2022 第二届亚太通信技术与计算机科学会议(ACCTCS) - 978-1-6654-0034-3/22/$31.00©2022 IEEE - DOI: 10.1

基于人工智能技术的学生实名数据信息处理在网络安全中的应用

河海大学马克思
主义学院叶文彦
江苏南京，211100
1063540541 @qq.com

摘要:随着网络技术以及科学技术的不断发展，人工智能技术及其相关的科技应用，在这个过程中诞生了。其中，人工智能技术在信息检测和数据处理中得到了广泛的应用，一直是当前的研究热点之一。 近年来，人工智能的研究主要集中在数据的网络安全处理、故障诊断和异常检测等方面的应用。本文针对学生实名数据的网络安全检测，分析了相关的人工智能技术并构建了模型。在此过程中，本文首先介绍并分析了聚类算法和均值算法的一些不足，然后提出了一种克隆算法来获得全局最优解。在此基础上，构建了基于信任原理和信任模型的学生实名数据信息处理网络安全模型。

关键词:人工智能，网络安全，学生实名数据，数据处理

I. 介绍

A. 基于人工智能技术的学生数据网络安全管理综述

人工智能技术作为计算机科学的前沿分支，在互联网大数据背景下引起了广泛关注。目前国内人工智能技术的主要研究方向是将人工智能与网络安全相结合，有效管理网络信息，防止信息丢失。在此过程中使用的主要技术包括机器学习、数据挖掘、计算机技术、计算机管理系统和网络服务器系统。

目前该领域的主要研究方向是将数据聚类与网络安全相结合。因此，从本质上讲，本文主要致力于研究人工智能在网络安全中的应用，其目的是寻找一种将人工智能与数据聚类相结合的技术，并以一种非常有效的方式进行研究。

入侵检测系统可以识别和拦截来自内部和外部的攻击，从而保护网络安全，是目前最常用的网络安全防护系统

978-1-6654-0034-3/22/$31.00©2022 ieee 314

系统实时运行。另外，上述方法一般称为误用检测方法这样，通过收集和统计网络安全过程中的相关数据，可以发现系统的异常行为，从而检测网络安全和系统攻击的情况。此外，作为国内研究的主要方向，目前入侵检测系统通常是利用已建立的正常服务器和用户之间的相关数据来制定异常活动数据表，目的是为了及时有效地判断系统的攻击情况。

B. 基于模糊聚类的异常数据检测算法综述

到目前为止，入侵系统的数据输入检测的检测方法，一般来说，通常是发挥优势的。此外，这种检测方法效率低，容易出现误报，适应性差。而且不适合当前数据量大的网络。因此，需要一种新的网络安全系统，对学生的实名数据进行有效的管理和防范[1]。

聚类算法一般用于多变量分析。这种统计方法通过寻找数据之间的相似性，有效地对数据进行分类，形成一个接一个相邻的数字数据集。此外，这类学习方法通常利用观察学习方法对数据样本进行学习和训练，可以在数据集中推导出相应的规则，对聚类问题进行分类，并将其转化为优化问题[2]。

通常，聚类分析使用模式分析对数据进行分类，这种分类包括两种类型，一种是有监督的，另一种是无监督的。一方面，监督分析通常对已知数据进行分析，分析数据的所有属性。另一方面，无监督分析方法通常使用聚类方法将数据集划分为簇，从而识别它们之间的紧密程度[3]。总而言之，这种分类方法的优点是不需要先验知识，因此需要较少的学习样本，应用范围广。同时，几种模糊聚类方法及其比较关系如下图 1 所示。

DOI 10.1109 / ACCTCS53867.2022.00071

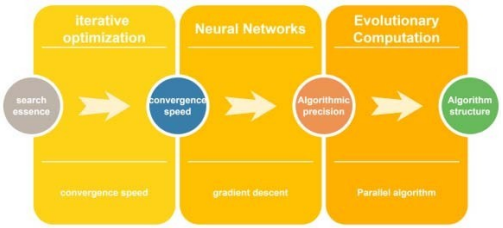

图 1 所示。模糊聚类方法的关系与比较

C. 基于模糊聚类的异常数据检测算法研究

目前所使用的聚类方法通常对数据进行硬划分，这种硬划分方法具有较高的算法效率，但其分类方法比较死板，不能灵活地对数据进行划分，容易导致数据分类错误[4]。目前使用的模糊聚类方法可以在数据类别之间产生有效的联系。而且，该聚类方法的优化效果始终优于上述方法，但其缺点也十分明显。在聚类过程中，有些数据集是交叉的，很难区分交叉的数据集，因此需要有待进一步优化。

