(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111953665 A
(43)申请公布日 2020.11.17

(21)申请号 202010737901.4

(22)申请日 2020.07.28

(71)申请人 深圳供电局有限公司
地址 518000 广东省深圳市罗湖区深南东路4020号电力调度通信大楼

(72)发明人 丘惠军 陈昊 连耿雄 孙强强

(74)专利代理机构 深圳汇智容达专利商标事务所(普通合伙) 44238
代理人 徐文城

(51)Int.Cl.
H04L 29/06(2006.01)
G06K 9/62(2006.01)

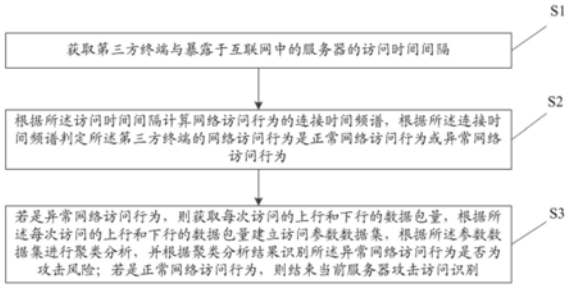
权利要求书2页 说明书8页 附图1页

(54)发明名称

服务器攻击访问识别方法及系统、计算机设备、存储介质

(57)摘要

本发明涉及一种服务器攻击访问识别方法及系统、计算机设备、存储介质，所述方法包括：获取第三方终端与暴露于互联网中的服务器的访问时间间隔；根据所述访问时间间隔计算网络访问行为的连接时间频谱，根据所述连接时间频谱判定所述第三方终端的网络访问行为是正常网络访问行为或异常网络访问行为；若是异常网络访问行为，则获取每次访问的上行和下行的数据包量，每次访问的上行和下行的数据包量建立访问参数数据集，根据所述参数数据集进行聚类分析，并根据聚类分析结果识别所述异常网络访问行为是否为攻击风险；若是正常网络访问行为，则结束当前服务器攻击访问识别。本发明能够解决目前对暴露于互联网络中的服务器进行攻击访问识别无法兼顾时效性和准确性的技术问题。



CN 111953665 A

1.一种服务器攻击访问识别方法,其特征在于,包括:

获取第三方终端与暴露于互联网中的服务器的访问时间间隔;

根据所述访问时间间隔计算网络访问行为的连接时间频谱,根据所述连接时间频谱判定所述第三方终端的网络访问行为是正常网络访问行为或异常网络访问行为;

若是异常网络访问行为,则获取每次访问的上行和下行的数据包量,每次访问的上行和下行的数据包量建立访问参数数据集,根据所述参数数据集进行聚类分析,并根据聚类分析结果识别所述异常网络访问行为是否为攻击风险;若是正常网络访问行为,则结束当前服务器攻击访问识别。

2.根据权利要求1所述的服务器攻击访问识别方法,其特征在于,所述获取暴露于互联网中的服务器的访问时间间隔,包括:

获取与暴露于互联网中的服务器建立连接的地址,并判定该地址为白名单地址或非白名单地址;若为非白名单地址,则采集非白名单地址的第三方终端与所述暴露于互联网中的服务器的访问时间间隔。

3.根据权利要求1所述的服务器攻击访问识别方法,其特征在于,所述根据所述参数数据集进行聚类分析,包括:

根据所有与所述暴露于互联网中的服务器建立连接的参数建立网络访问行为聚类分析图;

根据所述参数数据集在所述聚类分析图中设定对应点,得到聚类分析结果。

4.根据权利要求3所述的服务器攻击访问识别方法,其特征在于,所述根据聚类分析结果识别所述异常网络访问行为是否为攻击风险,包括:

根据所述参数数据集在所述聚类分析图中设定对应点与所述异常网络行为簇的距离判断是否为攻击风险。

5.根据权利要求4所述的服务器攻击访问识别方法,其特征在于,所述根据聚类分析结果识别所述异常网络访问行为是否为攻击风险,包括:

在所述对应点与所述异常网络行为簇的距离超出预设阈值时,判断所述对应点为离群点;

获取所述离群点在当前时间节点之前预设次数会话的会话时长,以及与所述会话时长对应的小包数量;

将所述会话时长输入和小包数量进行预处理得到预处理信息,利用预先训练好的异常行为判断神经网络模型对所述预处理信息进行识别确定所述异常网络访问行为是否为攻击风险。

6.根据权利要求5所述的服务器攻击访问识别方法,其特征在于,所述将所述会话时长输入和小包数量进行预处理得到预处理信息,包括:

