大数据挖掘技术在网络安全中的应用研究

邹琴琴
三亚学院信息与智能工程学院，中国·海南 三亚 572000

【摘　要】现在信息时代来到了，社会上各行各业都将信息融入到生产生活当中，同时信息也改变了人们的生活当时。在现在的时代当中使用人数的增加也伴随着安全问题的快速增加，这就需要对现在的网络安全进行管理。因此本文就现在的大数据挖掘技术在网络安全当中的应用进行简单的分析。

【关键词】大数据；挖掘技术；网络安全；应用研究

前言

现在是大数据的时代，网络结构和网络环境也逐渐变得复杂，在网络的使用过程当中就会关系到网络安全上的问题，如果不对网络安全进行管理，那么就很容易导致网络之中出现诈骗等现象。但是现在的网络世界当中存在太多的安全漏洞，防护的能力也比较弱，而大数据挖掘技术是一种新型的处理网络安全的手段，能对网络数据进行精准的分析，提高网络世界的安全性。

1　大数据挖掘技术的介绍

现在国家经济科技都得到了发展，互联网、人工智能等都得到了普遍的使用，而且使用的人数是诚信爆炸式增加，这就需要从这数据当中寻找出真正意义的数据，这样才能够满足当前用户的实际需求。社会上的人们在利用网络世界的时候所需要的要求都是不一样的，所以大数据都是需要满足不同用户的不同的需求，所以现在大数据挖掘技术就需要帮助各个产业从庞大的数据信息当中提取出需要的具有潜在价值的数据信息。首先就是需要对现在的数据库进行详细的分析，要筛选出用户所需要的一些数据信息，然后根据这些信息进行分析，并且进行适当的加工，让最后所呈现的数据是最为合适的模式。然后再采用适合的数据算法来对当前的数据进行提取，而提取之后就是对这些数据进行信息评估，这样就能够根据评估的一些信息进行整理，最后就是将所有的信息呈现给用户。用户也能够从这些信息当中找到自己所需要的东西。这样就形成了互惠互利的场景，从整体的局面来看就是大数据挖掘技术主要是对社会中数据库的提取，对所提取的数据进行简单的整理分析，然后根据所分析出来的数据进行了简单的处理。让处理之后的信息进行深度挖掘，这样就能够获得更多的信息。最后就是对深度挖掘的信息进行评估，这样就能够将所评估之后的信息进行使用。

而且现在的大数据挖掘技术有很多种方法能够进行选择，现在常用的就是数据关联、数据分类和数据聚类。这三种方法是目前最为常用的方法也是现在最方便快捷的方法，其中数据关联技术主要是利用数据与数据之间的相互关联性来对当前的数据进行分析，也可以从这些数据之间看到数据的关联程度。而在数据处理当中该方法主要是用在大数据的提取和数据的处理阶段，这样能够将数据进行简单的筛选。在数据关联技术的采用当中一般是对数据对象采用最小支持度，因为这样在进行数据处理的时候也会更加的快捷。如果说在进行数据提前或者是数据预处理的时候，数据对象的参数界定值低于最小的支持度，那么就说明提取到的数据之间是没有任何的关联，这样也说明提取到的数据存在错误。而为了判断数据关联之间的一些规则的可靠性，那么就需要采用最小的可信度来进行数据的提取。在一般情况下数据的提取都有一个最小的可信度，如果所提取到的数据低于了最小可信度，那么就说明提取到的数据之间关联规则是不行的。这两个参数的设定就是为了提取到用户最为需要的数据集合，也是最为重要的衡量标准。而且在进行数据分析的时候一般都是对数据进行深挖，这个阶段也是最重要的阶段，在这个阶段之中主要是对提取到的数据进行梳理，这个不同于之前的整理，之前的整理主要是将所提取到的数据进行分类，然后这些分类之后的数据再来对其进行信息的梳理。在进行梳理的过程当中也需要将数据算法或者是函数等方式融入到信息当中，最后转化成相应的模型，这样才能够实现对后面数据的预测分析。所以现在的数据分类技术的核心药店就是在于数据模型的建立，根据所得到的数据模型在对其数据进行分类、分析和预测。与数据聚类技术还有有一定区别的，数据分类技术主要是将不同性质的数据进行区分，而数据聚类技术主要是利用数据之间的相似性，然后对数据进行一定范围的缩小。数据聚类技术的算法与数据分类的算法也存在差异。

