基于 TCM-KNN 算法的多级网络访问安全控制方法

张创基[1] 林伟烜[2] 许景民[1]
ZHANG Chuangji LIN Weixuan XU Jingmin

摘 要 多级网络由多个层级组成，其中的每一级都需要安全防护，现有安全策略难以做到既保持一致性又体现差异化。从一致性角度看，整个多级网络应该遵循基本的安全原则，但从差异化角度看，不同层级网络面临的安全威胁可能不同，因此，制定合适的安全策略至关重要。对此，文章研究了一种基于 TCM-KNN 算法的多级网络访问安全控制方法。首先，针对收集到的用户基础信息进行标准化与数据聚合处理，以了解用户的基本特征。然后，将预处理后的用户行为数据作为训练样本引入 TCM-KNN 算法，进行多级网络的异常检测。并根据入侵检测结果进行安全控制策略制定，通过用户身份认证确定安全环节上的一致性，利用 ACL 访问控制列表设置不同层级的访问规则，确定安全环节上的差异性。最后，实时监测用户行为，当行为异常得分超阈值时动态调整用户访问权限，以此确保网络安全。对比实验结果表明：该方法可以满足多级网络的安全控制需求，实现对不同类型访问等级、权限的精准划分。

关键词 TCM-KNN 算法；异常检测；身份认证；安全控制；访问；多级网络

doi：10.3969/j.issn.1672-9528.2025.03.023

0 引言

随着信息技术的发展，网络安全问题日益凸显，尤其是网络访问的安全控制成为一个重要的研究领域。在复杂的网络环境中，如何有效地识别并阻止非法访问，保障网络资源的合法使用，是当前网络安全领域面临的一大挑战。TCM-KNN 算法作为一种先进的机器学习算法，因其高效、准确的特性，在网络安全领域展现出了广阔的应用前景。

李文军等人[1]基于可信度和智能合约，旨在应对物联网环境中分布式终端面临的多种安全威胁。在研究中，首先对数据属性进行分级，并根据用户历史行为计算其可信度。通过利用区块链技术，动态调整访问控制策略，确保只有高可信度的用户能够访问高级敏感数据。智能合约的引入，进一步确保了策略的高效执行。但其策略检索方法可能相对低效，特别是在处理海量数据时。宋岍龙[2]结合网络边界区域、传输信道区域及移动终端设备区域，建立了多个目标函数，如边界访问控制、安全威胁检测和用户身份认证等。通过 SPEA- Ⅱ算法对联合目标函数进行求解，实现了网络多层次安全访问控制机制的最佳方案。但 SPEA- Ⅱ算法的复杂度和计算量较大，可能导致系统性能下降。吴克河等人[3]通过边缘融合终端进行重加密，既保护数据安全，又减轻终端设备的通信开销，在策略授权方面，使用可扩展的访问控制标记语言设计授权策略和策略匹配算法，实现对多终端访问控制策略的同时下发，更高效地解决安全访问控制问题。虽然该方法通过边缘融合终端进行重加密可以减轻通信开销，但重加密过程本身会带来额外的计算资源消耗。特别是在资源受限的边缘设备上。蔡斌[4]在现有云计算数据存储安全体系架构基础上使用 AES 对称加密算法对 CDC 中的数据文件进行加密处理从而实现 USER 安全访问，与传统访问控制技术方案相比安全，可靠性更高。然而，AES 对称加密算法虽然具有较高的安全性和加密速度，但其密钥管理相对复杂。在云计算环境中，随着数据量和用户数量的增加，密钥的管理和分发成为一个挑战。为保障网络资源的合法使用，防范网络攻击，本文将引进 TCM-KNN 算法，以多级网络为例，开展访问安全控制方法的设计研究。

1 用户行为数据采集与处理

为满足多级网络访问的安全控制，设计方法前，使用数据挖掘工具，进行网络数据的检索与扫描，收集用户的 ID、姓名、年龄、性别、地区等基础信息，了解用户的基本特征和背景。

对采集数据进行标准化处理，公式为：

$$Y=\frac{y-\bar{y}}{\hat{y}} \tag{1}$$

1. 广州华立科技职业学院 广东广州 511325
2. 广州华商职业学院 广东广州 511325

[基金项目] 2023 年度广东省普通高校特色创新类项目（2023KTSCX409）

式中：Y 表示标准化后的数据；y 表示原始数据；$\bar{y}$ 表示 y 的平均值；$\hat{y}$ 表示 y 的标准差。在此基础上，对数据进行汇总统计，实现数据聚合处理。相关系数分析能够量化用户行为数据中各变量之间的关联程度，揭示它们之间的线性关系。这对于理解用户行为模式、识别关键影响因素至关重要。计算公式为：

