教师也可以将往届学生做得较成功的案例分享出来供学生进行开源。这样既启发了学生的思维，也培养了学生沟通能力，同时还开阔了学生的视野。

2.5 明确行业标准，培养良好的编程习惯

对于一个C开发者来说，良好的程序设计风格尤其重要。良好的编程习惯应该从第一节课开始培养。因此，教师在授课过程中要以软件工程的标准要求，比如：注释标记的使用、程序的段落缩进间距，程序嵌套顺序、代码书写习惯、语义明确的命名等方面的专业规范，使得学生在初学阶段就养成良好的设计风格。

2.6 充分利用网络资源，扩宽知识学习面

当今是知识爆炸的时代，各类网络资源丰富多彩，教师授课不应停留在自己的课件上。既要合理利用多媒体课件，更要利用网络进行线上学习，充分共享各类精品课程、慕课、微课、金课等优质网络资源，最大化扩宽学生学习面。

3　加强交流，深化教学改革

本课题所研究学院是一个校企合作的二级学院，学院非常重视C语言程序设计这门课程，多个专业把该课程安排在大一上学期，目的是让新生认知编程、训练学生的逻辑思维能力，提升专业课学习兴趣。为此，本课程成立了“C语言课程建设团队”，该团队开展了诸多教学活动：集体制定课程标准、集中备课；专兼教师共同参与同课异构讲课竞赛活动；相互听课评课、交流教学心得；申报为精品课程、制定金课建设计划等。

通过这些活动，既开阔了师生的眼界，也使得教师把握着教改前沿，对提高教学质量是显而易见的。

4　结论

教学改革与课程改革相辅相成，UBL人才培养模式能有效促进改革。UBL理念贯穿整个C语言教学过程使得教学目标更明确、人才培养路线更精准，其目标在于培养学生的编程规范与可迁移能力，以便让学生更好地掌握的学习方法。

时代在变、教学环境中的参与者也在变，作为教师，都应义不容辞地参与到教学改革中去，积极发挥驱动作用。

参考文献：

[1]tiobe 2019 年 12 月编程语言排行榜 https://www.tiobe.com/tiobe-index[DB/OL]，2019,12.

[2]王重英. C 语言程序设计教学改革与实践[J]. 软件，2012（5）.

[3]罗恺韵，等. 基于翻转课堂的 C 语言程序设计课程教学模式改革研究[J]. 课程教育研究，2019（46）：1-4，60.

[4]彭琼，等. 基于微课的“高级语言程序设计”教学模式改革研究[J]. 微型电脑应用，2018（12）.

基于人工智能的校园网络安全探索与研究

◆廖彬

（福州大学网络安全与信息化办公室　福建　350108）

摘要：本文针对校园网络安全问题提出了人工智能的解决策略，如：网络的防火墙配置对策、基于用户权限的管理等。本文还通过人工智能来判断防火墙政策规则的新增、删除及规则顺序调整的动作，作为调整防火墙政策规则的参考，保持防火墙系统维持较佳状态。

关键词：校园网络；网络安全；人工智能

1　引言

在大学校园电子化发达的情形下，使得原本传统的纸本作业以数字化的方式被处理及传递，虽然带来了便利，但也同时隐含着许多风险，例如含有机敏性及个人隐私的数据在公开的网络上遭窃取、或伪冒身份从事不当行为、瘫痪系统网络导致造成损失等，种种的网络安全事件已频传在政府、企业等单位，甚至在单纯校园里也难以幸免，虽然学校是以学术研究及培育人才为目的，对于入侵者来说不如政府机关拥有国家机密、企业有着商业机密来得有诱因，但也不可掉以轻心，因为在信息应用普及下，学校的行政流程以及学生的教学互动等作业大量依赖计算机系统的运作，同时伴随网络上种种越权存取(unauthenticated access)、入侵(cracking)、计算机犯罪(computer crime)的新挑战，在本研究中，针对人工智能对校园信息安全处理对策进行探讨。

2　AI 在网络安全中的应用场景

2.1　AI 网络安全分场景建设主要采用技术

AI 网络安全场景建设方面，可基于大数据做大安全。基于机器学习、深度学习算法的人工智能安全分析引擎，能够更好地处理模糊、非线性、海量数据，通过对不同数据类型的大量数据进行聚合、分类、序列化，有效检测识别各类网络安全威胁，大大提升安全检测效率、精准度和自动化程度。人工智能技术可对各种网络安全要素数据进行归并、关联分析、融合处理，通过大量安全风险数据进行关联性安全态势分析，综合分析网络安全要素，评估网络安全状况，预测其发展趋势，进而构建智能化网络安全威胁态势感知体系。