II. 学生实名数据信息处理的聚类模型

A. 聚类分析过程

在数据集分类的过程中，首先为数据样本定义样本。在定义样本集的过程中，主要是通过样本集的特征进行相应的赋值。赋值过程主要是用特征值来表示该数据在对应矩阵中的位置，来标记对应的子集，数据特征值的识别过程如下。

$$X1,\ \upsilon X2)\upsilon \quad \cdots \text{xk} = X;\ Xi\nu X = \text{j} \neg \Sigma,\ 1\sigma\ i\Sigma\ j\ \ k \tag{1}$$

数据分类后，对不相交的子集进行划分
通过聚类分析得出隶属关系，从而建立映射关系。流程如下。

$$\text{西}\quad xl \quad 1 \quad xl\xi\chi \quad il)=\mu \quad , \quad xl\xi\sigma \tag{2}$$

映射关系建立后，隶属函数中的子集为非空子集，对非空子集进行识别。另外，一般将这种方法称为硬划分，它在聚类过程中，证明了第一步。在除法过程中，对单位数据中的矩阵定义单位矢量，从而选择其矢量方向。取值方法如下。

$$Mh = \text{i}\{\mu\text{il}\ \mu_l\ \chi\{0,1\};\text{Jl}\ 1,\ \Sigma\mu 1;\ Jl = 61,\ <1\Sigma\mu<6\} \tag{3}$$

在模糊聚类过程中，通过划分样本集，将学生实名数据划分为多个样本。这些样本集之间存在从属关系，其从属关系如上式[5]所示。此外，这些数据集被证明具有特定的意义，并根据适当的定义进行划分。对于这些数据集的度量，通常使用它们之间的欧几里得距离来表示数据的互易程度。具体表示如下:

$$h = .\{\mu_j\ \chi.\ \text{M}.\quad \text{零}\{0,1\},\chi\text{我} \tag{4}$$

为了保证聚类算法的可靠性和准确性，通常对分割后的数据进行数据最小化处理。该处理方法可以计算和构造数据样本的失真，从而对模糊区域的函数进行处理。在此基础上，对目标函数进行优化，使优化算法能够作用于聚类模式。最优聚类优化方法如下:

$$M=[0,1];\text{Jl}\{\mu\ 1,\ \mu_{l;}\ \chi\text{Jl} \quad \sum \tag{5}$$

经过上述计算过程，可以将数据划分为子集。此外，在此基础上，可以对数据集进行进一步的详细分析和处理。

B. 学生实名数据克隆的选择过程

克隆数据算法最初被提出时，主要用于群体搜索。在后期的应用过程中，由于克隆算子的选择和通过群体优化策略，本质上也可以进行并行算法处理和搜索范围处理，因此也用于全局优化算法的计算[6]。

因此，在本文的研究过程中，将克隆选择算法应用到网络安全中，以确保其对聚类算法起到补充作用
在网络过程中对学生实名数据进行安全处理，使其在大容量数据输入过程中能够保持稳定运行。具体流程如下面的图 2 所示。

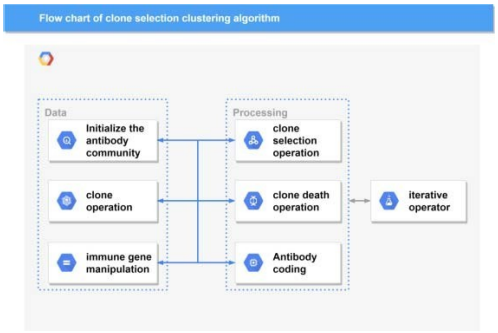

图 2。克隆选择模糊聚类算法流程图

克隆算法的具体过程为

上面了。首先，通过划分数据集的抗体群落，可以计算出初始亲和力。此外，使用不同的亲和度对数据集进行聚类。此外，在此基础上，设置抗体的克隆尺度，并计算克隆算子，得到 next
代人口数据集[7]。最后，在此基础上
克隆算子的概率序列由式计算
计算马尔可夫链。该过程如上所示。

C. 基于克隆选择的模糊聚类算法模型的建立

通过分析前一节中的克隆算法及其在网络安全模型中对学生实名数据处理的应用，具体

给出了基于克隆选择的模糊聚类算法的实现过程。此外克隆选择模糊算法的建立过程主要通过将聚类问题解码为抗体问题来证明[8]。此外，测量并构建抗体亲和函数从而对聚类问题项进行表征[9]。在这个过程中，