$$r=\sqrt{\left(Y-\bar{Y}\right)^2} \tag{2}$$

式中：r 表示相关系数；$\bar{Y}$ 表示 Y 的均值。基于此，数据的聚合处理过程计算公式为：

$$A=\operatorname{sum}\frac{Y(n)}{Nr} \tag{3}$$

式中：A 表示数据的聚合处理；n 表示第 n 个数据；N 表示数据个数 [5]。并将其归为一类，输出相似性较高的数据，以此种方式，完成用户行为数据的采集与处理。

2 基于 TCM-KNN 算法的多级网络异常监测

基于上述预处理后的用户行为数据，其作为训练样本数据引入 TCM-KNN 算法，进行多级网络的异常检测。此过程旨在通过分析用户行为数据，识别并阻止潜在的网络异常行为。从完成处理的行为数据中提取关键特征，用于 TCM-KNN 算法的训练和预测 [6]。在 TCM-KNN 算法中，计算待检测样本与训练样本之间的距离，此过程计算公式为：

$$d=\Delta A\cdot\sqrt{\sum\left(x_i-y_i\right)^2} \tag{4}$$

式中：d 表示待检测样本与训练样本之间的距离；x_i、y_i 分别表示第 i 个检测样本与训练样本数据。完成上述计算后，进行样本数据中关键数据的分类 [7]。为确保分类结果的准确性，引入权重分配机制，进行不同类别数据的权重计算。此过程计算公式为：

$$L=\frac{d}{\arg\max\left(w_i\cdot c_i\right)} \tag{5}$$

式中：L 表示数据的权重；w 表示数据分配系数；c 表示最大类别。同时，根据 K 个最近邻样本的类别，采用多数投票法或加权投票法进行分类决策，利用 TCM-KNN 算法对用户行为分类决策数据进行实时监测，即可实现对网络异常的检测 [8]。此过程计算公式为：

$$M=\frac{1}{L^2+\left(\chi+1\right)^2} \tag{6}$$

式中：M 表示异常数据检测结果；χ 表示最近邻样本的类别。基于此，异常检测系统能够识别并标记出潜在的网络攻击行为。

3 用户身份认证与多级网络访问安全控制

多级网络作为复杂且庞大的系统架构，通常由多个相互关联、功能各异的层级构成。每个层级在网络中扮演着不同的角色，承载着不同的数据流量和服务需求，因此也面临着各自独特的安全挑战。针对这种多层次的网络结构，制定一套既能保持一致性又能体现差异化的安全策略显得尤为重要。

根据上述异常检测结果，系统可以动态地调整用户的访问权限，制定具有一致性与差异性安全策略。具体步骤如下：

首先，在多级网络中，用户身份认证是基本的安全原则。通过式（7）进行用户身份认证，无论是哪个层级的网络，都遵循这一基本的安全操作。这确保了整个多级网络在用户身份验证这一关键安全环节上的一致性 [9]。

$$H(M)=\frac{1}{h(p)} \tag{7}$$

式中：H 表示用户身份认证；h 表示哈希函数；p 表示用户输入的密码。除了密码认证外，还可以引入其他认证因素，如生物特征（指纹、面部识别等）或物理设备（如手机验证码）。通过此种方式，进一步提高身份认证的安全性。

完成身份验证后，针对不同层级的网络面临不同的安全威胁，ACL 能够很好地体现这种差异化。因为 ACL 可以针对每个用户在不同层级网络中的情况设置具体的访问规则。例如，对于核心层级网络中的关键资源，ACL 可以设置非常严格的访问权限，只允许少数具有特定身份标识的用户进行非常有限的操作；而对于边缘层级网络中的一些公开资源，ACL 可以设置相对宽松的访问权限，允许更多用户进行读取等操作。

引入 ACL 后，系统能够针对每个用户设置具体的访问规则，从而精确地控制不同层级间的差异性问题。此过程计算公式为 [10]：

$$\mathrm{ACL}=H(M)\sum a\cdot\frac{\delta^2}{m+1} \tag{8}$$

式中：ACL 表示访问控制列表设置；a 表示用户身份标识；δ 表示网络资源；m 表示访问控制返回值。对用户行为数据进行实时监测和分析。当用户行为异常得分超过某个阈值时，可以临时降低其访问权限或限制其访问某些敏感资源。用户身份动态权限调整过程计算公式为：

$$Q=\frac{1}{H(M)\cdot\mathrm{ACL}}+\frac{1}{f(e)} \tag{9}$$

式中：Q 表示用户身份动态权限调整；f 表示用户当前行为特征的值；e 表示异常值的阈值。通过整合用户身份认证与多

级网络访问安全控制，确保只有合法用户才能访问网络，并实时监测用户行为以防止潜在的网络入侵。

4 对比实验

4.1 实验准备

本次实验选择某大型企业内网作为研究试点，该网络结构复杂，包含多个子网和防火墙，实现了数据的分级存储和访问控制。多级网络的技术参数、规模等进行分析，如表 1 所示。