2.2　AI 网络安全分场景

在网络入侵检测方面。入侵检测技术是利用各种手段方式，对异常网络流量等数据进行收集、筛选、处理，自动生成安全报告提供给用户，如 DDoS 检测、僵尸网络检测。

在预测性恶意软件防御方面。预测性恶意软件防御技术通过使用机器学习和统计模型，寻找恶意软件家族特征，预测进化方向，提前进行防御。包括智能防病毒网关、智能 Web 应用防火墙、智能防火墙、智能网络流量分析等。

在网络安全动态感知方面，包括网络安全预警通报、网络系统安全风险自评估、网络安全自动化运营等，网络安全态势感知技术利用数据融合、人工智能、智能分析和可视化等技术，直观显示、预测网络安全态势，为网络安全预警防护提供保障，可在不断的自学习过程中提高系统的防御水平。

此外，人工智能技术在网络安全运营管理、网络系统安全风险自评估及物联网安全问题上多有应用。

3　基于人工智能的网络安全防御策略

近年来有部分研究运用防火墙日志记录进行分析，尝试运用人工智能技术来找出隐含于防火墙日志记录的规则，进而提供管理者作为加入或更新防火墙政策规则的参考，以提升防火墙的效率。本研究所提出防火墙规则自动更新方法流程如图 1 所示，主要可以分为四个步骤，依次为：数据前处理、关联规则挖掘、改变挖掘及防火墙政策规则评估。

关联规则与防火墙政策规则的整合评估流程如图 1 所示。经由数据挖掘，可以得到新兴样式、新增样式及消失样式等三种不同样式的关联规则。其次，不同样式的关联规则再与现存的防火墙政策规则（或称原规则表）进行比较与整合。本研究根据防火墙系统运作的特性，最终比对不到规则的封包都将会拒绝（Deny），而原本允许（Allow）的记录则表示这些规则已存在于现行防火墙政策规

则表中，最后通过调整允许规则及新增、删除拒绝规则来持续提升并保持防火墙系统的效率。

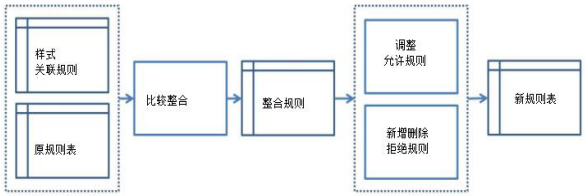

图 1 防火墙政策规则整合流程图

本研究的防火墙政策调整动作原则如表 1 所示，此表汇整出任何两个时间点所产生的关联规则比对表，符合该表的特征即执行后续相关动作。例如：在连续两周所挖掘出来的拒绝关联规则符合新兴样式（即支持度增加），就将此结果通知管理人员并且建议可将该笔拒绝类型的关联规则加入防火墙政策规则中。同样地，在连续两个月所挖掘出来的允许类型的关联规则符合新兴样式（即支持度增加），而且此规则已经存在现有规则表中，即可建议管理人员调整此笔允许类型关联规则的优先比对顺序，使得防火墙系统运作更有效率。

表 1 各种类型规则的执行动作

No	关联规则类型	样式	现有防火墙规则表	防火墙政策调整动作
1	允许	新增样式	有	维持现状
2	允许	新增样式	无	Not Available
3	允许	消灭样式	有	维持现状
4	允许	消灭样式	无	Not Available
5	允许	新增样式	有	依据支持度调整政策顺序
6	允许	新增样式	无	Not Available
7	拒绝	新增样式	有	维持现状
8	拒绝	新增样式	无	维持现状
9	拒绝	消灭样式	有	评估为删除规则
10	拒绝	消灭样式	无	维持现状
11	拒绝	新增样式	有	依据支持度调整政策顺序
12	拒绝	新增样式	无	加入规则

