Universe Scientific Publishing
Scientific Research Management 科研管理（2）2020，2
ISSN：2661-3751（Print）；2661-376X（Online）

数据挖掘技术在网络安全未知威胁检测中的应用价值研究

张淑娟

[摘　要] 近些年，随着互联网技术的高速发展，逐渐渗透到人们生活和工作中的方方面面，带给人们极大的便利条件，但是随之而来的网络安全威胁问题也得到了人们的广泛关注。使用数据挖掘技术可以快速、准确的检测出网络中存在的未知威胁并通过安全防护软件等予以解决，为人们创造一个良好的网络环境。为此，本文对数据挖掘技术在网络安全未知威胁检测中的应用价值进行了研究，以供参考。

[关键词] 数据挖掘技术；网络安全；未知威胁；检测；应用

引言

数据挖掘技术在全部与互联网有关的事务中都有良好的应用，例如电子商务、网络入侵检测等方面，可以通过其独特的性能和作用为网络使用者提供数据挖掘和分析服务，保护网络使用者的网络安全，保护国家和个人的合法权益。在互联网日益普及的背景下，数据挖掘技术的合理应用可以有效的检测网络安全未知威胁，避免网络被黑客入侵，有助于绿色网络的建立。

1 数据挖掘技术概述

数据挖掘技术从本质上讲就是借助我国现有的数据库，通过数据提取、分析和处理操作，以此为基础检测网络安全未知威胁。数据挖掘技术在应用的过程中可以分为几个阶段，首先需要在数据挖掘前开展必要的准备工作，适当的清理无用数据，只保留有效数据[1]。其次，在准备工作中要将来源与不同数据库和数据源中的有关数据进行结合和集成，保证数据的完整和准确。最后，要将挖掘后的数据进行一定形式的转换，并联合应用智能化分析技术以及提取技术等对数据源中拥有一定规律和知识利用性的信息实时挖掘，完成网络安全未知检测。

2 数据挖掘技术在网络安全未知威胁检测中应用的计算方式

2.1 关联分析算法

在关联分析算法中，主要涉及到支持度和置信度两方面，其中，支持度帮助人们将不需要和不关系的数据予以删除，仅对关键的网络入侵数据进行检测。而置信度则体现了数据挖掘技术在网络安全未知威胁检测中应用的可行性和可信度，进而保证了数据挖掘技术的数据检测效果。在应用数据挖掘技术开展网络安全未知威胁检测工作时，人们主要关注的因素是支持度和可信度，要保证两者均大于网络用户的最大需求。

2.2 序列分析算法

数据挖掘技术应用过程中使用到的序列分析算法主要针对的是数据记录，需要在使用的过程中先按照一定的顺序规则制定一个有序数列，然后在数据记录中找到找到符合有序数列顺序的相关数据，进而实现对未知数据的检测，并以此为基础去判断网络完全威胁是否存在[2]。序列分析算法作为数据挖掘技术中应用十分广泛的一种算法，在网络安全未知威胁检测中的应用价值很高，是构建完全网络环境的重要保障。

2.3 分类和聚类分析算法

分类算法和聚类算法相似，在使用的过程中都需要数据挖掘工作人员有效的整理和归类数据库中的相关数据，以此将网络中存在的未知数据进行良好的分类和对比，为网络安全未知检测提供基本的数据保障。总体上看，数据挖掘技术应用中涉及的三种算法，分别解决了数据之间的关联性分析问题、找到了数据记录之间的关联性，并通过对比和分类数据模型中的数据差异，以此判断网络中入侵的数据是否存在威胁[3]。

3 数据挖掘技术在网络安全未知威胁检测中的应用

3.1 数据挖掘技术应用价值

目前，随着互联网应用的普及，数据挖掘技术在网络安全未知威胁检测中的应用越来越广泛，获得了很高的应用价值。与其它传统的网络安全未知威胁检测技术相比，数据挖掘技术的应用优势有很多，例如可以将网络安全未知威胁作为一种数据基础建立数据库，并在网络运行过程中发生的安全威胁问题及时、准确的检测出来，采取积极的应对。数据挖掘技术的应用具有很高的检测效率，适用范围更广，能够普遍应用在任何类型的网络安全未知威胁检测中[4]。另外，为了进一步提高网络安全防护等级，需要依托于数据挖掘技术构建网络入侵检测系统，实施网络安全深度防御，提高网络安全未知威胁检测速度和准确性，提高检测可行性和可靠性。

3.2 数据挖掘过程

数据挖掘技术在网络安全未知威胁检测中的应用需要经历以下几个步骤完成。第一，构建网络安全检测模型。在应用数据挖掘技术开展网络安全未知威胁检测之前，第一个步骤是以数据挖掘技术为基础建立一个适应网络安全运行环境的检测模型，对所有入侵网络的异常数据进行分类和整理，挑选出其中无效的数据予以清理，并将可疑的威胁数据统一起来纳入数据库，完成网络安全检测模型的建立[5]。第二，数据比对。网络安全未知威胁检测人员需要灵活的运用关联分析算法、序列分析算法、分类和聚类分析算法，在检测过程中制定标准的匹配序列规则，将检测到的网络异常数据与网络安全数据库中的有效数据进行一一比对，判断网络入侵数据是否存在威胁网络安全的行为，进而及时发现网络安全威胁问题。

3.3 数据挖掘技术应用发展趋势

现阶段，我国现有的数据挖掘技术在应用于网络安全威胁检测中时，还存在着检测速度慢、检测准确性低等问题，需要进行进一步的优化和改善。另外，数据挖掘技术应用的优势是比较明显的，可以检测出传统检测方式无法自动发现的网络未知威胁数据，具有较高的自动化和智能化。因此，在今后的技术应用发展过程中，主要的发展方向应该朝着高速、高准确率的方向发展，通过计算方法改良和技术创新应用等手段不断提高数据挖掘技术的应用效果和适用范围，提高其应用价值。

4 结论

总之，在网络安全未知威胁检测中应用数据挖掘技术，可以起到有效防护黑客入侵以及异常数据入侵网络的作用，以此建立一个安全、稳定的网络运营环境，保护网络用户的个人信息安全。为此，我们要重视数据挖掘技术的应用价值，要不断提高技术水平和检测理念，提高技术应用便捷性和可靠性，为网络安全做出更大的贡献。

[参考文献]

[1] 马泽鑫．数据挖掘技术在网络安全未知威胁检测中的应用价值[J]．网络安全技术与应用，2020(03):61-62.

[2] 徐敏，蒋伟梁．数据挖掘技术在网络入侵检测中的应用研究[J]．网络安全技术与应用，2016(6):68-69.

[3] 张志杰．基于数据挖掘的网络安全态势分析[J]．网络安全技术与应用，2016(3):62-62.

[4] 李燕，李策，冯丽丽．数据挖掘在电力信息系统网络安全的应用[J]．集成电路应用，2019(6):71-73.

[5] 刘鑫．数据挖掘在计算机网络安全领域的应用价值[J]．辽宁广播电视大学学报，2017(1).

作者简介：张淑娟（1983—），女，汉，云南寻甸，副教授。研究方向：软件工程、数据挖掘。