表 1 多级网络的技术参数、规模

序号	项目	参数
1	网络层级数	4 层（核心层、汇聚层、接入层、隔离层）
2	总节点数	5 000 个节点
3	防火墙数量	10 台高性能防火墙
4	带宽容量	100 Gbit/s
5	并发连接数	500 000 个并发连接
6	VLAN 数量	100 个 VLAN
7	安全策略数量	500 条安全策略
8	入侵检测系统 (IDS)	5 套 Snort IDS
9	日志审计系统容量	1 TB 存储空间
10	平均响应时间	5 ms

4.2 实验步骤

实验中，为了模拟真实的多级网络环境，搭建四层架构环境。核心层负责高速数据传输，汇聚层进行流量控制和安全策略实施，接入层提供用户接入，隔离层则用于保护关键资源。同时，在汇聚层或接入层部署 TCM-KNN 算法，用于实时监测和分析网络流量，识别异常访问行为。为了验证实验的有效性，搭建一个测试环境，包括模拟攻击和合法访问请求，确保测试环境与实际网络环境具有相似的特征和复杂性。测试环境架构如图 1 所示。

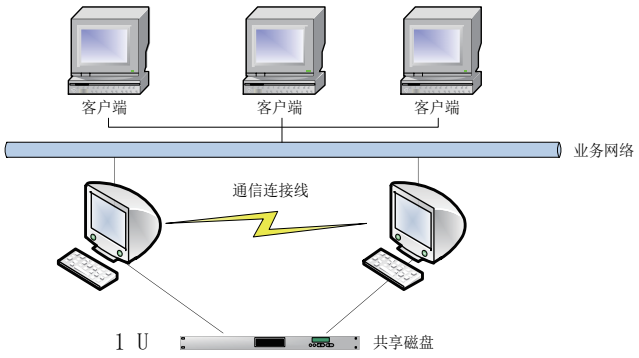

图 1 多级网络访问安全控制方法测试环境架构

启动多级网络环境，并收集一段时间内的网络流量数据。利用收集到的网络流量数据，训练 TCM-KNN 算法模型。模拟 10 名用户，将其编号 1~10，每名用户在网络中的访问权限不同。具体内容如表 2 所示。

表 2 多级网络访问用户的等级与权限分配

用户编号	多级网络访问等级	访问权限
1	一级	浏览网页
2	二级	深度检索网络、浏览网页
3	0 级（无权限）	无法登录此网站
4	三级	下载文件、深度检索网络、浏览网页
5	四级	上传文件、下载文件、深度检索网络、浏览网页
6	五级（最高）	管理用户账户、上传文件、下载文件、深度检索网络、浏览网页
7	三级	与用户 4 相同
8	二级	与用户 2 相同
9	一级	与用户 1 相同
10	四级	与用户 5 相同

模拟用户 1~10 访问多级网络，引进文献 [1] 提出的基于可信度的安全控制方法、文献 [2] 提出的基于 SPEA- Ⅱ 算法的安全控制方法，将其作为对照。同时应用 3 种方法，对用户的多级网络访问过程进行安全控制。

4.3 实验指标

在多级网络访问安全控制中，误报意味着将正常的用户行为判定为异常。如果误报率过高，安全系统会将大量的资源浪费在处理这些误判的情况上。使得网络安全访问控制性能大大下降。误报率，将正常行为误判为异常行为的比例。假设在测试集中有 N_n 个正常样本，被误判为异常的样本数为 N_{fp}，则误报率表达为：

$$FPR = \frac{N_{fp}}{N_n} \tag{10}$$

4.4 实验结果与分析

三种方法的异常行为误报率结果如图 2 所示。

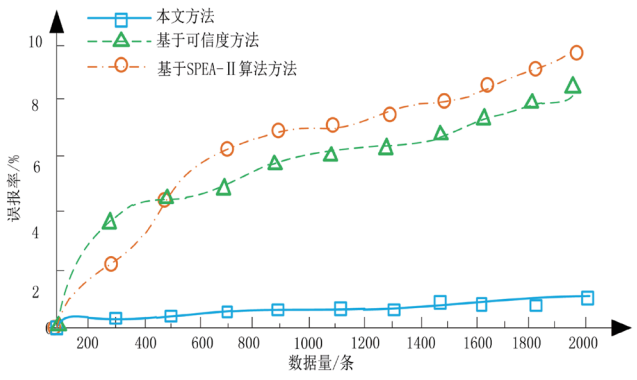

图 2 安全控制结果

根据图 2 结果可以看出，本文方法的误报率明显低于对比方法，当数据量达到 200 条时，仅为 1.2%. 而对比方法误报率最高分别达到 8% 与 9.7%。由此说明本文方法能够有效实现网络异常检测，为后续的安全访问控制提供帮助。

