数据挖掘技术在深度防御网络安全体系分析

夏江丽

中国移动通信集团江西有限公司　江西　南昌　330000

[摘　要]目前，身处在信息时代下，各个行业在发展的过程当中都无法脱离来自于信息技术方面的支持，能够实现工作效率的提高，对我国经济发展速度的加快有着较大的推动作用。网络安全一直以来成为民众所关注的重点问题。所以，在现阶段，应该对数据挖掘技术进行运用，将技术在深度防御网络安全体系中的价值进行突出，从而让网络安全系数得到大幅度提高。

[关键词]数据挖掘技术；深度防御；网络安全体系

【DOI】10.12252/j.issn.2096-6288.2020.02.1779

前言

伴随着互联网高速发展，网络逐渐的进入到人们的视野、工作、娱乐和生活当中，但网络本身的安全性与开放性是矛盾体，由于互联网本身具备着不设防、无主管等特点，为人们带来诸多便利的同时也会导致安全问题尤为突出。所以，在现阶段，在深度防御网络安全体系当中可以尝试着对数据挖掘技术进行运用。从而让安全系统的作用得到发挥，保障信息更加具备机密性和完整性。

一、数据挖掘技术的具体内容及应用方式

（一）具体内容

在现阶段，伴随着信息技术高速发展，大数据逐渐的成为社会发展所关注的重点和焦点。无论是学术界、商业、工业还是政府工作和基层工作的开展都广泛受到来自于大数据的洗礼，能够从海量数据当中运用挖掘技术对最为有利和有价值的数据进行获取，提高工作效率，已经成为行业发展必然趋势。针对于数据挖掘技术，其核心在于对有价值的数据和信息进行挖掘，并不是硬件软件的堆砌。在现阶段，信息的呈现已经呈现出爆发式的姿态，而从技术角度出发，数据挖掘技术能够从大量模糊和不确定性的应用数据当中对有价值内容进行提取，对信息潜在价值进行发挥，是十分重要的技术内容。

（二）应用方式

针对于数据挖掘这一技术从整体上看可以划分成两类，一类是对内容的有效挖掘；另一类别则是对记录挖掘的使用[1]。内容挖掘工作主要就是指相关个人或企业通过技术的运用能够在丰富资源当中找寻到对自身发展有利或者对企业整体发展有利的数据资源，并且需要后台设置监控程序，对内容进行保护，避免数据挖掘中出现数据信息丢失、泄露等情况。而记录挖掘工作主要是指，对数据挖掘过程当中的操作记录进行获取，便于对网络信息安全方面的核查检查，从而更好的让网络信息得到监控，让安全系数得以提高，让攻击风险得到降低。

二、数据挖掘技术在深度防御网络安全体系的运用优势

（一）实现动态防护

在传统模式下，安全技术主要用于系统防护和加固。但由于攻击层出不穷，防护重点也需要得到转变，从原本静态防护逐渐过渡到动态防护[2]。在现阶段，通过数据挖掘技术的有效运用就能够让静态防护朝着动态防护不断转变，为系统响应及恢复提供有效依据。技术的运用能够做到日常防御、设施防御、基础设施，具备较强可扩展性，从而真正的实现动态防护。

（二）满足安全需要

在现阶段，伴随网络规模持续扩大，网络用户群体持续增加，网络安全逐渐面临着更加复杂和严峻的挑战。为了更好的满足需要，对深度性防御体系进行构建就可以对数据挖掘技术进行良好的运用，能够使得防御体系朝着开放式、操作式方向持续发展。从而真正的打破传统的制约性，让防御的效率和有效性得到良好的提高，让技术优势和价值得到最大化的发挥。

（三）发挥技术优势

新时期下，各类攻击技术层出不穷，攻击形式、数量也在与日俱增[3]。通过数据挖掘技术的良好运用能够更好的展开防护效力，真正的在深度防御体系中对挖掘技术的作用进行展现。在面临海量信息时能够快速对有效信息进行补充和挖掘，带动预防能力的提高，真正的做到深度防御，在无形当中突显技术的优势和价值，让网络安全得到最大化的保障。

三、数据挖掘技术在深度防御网络安全体系的运用对策

（一）数据挖掘技术在“数据收集”中的运用

在深度防御体系当中，数据挖掘技术最大的优势和价值就是能够对数据价值进行快速挖掘和找寻，该技术是现代智能化系统技术和理论的重点研究内容，能够在面临海量数据时对隐含和有价值的数据和知识进行快速挖掘。在挖掘的过程当中能够实现收集、预处理、特征筛选、挖掘、表达及理解以及知识有效运用等等。所以，在现阶段，应该在技术运用的过程当中立足数据挖掘功能的发挥，让技术价值得到展现。

例如，在收集数据阶段，首先应该对研究对象各类数据加以收集；在预处理时可以根据对象优化要求和建模，加强数据分类、定性描述和格式规划处理，做到数据去噪；在筛选特征时应该对信息特征进行去除，有效的实行数据降维，让知识理解性变得更强；在挖掘阶段应该运用数据库，挖掘显示和算法来对知识进行获取和挖掘；在表达和理解阶段应该对知识表达形式进行挖掘，并在此基础上借助人机交互验证和显示；在知识应用阶段可以对知识库当中的LPS进行有效管理，实现控制，对分支行为进行分散监控，使得系统效能

得到最大化的发挥，让整个系统更加具备防御能力，让系统优势得以突出。

（二）数据挖掘技术在“算法模型”中的运用

将大数据和网络安全作为基础，也可以将数据挖掘技术有效的融合在算法模型的应用和构建当中，能够真正的实现对系统的控制，达到理想中最佳的技术运用效果。在其中，可以对运行模型进行构建，让网络安全得到保障[4]。

