEBA系统可以自适应地评估行为风险系数,从而有效检测出传统规则引擎难以发现的、复杂且隐蔽的异常行为与内部威胁。

UEBA技术的出现弥补了传统基于固定规则和特征库的安全方案在应对移动网海量数据、未知攻击模式(如零日漏洞利用、新型欺诈)时的局限性,为运营商提供从账号安全、终端安全、到数据安全、业务安全等多维度的、系统化的内部风险监管能力。

2 UEBA技术流程

UEBA系统的实现流程通常包括以下几个关键步骤:多源异构数据采集与融合、AI行为分析模型建立、实时异常检测与动态风险评估以及智能化的自适应响应处置。

2.1 多源异构数据采集与融合

数据收集是UEBA系统的基础,UEBA系统需要通过分布式流处理框架实时接入移动通信网多维度数据源,获取包括5G核心网信令、用户话单、深度包检测流量、网元设备日志、终端探针数据及身份管理记录等原始数据[7]。对原始数据进行标准化清洗后,基于图数据库进行实体关联解析,构建以用户ID、终端ID等关键身份信息为枢纽的统一关系图谱。通过特征工程提取时空行为模式(如位置切换熵值、信令交互频率)、统计指标(会话量标准差)及上下文特征(业务敏感度评级),最终生成结构化特征向量用于AI模型训练。

2.2 AI行为分析模型建立

UEBA系统通过持续收集和分析用户的历史行为数据,运用统计分析技术构建动态更新的“正常行为基线”。这一基线并非静态阈值,而是基于时间序列分析、聚类分析及概率模型,从登录时间、访问频率、操作序列、资源使用量等多个维度刻画用户的典型行为模式。系统采用无监督学习算法对历史数据进行初步建模,识别出常见行为模式并自动排除异常噪声,从而形成基准行为轮廓。随后,系统结合监督学习与半监督学习算法,进一步优化模型精度。例如,决策树算法通过规则分裂直观地标识异常行为路径;随机森林集成多棵决策树,通过投票机制降低过拟合风险,提升对未知攻击检测的鲁棒性;支持向量机(SVM)在高维特征空间中寻找最优超平面,尤其适用于区分细微的异常行为模式;神经网络(尤其是深度学习模型)则能自动提取行为特征中的非线性关系,处理大规模高维数据,并通过循环神经网络(RNN)或长短期记忆网络(LSTM)捕捉行为序列中的时序依赖关系。这些算法通常以集成方式协同工作,通过加权投票或堆叠策略融合多模型结果,最终输出用户行为的风险评分[8]。同时,系统会持续通过在线学习机制更新模型,以适应行为模式的缓慢漂移,确保基线始终反映当前的真实环境。

2.3 实时异常检测与动态风险评估

UEBA系统会实时监测用户与实体的行为数据,并将其与既定的行为基线进行对比,识别异常行为。一种常见的方法是使用统计分析技术,比如基于机器学习的模型。这些模型可以识别出不符合用户或实体历史行为特性的异常行为,如大量的文件访问、异

常的登录活动或未经授权的数据传输。通过监控用户和实体的行为变化，系统可以发现如账号被盗、异常下载等潜在的安全威胁[9]。此外，UEBA技术还可以结合上下文信息进行异常行为检测。例如，当一个用户在非常规的时间段登录系统，或者在从未访问过的地理位置进行操作时，系统会产生警报。通过综合考虑行为模式、上下文信息以及实时威胁情报，UEBA系统能够更准确地识别出异常行为，提高检测的可信度[10]。

2.4 智能化的自适应响应处置

UEBA通常可集成在安全自动化响应系统或安全运营中心系统中，在收到告警信息后为系统提供相应的策略和解决方案，并采取适当的响应措施。对于级别较低、优先性较低的告警信息，系统可以自动执行一些事先定义好的规则或响应措施。例如，暂时禁止用户的访问权限、发送警告通知或触发进一步的审查流程。这些自动化的响应有助于迅速应对低级别的风险事件，减轻人工干预的压力。而对于级别较高、风险系数较高的告警信息，系统会将详细的日志与分析报告提供给安全团队，以便安全人员及时准确地确认风险点位与风险原因，结合既定的安全策略与方案，对异常来源进行封堵和处理。