将所述会话时长输入和小包数量通过傅里叶变换转化为相应的频谱图像。

7.一种服务器攻击访问识别系统,用于实施权利要求1-6任一项所述的服务器攻击访问识别方法,其特征在于,包括:

访问间隔获取单元,用于获取第三方终端与暴露于互联网中的服务器的访问时间间隔;

访问行为判定单元,用于根据所述访问时间间隔计算网络访问行为的连接时间频谱,

根据所述连接时间频谱判定所述第三方终端的网络访问行为是正常网络访问行为或异常网络访问行为;以及

攻击风险识别单元,用于若是异常网络访问行为,则获取每次访问的上行和下行的数据包量,每次访问的上行和下行的数据包量建立访问参数数据集,根据所述参数数据集进行聚类分析,并根据聚类分析结果识别所述异常网络访问行为是否为攻击风险;若是正常网络访问行为,则结束当前服务器攻击访问识别。

8.一种计算机设备,包括:根据权利要求7所述的服务器攻击访问识别系统;或者,存储器和处理器,所述存储器中存储有计算机可读指令,所述计算机可读指令被所述处理器执行时,使得所述处理器执行根据权利要求1-6中任一项所述服务器攻击访问识别方法的步骤。

9.一种计算机可读存储介质,其上存储有计算机程序,其特征在于:所述计算机程序被处理器执行时实现根据权利要求1-6中任一项所述服务器攻击访问识别方法。

服务器攻击访问识别方法及系统、计算机设备、存储介质

技术领域

[0001] 本发明涉及网络安全技术领域，具体涉及一种服务器攻击访问识别方法及系统、计算机设备、存储介质。

背景技术

[0002] 在电力网络中，通常会有比较明显的边界。防火墙/UTM通常会作为边界防护设备，连通内网和外网(广域网)，同时也保护内网中的主机和服务器，阻止外部到内部的非法访问和攻击。但由于业务需要，不可避免的会存在部分主机或者服务器直接暴露于互联网，存在着较大的安全风险。

[0003] 随着网络技术的不断发展，对于主机或者服务器的攻击手段也在不断加强，具体体现在对于有价值的信息，攻击者会结合各种网络漏洞进行攻击，持续瞄准目标以达到攻击目的。同时攻击手段和工具也处于不断变化中，传统的防范工具反应滞后，很难对其进行防范。

[0004] 为解决滞后问题，目前，现有的主要防范方式主要有以下两种：沙箱检测识别和基于规则的异常检测识别。沙箱检测识别的主要原理为：将实时网络流量先引入旁路沙箱模型，审计各种进程的网络流量，通过代码检查器扫描是否存在恶意代码。基于规则的异常检测识别主要原理为：通过对网络中的正常行为模式设定安全方位规则，进而识别异常。沙箱检测识别由于对代码进行识别，但过程中，需要对数据包进行分解重组获取代码，并对代码进行检测识别，在面对大流量访问时，很难快速及时准确的给出检测识别结果，影响正常访问。而基于规矩的异常检测识别则取决于规则的复杂程度，简单的规则会使得异常访问能够通过规则检测识别，而过于复杂的规则又会严重影响检测识别的时效性。

发明内容

[0005] 本发明的目的在于提出一种服务器攻击访问识别方法及系统、计算机设备、计算机可读存储介质，以解决目前对暴露于互联网络中的服务器进行攻击访问识别无法兼顾时效性和准确性的技术问题。

[0006] 为实现上述目的，根据第一方面，本发明实施例提出一种服务器攻击访问识别方法，包括：

[0007] 获取第三方终端与暴露于互联网中的服务器的访问时间间隔；

[0008] 根据所述访问时间间隔计算网络访问行为的连接时间频谱，根据所述连接时间频谱判定所述第三方终端的网络访问行为是正常网络访问行为或异常网络访问行为；

[0009] 若是异常网络访问行为，则获取每次访问的上行和下行的数据包量，每次访问的上行和下行的数据包量建立访问参数数据集，根据所述参数数据集进行聚类分析，并根据聚类分析结果识别所述异常网络访问行为是否为攻击风险；若是正常网络访问行为，则结束当前服务器攻击访问识别。

[0010] 优选地，所述获取暴露于互联网中的服务器的访问时间间隔，包括：

[0011] 获取与暴露于互联网中的服务器建立连接的地址，并判定该地址为白名单地址或非白名单地址；若为非白名单地址，则采集非白名单地址的第三方终端与所述暴露于互联网中的服务器的访问时间间隔。