*Not Available：不可能出现的情况。

*若规则不属于上述类型的规则，则维持现状（对现有防火墙规则表不做任何异动）。

由于防火墙运采用正面表列的方式，若封包与现有防火墙规则表中的规则都比对不到的话，就会拒绝该封包存取。各种规则类型的执行动作详细描述如下：

（1）因为该规则既然已经存在现有防火墙规则表（有），而且关联规则类型属于允许，故对现有防火墙规则表不做任何异动，即维持现状。

（2）因为该规则既然未存在现有防火墙规则表（无），代表不可能有任何封包因为该规则而通过防火墙（即不可能出现此规则），故此状况属于 NotAvailable。

（3）因为该规则既然已经存在现有防火墙规则表（有），而且关联规则类型属于允许，故对现有防火墙规则表不做任何异动，即维持现状。

（4）因为该规则既然未存在现有防火墙规则表（无），代表不可能有任何封包因为符合该规则而通过防火墙（即不可能出现此规则），故此状况属于 NotAvailable。

（5）因为该规则属于 Emerging（即规则的支持度大幅增加），代表符合此规则的封包将大幅增加，为了让封包与防火墙规则的比对次数减少。因此，将调整该规则在防火墙规则表中的先后顺序，即该规则的顺序往前调整，让此符合此规则的封包尽快通过，以降低封包的比对次数。

（6）因为该规则既然未存在现有防火墙规则表（无），代表不可能有任何封包因为符合该规则而通过防火墙（即不可能出现此规则），故此状况属于 NotAvailable。

（7）因为该规则既然已经存在现有防火墙规则表（有），而且关联规则类型属于拒绝，故对现有防火墙规则表不做任何异动，即维持现状。

（8）因为该规则既然未存在现有防火墙规则表（无），而且关联规则类型属于拒绝，故对现有防火墙规则表不做任何异动，即维持现状。

（9）因为该规则属于 Perished（即规则的支持度低于最小支持度门槛值），代表符合此规则的封包已经大量减少或消失，为了让封包与防火墙规则的比对次数减少。因此，可以评估将该规则从防火墙规则表中删除，以降低封包的比对次数。

（10）因为该规则既然未存在现有防火墙规则表（无），而且关联规则类型属于拒绝，故对现有防火墙规则表不做任何异动，即维持现状。

（11）因为该规则属于 Emerging（即规则的支持度大幅增加），代表符合此规则的封包将大幅增加，为了让封包与防火墙规则的比对次数减少。因此，将调整该规则在防火墙规则表中的先后顺序，即该规则的顺序往前调整，让此符合此规则的封包尽快拒绝，以降低封包的比对次数。

（12）因为该规则既然未存在现有防火墙规则表（无），然而该规则属于 Emerging（即规则的支持度大幅增加），代表符合此规则的封包将大幅增加，为了让封包与防火墙规则的比对次数减少，故防火墙规则表中应加入此规则，让此符合此规则的封包尽快拒绝，以降低封包的比对次数。

本研究尝试整合关联规则挖掘及改变挖掘等技术，提出基于人工智能的防火墙规则自动更新方法。首先挖掘出关联规则，进而运用改变挖掘技术分辨出新兴样式、新增样式及消失样式等 3 种不同样式的关联规则。最后，将具有不同样式的关联规则运用于防火墙政策规则的调整，进而提升防火墙效率。实验结果也证实基于人工智能的防火墙规则自动更新方法的效果优于原始规则表及 Apriori 方法，同样的网络攻击方法，本文提出的方法可以比原来的方法甄别效率提高一倍，效果提高一倍。

4 总结

本文以解决校园网络信息安全问题的角度开发出分析人工智能在网络信息安全中的应用，协助管理人员可以快速地完成侦测网络攻击和异常。本文以解决部门信息安全问题的角度分析人工智能在网络信息安全中的应用，协助管理人员可以快速地完成网络攻击和异常。本文所开发的网络安全管理系统不但可以节省网络管理员的管理时间，还可以提高管理效率。而当面临如目标式攻击此类需要长时间且大量的数据以进行分析时，传统的关联式数据库无法处理如此巨量数据，因此，本研究利用人工智能技术以解决此问题，而实验证明本研究所设计的系统大幅提升解决巨量记录文件分析效率的问题。

参考文献：

[1]王兴国.企业网安全管理问题与策略研究[J]. 辽宁行政学院学报，2015（05）：23-25.

[2]陈坚.校园网络安全问题分析及解决方案设计[D]. 长春工业大学，2016：23-26.

[3]崔孝林.网络安全评估系统的设计与实现[D]. 中国科学技术大学，2019：56-59.

[3]李江涛.基于行为的病毒检测系统的设计与实现[D]. 北京交通大学，2018：90-92.