2　大数据挖掘技术在网络安全中的应用机制

2.1 大数据挖掘技术在数据收集方面的应用

现在是网络数据的时代，无论是哪一个行业的网络数据都是非常庞大的，尤其是现在很多人都是有私人的数据还有就是公司企业的一些隐私的数据，这些数据对于网络安全有很高的要求。而网络当中的泄密或者是网络当中的病毒入侵都是会造成数据信息的泄露，这些对于大型的企业或者是公司而言是非常危险的，因为有很多的核心技术就在这些数据当中。而大数据挖掘技术就是通过收集这些数据信息来寻找网络当中的安全隐患，如果说发现网络当中存在很多的隐患代码，就会直接将其找出来，并且给相应的提示，这样就能够更好的进行预防。除了将有病毒的代码找出来之外，还有就是能够对整个网络世界当中的一些异常入侵情况、恶意攻击的情况进行提示，这样也能够保护住网络中的数据。在通常的情况下，网络病毒主要是以代码的方式进入到计算机系统当中的，然后计算机在运转的时候就会将这些代码一同进行运行，这样就能够慢慢的渗入到整个计算当中，对计算机的系统进行渗透性的破坏。而大数据挖掘技术就通过对计算机中的各种代码程序进行仔细的分析，主要是分析各个代码中的关键点，这些关键点是比较容易隐藏病毒代码的，一旦在这些代码当中发现了一些病毒代码或者是其他的代码存在就采取一定针对性的预

防工作来进行。其次就是网络病毒的程序与部分计算机软件的程序有点相似，在进行整个病毒代码检测的过程当中不易被察觉，这样就很容易导致整个计算机系统的崩溃，所以在进行大数据挖掘技术的时候就需要先对网络世界当中的病毒代码进行收集，然后在对这些网络信息进行分类，最后就是将这些信息与当前的网络安全防御机制建立提供一定的数据支持。

2.2 大数据挖掘技术在数据处理当中的应用

上文简单的分析了大数据挖掘技术在数据的收集阶段的应用，在这个阶段之中主要是对网络世界当中的数据进行收集然后分类，为之后的数据处理提供一定的基础。而大数据挖掘技术就在这些数据收集的基础上对这些数据信息进行分析处理，然后根据分析的内容对网络世界进行科学有效地寻找和确定网络安全问题的根源。其实在网络世界当中，主要是以程序代码的形式对网络安全进行破坏，所以在进行网络安全管理的时候需要对这些网络程序代码进行转换和破解，这样才能够让技术人员对此进行识别，而且破解相应的程序代码的根本意图就是为了能够进行针对性的防御。在进行程序代码的转换和破解的时候，都是借助数据处理模块来进行的，因为对于程序代码的转换和破解主要是对数据源的位置和信息进行识别，能够识别出最初的信息源来自哪里，对于数据代码的源IP进行精准的定位，这样就能够进行病毒根源地的锁定。其次就是需要了解网络所中的病毒是哪一类，因此要对网络世界当中的病毒进行分类，要了解它们的类型，同时在进行网络安全分析的时候有必要的时候就需要封锁网络病毒的传播方式，将病毒的传播尽可能的控制在一定的范围内，这样就能够有效的控制病毒的范围，也能在这个范围内对病毒进行寻找。同时大数据挖掘技术还能够对现在的数据信息终端进行分析、分类和处理，而在进行处理的时候大数据挖掘技术提高了程序破解的效率，还为网络信息安全提供了重要的保障。

2.3 大数据挖掘技术在数据可中的应用

将大数据挖掘数据运用到数据库中主要是对数据库进行关联分析，这也能够为当前的数据聚类技术的应用提供一定的基础，在对当前的网络安全问题进行深入识别的时候就能够以这个应用技术为基础。现在很多的网络病毒程序在运行的时候主要是和所关联的数据库进行攻击，并且还能够对病毒的攻击轨迹和攻击的程度进行全面的记录。这些都是针对于现在的病毒所得到的数据，然后利用聚类分析算法来识别网络病毒的特征，最后从病毒的特征当中进行分析，然后提升计算机的程序系统的防御能力。