对聚类算子的选择和操作参数的选择进行了研究。

III. 基于改进的学生实名数据信息处理网络安全模型

证据组合

A. 证据组合规则模型的建立

在建立证据选择模型的过程中，主要是用来定义数据的近似算法。在这个过程中，目的被证明是在数据被证明不确定的情况下产生有效的信息推理[10]。该算法一般用于证据和信息数据的融合和泛化。

B. 信任模型的建立

在证据数据合成的过程中，会产生一定数量的错误数据。因此，在
证据理论的过程中，通常是可信度分析
进行数据分析的人。在此基础上，a
设置一组可能的结果来分析和表示信任

模型。

首先，构建并定义了学生实名数据信息的信任函数。通过
对识别框架、领域进行了定义，从而

定义一个有效的信任函数，如下所示。

$$m(XY)\ 1\ \underline{m}(X)m=\frac{(Y)}{2_{12}} \quad (6)$$

经过上述定义，通过定义和计算自然函数，可以计算出数据中兼容性的基本可靠度，如下所示。

$$mX(^{Y})1=\frac{1\ 米(X)}{2m(X)\ m+(Y)\ 12}=\frac{1\{米(X)2\ 米(Y)\}}{2m\ (X)\ m+\ (Y)} \quad (7)$$

在计算过程中，自然函数与可靠度函数的关系如下:

$$\text{☎}\quad x)=2_{1}=\frac{2}{} \quad (8)$$

在计算过程中，一般会涉及到信任区间的计算。信任区间的度量用下式来说明。

$$米(XY)=-\quad m\ (X)m\ (Y)\ 12+\frac{1\ m\ \Omega\ \text{❀}^{2}}{2\ 1\ 2m\ (Y)\ 2m+\ (Y)} \quad (9)$$

数据集中的信任区间通常由命题的重要信息给出。在给定的过程中，涉及到数据集的特征值。命名过程如下图所示。

$$mX(^{Y})=\frac{1\{米(X)2\ 米(Y)\}}{2m1\ (X)\ 2m2\ +(Y)} \quad (10)$$

在证据组合过程中，数据通常用信任来表示。在表示过程中，通过冲突证据发现数据的弱点，从而判断网络的安全性。定义过程如下式所示。

$$m\ \text{☎}\ 0 \quad (11)$$

$$m(XY)\ 0=(12)$$

在此过程中，信任数据一般采用组合规则表示。组合规则的信任程度计算公式如下:

$$mX(^{Y})1=\frac{m\ (X)\qquad \text{❀}m\ (X)\ \}_{2m}\ (Y)}{m\ (X)\ +m\ (Y)\ 12\qquad m\ (X)\ +m\ (Y)} \quad (13)$$

$$X()=\frac{m2(Y)m\ (X)m\ (Y)\ m1(X)m2(Y)=\{\}^{2}}{m\ (X)\ +m\ (Y)\ 12\qquad m\ (X)\ +m\ (Y)} \quad (14)$$

C. 基于改进证据组合的网络安全信任模型结构

改进的网络安全信任模型主要是

通过 P2P 网络进行开发和仿真。此外，该网络的主要方法是对数据的信任程度进行分析。在此过程中，利用信任管理机制对数据进行分类和判断，从而将网络服务与信息安全相结合
处理。的具体过程进行了演示

下面的图 3。

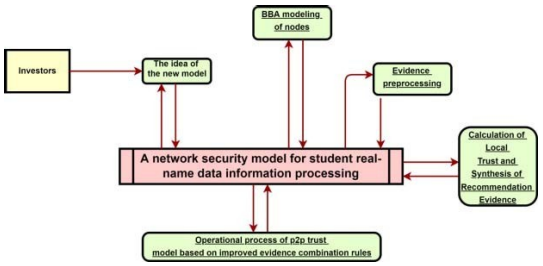

图 3。基于改进证据组合的学生实名数据信息处理网络安全模型框架

本文主要研究人工智能技术。在此基础上，通过分析人工智能技术在聚类分析过程中的应用，得出如何对学生实名数据进行聚类。在此基础上，本文分析了上述方法的优缺点，指出了它们的相关不足，并提出了数据克隆算法的推导方法。经过以上分析，本文构建了人工智能技术学生网络安全实名数据信息模型的相关内容。本文通过这种方式对该方向提出了一些展望，为其他研究者提供了一些研究思路，未来该方向的内容主要是网络安全。