3 UEBA在移动通信网风险管控中的应用价值

UEBA系统通过AI驱动，对海量用户与实体行为进行持续监管与自适应分析，为移动通信网络运营商提供了强大的内部风险管控能力。

3.1 赋能运营管理

UEBA技术可以帮助网络运营管理者精准识别内部威胁与失陷实体。通过分析用户和实体的行为模式，UEBA系统能够有效发现恶意内部人员（如违规查询用户隐私、篡改业务数据）、被社工或劫持的合法用户账号（如异常登录、异常业务操作）以及被植入恶意软件的终端设备（如信令异常、异常流量外联），防止其造成数据泄露、业务欺诈或网络破坏[11]。

3.2 保护用户隐私

UEBA技术能够帮助网络运营者主动预防用户数据泄露。通过监控对用户敏感数据（如详单、位置、身份信息）的访问、查询、导出等操作，系统能及时发现并阻止内部人员滥用权限或外部攻击者通过失陷账号进行数据窃取行为，确保用户隐私和运营商数据资产安全[12]。

3.3 合规与反诈

通过引入UEBA系统，可以有效强化业务合规与反欺诈。UEBA系统可监测异常的业务办理模式（如养卡、套利）、高欺诈风险的业务使用（如异常国际漫游、高额欠费风险）以及合作伙伴或内部人员的违规操作，保障业务健康运营，减少经济损失[13]。

3.4 提高安全运营效率

UEBA技术可以大大提高安全运营效率。通过AI驱动的自动化分析和自适应的分级响应，可以大幅减少安全团队处理海量低价值告警的负担，使安全团队能够聚焦真正的高风险事件，提升整体安全运营效率。

总体而言，UEBA作为一个强有力的工具，通过持续监控和分析用户与实体的行为，为安全管理团队提供了必要的信息，以便及时响应各种内部威胁。随着机器学习和人工智能技术的发展，UEBA系统的分析能力将进一步增强，从而提供更为高效和精准的内部风险管理解决方案。

4 技术发展与未来挑战

随着人工智能技术的不断发展和企业对内部威胁的重视程度的提升，UEBA技术前景广阔，但同时也面临着一系列的技术挑战与未来发展问题。

4.1 技术挑战

UEBA技术的实现基于大量的网络核心数据，而数据来源范围大、缺乏数据标准化格式以及关键数据缺失等都会影响UEBA在模型建立初期的模型准确度和泛用度。随着网络活动产生的数据量不断提升，大量低质量的数据会导致UEBA系统产生误报，对正常行为产生错误的反馈，从而误导安全团队产生错误判断并忽视真实安全事件的风险。

同时，在使用UEBA技术进行行为分析时，涉及到大量用户和实体的数据，因此需要兼顾数据分析中对数据完整性的要求和保护用户重要隐私的要求。

4.2 未来发展

未来，UEBA技术将在内部安全管理和威胁检测领域发挥更重要和广泛的作用。随着大数据、人工智能和机器学习等技术的不断进步，UEBA技术的未来发展前景十分广阔。

随着深度学习和人工智能技术的不断发展，UEBA系统将更加智能化。未来UEBA系统能够发现和识别更复杂、更隐蔽的威胁行为模式。例如，基于

神经网络的模型可以更好地识别用户行为中的异常模式，减少误报率，提高威胁检测的准确性[14]。

同时，随着硬件性能的提升，未来的UEBA系统将更加注重预警的实时性和响应的自动化，通过更快地对大规模数据进行分析和处理，实现更快速的威胁检测和响应。自动化响应技术也将得到进一步发展，系统可以根据预先定义的规则或模型自动触发响应措施，缩短安全事件的响应时间[15]。

此外，未来的UEBA系统将整合更多的数据源，包括终端设备数据、云服务数据等，通过多维度的数据收集实现对用户和实体行为更全面的分析。而随着隐私保护法规的不断完善，未来UEBA系统在大量收集数据的过程中还需采用更先进的数据加密、脱敏技术，来确保数据隐私保护和数据合规。