2.4 大数据挖掘技术在决策机制当中的应用

在计算机程序当中是有记忆模块的，而采用数据挖掘模块能够对记忆模块当中的数据进行分析。不仅需要对记忆模块当中的数据进行分析，还需要与规则库中的模块数据进行对比分析，然后根据两者之间数据的匹配度来进行比较，如果说两者之间的数据存在比较高的匹配度，那么这个计算机网络系统当中就存在安全隐患。其实在市场之中有很多的防火墙的软件，大师这些软件对于网络当中的病毒属性的判断准确率并不高，而且现在的网络病毒随时在进行更新，所以现在的病毒软件还存在与当前的网络世界当中。再者就是网络安全决策机制目前还不是太完善，还需要数据挖掘技术和决策模块相互配合才能进行应用。所以为了保证大数据挖掘技术的准确决策，就需要对现在网络世界中的病毒特征进行归纳总结，这样才能更加科学有效。但是在进行运用的时候要避免系统误判而导致数据干预不当，如果是这样是会为病毒程序提供了遗留的契机。

2.5 大数据挖掘技术在数据预处理当中的应用

对大数据库中的数据进行收集之后就是对其进行整理，而整理之后就是对数据进行处理，在数据处理的阶段就主要是对这些数据进行分析，然后将分析所的得到的结果进行数据模型的形成。而数据预处理是在病毒特征信息和决策条件的基础上进行下一步的分析归类的审核，这样才能够完善数据处理的结果。而且现在的大数据挖掘技术对于整个数据预处理方案的应用主要是对网络安全的相关信息进行科学的验证，在验证的过程当中就对程序系统中的一些关键数据参数和验证的指标进行提取，然后将其进行整理然后处理。处理之后的数据就会为计算机防御系统的构建提供重要的依据。但是在进行数据预处理的时候还需要对网络病毒的类型和特点进行分析。总而言之，在进行大数据挖掘技术的运用的时候都是需要对现在的网络病毒类型和特点进行归纳、分类。而对于这些病毒漏洞的原始特征进行分析判断的时候，就能够在一定程度上提升现在计算机系统中的预防能力。

3 结束语

现在的科技发展已经非常快速，网络信息时代也已经到来而且现在的网络应用已经渗透到人们的生产生活当中，在给人们带来便利的同时也带来了一定危险，所以要不断的加强网络安全管理。在进行管理的时候就需要采用大数据挖掘技术，这样能够充分的利用大数据挖掘技术的优势，提高计算机网络安全，抵抗外界病毒程序的入侵，促进当前的网络环境健康发展。

参考文献:

[1]覃凤萍,罗锦光.大数据挖掘技术在网络安全中的应用与研究[J].计算机产品与流通,2020(5).

[2]王志红.大数据挖掘技术在网络安全中的有效应用[J].信息与电脑(理论版),2020,v.32;No.460(18):198-200.

[3]周文.网络安全分析中的大数据技术应用研究[J].国际教育论坛,2020,2(4):21.

[4]田汉峰.网络安全分析中的大数据技术运用研究[J].锋绘,2020,000(002):P.234-234.

[5]王颖.网络安全分析中的大数据技术应用探究[J].电脑知识与技术:学术交流,2017,13(033):20-21.

[6]王艳华.大数据挖掘技术在网络安全中的应用与研究[J].电子世界,2019,No.581(23):63-64.

[7]冀冠楠.大数据挖掘技术在网络安全中的应用与研究[J].信息技术与信息化,2020,No.247(10):254-255.

[8]杨宇峰.大数据挖掘技术在网络安全中的应用研究[J].造纸装备及材料,2020,v.49;No.185(02):91-91.

作者简介:

邹琴琴（1982.6-），女，湖南怀化人，硕士，讲师，主要从事高校计算机公共教学研究。