例如，可以在技术支持下对模拟神经网络这一模式进行使用来实现算法模型的构建。如，可以将大数据作为支持对网络环境当中信息加以分析。在面临庞大数量的数据时可以对最新分析模式进行使用，对数据加以追溯，实现模型构建。在构建模型时可以结合环境中潜在风险对风险性加预判，假如网络环境相关程序已经遭受到病毒感染并引发安全问题，如信息、程序丢失等等，那么在框架构建时应该对应对措施进行合理采取，规避安全问题带来的影响。在安全控制系统构建时应该让程序得以分层运行，有效拆分数据库，对子数据集合进行形成，立足程序框架整体配合，保障任务功能得到高效控制和发挥。从而在面对风险时能够做到高效预判，并结合风险等级和风险特征对安全控制框架进行合理构架，使得数据库间发挥交换作用，实现数据库的创新，降低环境中可能存在的安全风险，保障运行程序能时时刻刻处在安全层面。

（三）数据挖掘技术在“入侵检测”中的运用

在安全系统当中，入侵检测是十分重要的一个组成部分，能够对滥用资源、未经允许随意运用资源的行为进行有效的检测和预防，保障信息更加具备完整性以及机密性，防止信息资源泄露等情况的出现。所以，在现阶段，也应该将数据挖掘技术有效的融合在入侵检测当中，达到理想中最佳的技术运用效果。

例如，在现阶段，通过数据挖掘技术的有效运用能够针对于互联网内的审计记录加以分析，从中对未知、隐含、潜在的有价值的数据和信息进行挖掘。结合信息对异常入侵以及已知入侵进行有效的检测，从而更好的让入侵检测的效率和质量得到提高。在这其中，可以对人工免疫这一挖掘新型方法进行运用，主要由生物免疫所获得启示逐渐发展，能够实现动态学习、自我监控、自适应和计算。从而真正的让传统陈旧技术当中的问题和缺陷得到克服，适应环境变化，实现动态管控，对于未知攻击也能够做到实时防御。从而为网络当前异常入侵检测提供全新方法和思路，需要在现阶段有效的对技术价值进行发挥，让入侵检测的效果变得更好。

（四）数据挖掘技术在“控制系统”中的运用

数据挖掘技术的有效运用，能够更好的在控制系统中展现技术价值和作用。所以，在现阶段，也应该对技术优势不断进行挖掘，让整个完善性控制系统的整体框架得到构建。

例如，在框架构建的过程当中首先应该规避各功能层间程序可能出现的冲突，可以对误差补偿这一方法进行采用，实现各部分相关框架的整体构建。在这其中，可以对数据挖掘技术进行良好运用，对于网络系统中可能遭遇的一些问题和风险进行良好的模拟，在此基础上对针对性较强的技术结构进行设计，让控制系统框架变得更加完善。特别是网络领域中变化比较频繁的一些隐患，应该对保护技术进行合理提高，对应用起点、终点、服务边界进行明确，让控制结构更加科学合理。这样就能够立足网络环境及时在面临威胁情报时加以收集、控制及处理，并且能够实现技术框架自动更新，对风险有效应对和预防，使得技术优势得到突出。此外，该技术也能够对网络现存风险有效的应对和预防，对技术融合进行落实，使得安全控制系统的价值得到发挥，能够自动获取并对网络环境进行更新，让数据库得到优化和构建。

（五）数据挖掘技术在“离线状态”中的运用

除了以上这几个方面，在数据挖掘技术运用的过程当中也可以将其利用在离线状态下。为了让系统运行更加具备安全性，处在离线状态时也应该提高控制能力。所以，就可以对技术进行运用，对技术的内在潜能充分的进行发挥。

例如，当整个系统处在离线状态时，对风险进行有效的控制也是安全设计当中十分重要的一项内容。相关工作人员应该在程序计算的过程当中对相应系统进行设置，保障计算机虽然处在离线状态但依旧可以对系统实际情况进行安全检测，可以在离线状态时对安全控制相关功能进行发挥，对数据库进行自动启动。一旦系统与网络之间断开可以对备用数据库进行启动，对参数进行观察和对比。在脱离网络连接下也能够对数据库的价值进行发挥，一旦参数出现异常，就表明内部可能存在一定的威胁和风险，对风险及问题加以识别。此外，应该加强安全管控系统的构建，当网络和系统之间断开后计算机的内部会对独立性控制系统进行启动，更好地对运行环境加以检测，对数据间的差异进行检测，及时发现病毒隐患，达到理想中技术运用效果。

结论

总之，在新时期的背景下，为了实现深度防御，让网络安全得到良好保障，对数据挖掘技术的具体内容、应用方式、应用优势和运用对策进行明确是尤为必要和关键的。在这其中，主要可以通过技术在数据收集、算法模型、入侵检测、控制系统、离线状态的运用实现动态防护、满足安全需要、发挥技术优势，达到理想当中最佳的技术运用效果。

参考文献

[1]数据挖掘在高校教学质量评价中的应用[J].赵伟，武力兵.产业与科技论坛.2018（17）

[2]周雨辰.数据挖掘技术在软件工程中的应用研究[J].电脑迷，2017（08）：27-28.

[3]计算机网络安全病毒防御中的数据挖掘技术应用探析[J].王海军.信息与电脑（理论版）.2019（12）

[4]数据挖掘在计算机网络病毒防御中的应用[J].李倩.电子技术与软件工程.2019（04）