为了验证设计方法的有效性，将控制后用户可访问的内容与其实际访问的内容进行比对。通过模拟用户登录和网络访问行为，观察并记录用户实际能够访问的内容。在此基础上，将实际访问内容与预设的可访问内容进行比对，检查是否存在超出权限的访问行为或未被授予权限的合法访问被阻止的情况。如果实际访问内容与预设的可访问内容高度一致，说明安全控制方法能够有效地限制用户的访问行为，保护网络资源和数据的安全。实验结果如图 3 所示。

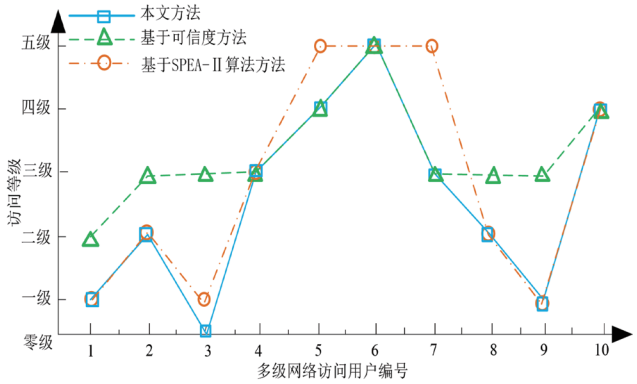

图 3 安全控制结果

从图 3 所示的结果可以看出，应用本文提出的方法进行用户多级网络访问的安全控制，得到的等级划分结果与表 1 结果一致，说明本文方法可以实现对不同类型访问等级、权限的精准划分。而应用基于可信度与基于 SPEA-II 算法均存在分配的结果与实际结果均存在不一致的现象，此种现象可能导致部分不法分子入侵网络，从而造成网络数据丢失等异常现象。

综合上述结果可以证明，本文此次设计的方法，可以满足多级网络的安全控制需求，全面保障网络的安全性。

5 结语

本文基于 TCM-KNN 算法的应用，通过用户行为数据采集与处理、多级网络入侵检测、用户身份认证与多级网络访问安全控制，完成了此次设计。旨在结合 TCM-KNN 算法的高效分类能力和多级安全策略的精细化控制，实现对网络访问的全面、准确监控。通过本次研究，发现该方法还具有较好的可扩展性和自适应性。随着网络环境的变化和攻击手段的不断更新，该方法能够通过更新训练数据集和优化算法参数，不断提高其检测准确率和适应能力。

参考文献：

[1] 李文军，李彩玲．基于可信度和智能合约的物联网分布式操作终端安全访问控制研究 [J]. 信息系统工程，2024(8): 16-19.

[2] 宋岍龙．基于 SPEA- Ⅱ算法的网络多层次安全访问控制方法 [J]. 计算机测量与控制，2024, 32 (6): 173-179.

[3] 吴克河，韩扬，田峥，等．新型电力系统面向云边端架构的安全访问控制技术研究 [J]. 电力信息与通信技术，2024, 22 (7): 1-8.

[4] 蔡斌．基于属性加密算法的计算机数据安全访问控制技术 [J]. 科技创新与应用，2024, 14 (10): 165-168.

[5] 徐浩，张侃，刘亚天．云计算平台下属性基数据加密与安全访问控制技术研究 [J]. 软件，2023, 44 (11): 91-93.

[6] 张迪，曹利，李原帅．车联网环境下基于多策略访问树的安全访问控制算法 [J]. 计算机应用研究，2023, 40 (11): 3394-3401.

[7] 徐胜超，杨波．基于进化泛函网络的云安全访问控制模型研究 [J]. 云南师范大学学报 (自然科学版), 2023, 43 (3): 36-40.

[8] 苗安影．云环境下的数据安全访问控制模型设计及实现 [J]. 信息与电脑 (理论版), 2023, 35 (8): 63-65.

[9] 黄海艇，徐盼，唐沸涛．工业互联网感知层多端口安全访问控制系统设计 [J]. 电子设计工程，2023, 31 (5): 153-157.

[10] 邢慧芬，车辉．基于 ACL 和防火墙的网络安全访问控制的设计与实现 [J]. 曲靖师范学院学报，2022, 41 (3): 67-74.

【作者简介】

张创基（1983—），男，广东揭阳人，硕士，副教授，研究方向：计算机网络安全、大数据等。

林伟烜（1983—），女，广东汕头人，硕士，副研究员，研究方向：软件设计、数据库、大数据分析与应用。

许景民（1993—），男，广东茂名人，本科，助教，研究方向：计算机网络安全、计算机应用等。

（收稿日期：2024-11-07）