5 结语

移动通信网作为数字社会的神经中枢，其安全稳定运行至关重要。面对日益严峻的内部风险和复杂多变的用户行为威胁，传统的静态防御手段已力不从心。本文研究的AI驱动的移动通信网用户行为监管技术，通过深度融合大数据处理与人工智能技术，特别是机器学习、深度学习、图分析等，实现了对海量用户与实体行为的动态基线建模、实时异常检测、精准风险评估以及智能化的自适应响应。这一技术为运营商提供了强大的工具，能够有效应对恶意内部人员、失陷账号、异常终端以及各类业务欺诈等风险，在保障用户数据安全、维护业务合规、优化网络资源、提升运营效率等方面具有显著价值。

尽管在数据规模、实时性、隐私合规、模型优化等方面仍面临挑战，但随着AI技术的持续突破、隐私增强计算的成熟应用以及标准化生态的完善，该系统的智能化、实时性、精准度和隐私保护能力将不断提升。未来，AI驱动的用户行为监管与自适应分析必将成为构建智能、弹性、可信的新一代移动通信网络安全防御体系的核心支柱，为网络强国和数字中国建设提供坚实的安全保障。

参考文献：

[1] Ponemon Institute. 2022 Cost of insider threats global report[R]. Traverse City：Ponemon Institute，2022.

[2] CAPPELLI D，MOORE A P，TRZECIAK R F. The CERT guide to insider threats：how to prevent，detect，and respond to information technology crimes（theft，sabotage，fraud）[M]. Reading：Addison-Wesley Professional，2012.

[3] 王琦. 基于UEBA技术对关键信息基础设施中网络异常行为检测的研究[J]. 电子元器件与信息技术，2024，8(2)：186-189.

[4] 中国信通院，安恒信息. 网络安全先进技术与应用发展系列报告 用户实体行为分析技术（UEBA）（2020年）[R/OL]. [2025-02-08]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202006/P020200619441768543756.pdf.

[5] 赵璐瑾. 基于UEBA的电力行业重要数据安全分析方案的研究与实现[D]. 北京：北京邮电大学，2022.

[6] 徐飞. 基于UEBA的网络安全态势感知技术现状及发展分析[J]. 网络安全技术与应用，2020(10)：10-13.

[7] 刘进，李江波，叶兵. 对于UEBA数据安全内控风险管理的研究[J]. 网络空间安全，2021，12(3)：43-48，55.

[8] 莫凡，何帅，孙佳，等. 基于机器学习的用户实体行为分析技术在账号异常检测中的应用[J]. 通信技术，2020，53(5)：1262-1267.

[9] GHIASSI M，PHAN T. Beyond intrusion detection：a survey of user and entity behavior analytics[J]. ACM Computing Surveys（CSUR），2021，54(1)：1-39.

[10] LISON P，JOUFFROY J. UEBA：a holistic approach to cybersecurity[C]//2019 IEEE European Symposium on Security and Privacy Workshops（EuroS&PW）. Stockholm：IEEE，2019：14-19.

[11] SHASHANKA M，SHEN M Y，WANG J S，et al. User and entity behavior analytics for enterprise security[C]//2016 IEEE International Conference on Big Data（Big Data）. Washington，DC：IEEE，2016：1867-1874.

[12] ALSHAMMARI R，ZHANG J，XIANG Y，et al. A comprehensive survey on user and entity behavior analytics for insider threat detection[J]. IEEE Communications Surveys & Tutorials，2017，19(2)：762-785.

[13] KIRAN R U，MALLICK T K，JAIN R C，et al. A review on user and entity behavior analytics for insider threat detection[J]. International Journal of Computer Applications，2018，181(38)：28-33.

[14] CHOUDHARY K R，RAMAN R. An ensemble approach for ueba using deep learning and machine learning algorithms[C]//Proceedings of the 4th International Conference on Computing Methodologies and Communication. Singapore：Springer，2020：841-848.

[15] BASU S，GANGULY S. A survey on user and entity behavior analytics（UEBA）using machine learning[J]. International Journal of Computer Applications，2018，181(38)：38-42.

作者简介：
谢中怀，毕业于香港理工大学，工程师，硕士，主要研究方向为网络与信息安全；张曼君，毕业于西安电子科技大学，高级工程师，博士，主要研究方向为网络与信息安全；谢泽铖，毕业于北京交通大学，工程师，硕士，主要研究方向为网络与信息安全。