随着互联网技术的不断升级和扩展，网络空间的发展已经变得非常丰富。人工智能的出现，使网络空间更加灵活，空间结构向着更加智能化、复杂化的方向发展。结合人工智能技术对人类思维的模拟能力及其对大数据的强大学习能力，从人工智能技术在网络空间安全防御中的应用成果来看，可以更好地将人工智能技术与安全防御技术灵活结合。弥补传统网络空间安全防御的不足。人工智能是社会发展和技术创新的产物，是推动人类进步的重要技术形式。人工智能发展以来，已成为新一轮科技革命和产业变革的核心动力，正在深刻影响世界经济、社会进步和人民生活。在世界经济中，人工智能是引领未来的战略性技术。世界主要国家和地区将发展人工智能作为提升国家竞争力、促进国民经济增长的重大战略;在社会进步方面，人工智能技术为社会治理提供了新的技术和思路。人工智能在社会治理中的应用，是降低治理成本、提高治理效率、减少治理干扰最直接有效的途径。在日常生活中，深度学习、图像识别以及 AI、语音识别等人工智能技术已经广泛应用于智能终端、智能家居、移动支付等领域。未来，人工智能技术将在教育、医疗、旅游等与人们生活密切相关的领域发挥更加显著的作用。为普通民众提供覆盖面更广、体验更好、便利性更好的生活服务。

IV. 结论

总之，随着互联网技术的快速发展和网络空间的扩大，世界各国之间的距离越来越近。同时，各种人工智能的出现丰富了网络空间，弥补了现实空间的不足。但也推动了网络空间结构向多元化、智能化方向发展，这一趋势更加复杂。毫无疑问，作为社会发展和技术创新的产物，人工智能技术的出现直接推动了全球人类文明的进步。本文提出了一种基于人工智能技术的学生实名数据信息模型，将聚类分析和数据克隆算法相结合，大大提高了学生实名数据信息系统的可行性、有效性和准确性。

参考文献

[1] N. Ahmad, U. A. Mokhtar, j . Fariza . Paizi . Fauzi, Z. A. Othman, Y. Hakim Yeop, S. N. Huda Sheikh Abdullah，“网络安全情境意识在家长中的应用”，2018 年网络弹性会议(CRC)，布城，马来西亚，2018，页 1-3。

[2] k . Bhat;诉 Sundarraj;美国 Sinha;A. Kaul，“IEEE 智能电网的网络安全”，载于《IEEE 智能电网网络安全》vol.， no. 1。， pp.1-122, 2013 年 9 月 16 日，doi: 10.1109 / IEEESTD.2013.6613505。

[3] 张新民，吴文良，张新民，吴文良，“基于隐马尔可夫模型的高速网络安全大数据”，2017 年第 13 届国际自然计算、模糊系统与知识发现会议(ICNC-FSKD)，中国桂林，2017,pp. 2080-2083。

[4] 王志强，“基于网络绩效指标的网络安全投资回报研究”，中国计算机科学，2019，第 4 期，第 1-8 页。

[5] F. Skopik 和 S. Filip，“国家网络安全传感器网络的设计原则”; 小规模示威的经验教训，”2019 年网络安全和数字服务保护国际会议(网络安全)，牛津，英国，2019，第 1-8 页。

[6] E. Kritzinger 和 S. von Solms，“家庭用户安全——从面向安全的家庭用户到面向安全的家庭用户”，2013 年科学与信息会议，伦敦，2013,pp. 340-345。

[7] M. Frank, M. Leitner 和 T. Pahi，“网络安全测试平台的设计考虑:教育网络安全测试平台的案例研究，“2017 IEEE 第 15 届可靠、自主和安全计算国际会议，第 15 届普适智能与计算国际会议，第 3 届大数据智能与计算国际会议与网络科学技术大会(DASC/PiCom/DataCom/ cybersciitech)，奥兰多，佛罗里达州，2017,pp 38-46。

[8] T. M. Mbelli 和 B. Dwolatzky，“网络安全，对南非网络银行的威胁; 网络与应用安全方法，”2016 IEEE 第三届网络安全和云计算国际会议(CSCloud)，北京，中国，2016,pp 1-6。

[9] K. N. Sevis 和 E. Seker，“网络战争:术语、问题、法律和争议”，2016 年网络安全与数字服务保护国际会议(网络安全)，伦敦，英国，2016，第 1-9 页。

[10] M. Swann, J. Rose, G. Bendiab, S. Shiaeles 和 F. Li，“开源和商业捕获旗帜网络安全学习平台”
——一个案例研究，”2021 年 IEEE 网络安全和弹性国际会议(CSR)，罗德，希腊，2021 年，第 198-205 页。