[0012] 优选地，所述根据所述参数数据集进行聚类分析，包括：

[0013] 根据所有与所述暴露于互联网中的服务器建立连接的参数建立网络访问行为聚类分析图；

[0014] 根据所述参数数据集在所述聚类分析图中设定对应点，得到聚类分析结果。

[0015] 优选地，所述根据聚类分析结果识别所述异常网络访问行为是否为攻击风险，包括：

[0016] 根据所述参数数据集在所述聚类分析图中设定对应点与所述异常网络行为簇的距离判断是否为攻击风险。

[0017] 优选地，所述根据聚类分析结果识别所述异常网络访问行为是否为攻击风险，包括：

[0018] 在所述对应点与所述异常网络行为簇的距离超出预设阈值时，判断所述对应点为离群点；

[0019] 获取所述离群点在当前时间节点之前预设次数会话的会话时长，以及与所述会话时长对应的小包数量；

[0020] 将所述会话时长输入和小包数量进行预处理得到预处理信息，利用预先训练好的异常行为判断神经网络模型对所述预处理信息进行识别确定所述异常网络访问行为是否为攻击风险。

[0021] 优选地，所述将所述会话时长输入和小包数量进行预处理得到预处理信息，包括：

[0022] 将所述会话时长输入和小包数量通过傅里叶变换转化为相应的频谱图像。

[0023] 根据第二方面，本发明实施例还提出一种服务器攻击访问识别系统，用于实施第一方面所述的服务器攻击访问识别方法，包括：

[0024] 访问间隔获取单元，用于获取第三方终端与暴露于互联网中的服务器的访问时间间隔；

[0025] 访问行为判定单元，用于根据所述访问时间间隔计算网络访问行为的连接时间频谱，根据所述连接时间频谱判定所述第三方终端的网络访问行为是正常网络访问行为或异常网络访问行为；以及

[0026] 攻击风险识别单元，用于若是异常网络访问行为，则获取每次访问的上行和下行的数据包量，每次访问的上行和下行的数据包量建立访问参数数据集，根据所述参数数据集进行聚类分析，并根据聚类分析结果识别所述异常网络访问行为是否为攻击风险；若是正常网络访问行为，则结束当前服务器攻击访问识别。

[0027] 根据第三方面，本发明实施例还提出一种计算机设备，包括：根据第二方面所述的服务器攻击访问识别系统；或者，存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行根据第一方面所述的服务器攻击访问识别方法的步骤。

[0028] 根据第四方面，本发明实施例还提出一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现根据第一方面所述的服务器攻击访问识别方

法。

[0029] 本发明的实施例提出了一种服务器攻击访问识别方法及其系统、计算机设备、计算机可读存储介质，可以利用网络攻击工具访问的自动性，确定对应的访问时间间隔，并将访问时间间隔转换为连接时间频谱，并利用连接时间频谱判断是否为异常网络访问行为，进而实现对可能的网络攻击行为进行初步筛查，在确定其可能为网络攻击行为时，利用访问数据特征进一步进行聚类分析，进而判断是否为攻击风险。由于采用访问时序特征对可能的攻击行为进行初步排查，可以有效减少后期判断的运算量，同时，聚类分析相对于规则匹配等方法运算量交底，可以较快的得到判断结果，并且能够保证判断的准确性。从而解决了目前对暴露于互联网络中的服务器进行攻击访问识别无法兼顾时效性和准确性的技术问题。

[0030] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而得以体现。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0031] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0032] 图1为本发明一实施例中一种服务器攻击访问识别方法的流程图。

[0033] 图2为本发明一实施例中一种服务器攻击访问识别系统的框架图。

具体实施方式

[0034] 以下将参考附图详细说明本公开的各种示例性实施例、特征和方面。另外，为了更好的说明本发明，在下文的具体的实施例中给出了众多的具体细节。本领域技术人员应当理解，没有某些具体细节，本发明同样可以实施。在一些实例中，对于本领域技术人员熟知的手段未作详细描述，以便于凸显本发明的主旨。

[0035] 参阅图1，本发明一实施例提出本发明实施例提出一种服务器攻击访问识别方法，包括：

[0036] 步骤S1、获取第三方终端与暴露于互联网中的服务器的访问时间间隔；

[0037] 具体而言，为了达到攻击目标，攻击者往往会利用各种工具进行长时间、持续的入侵和渗透，直到攻破。从最初的侦查阶段完成到信息资产的窃取。需要多次对攻击目标多次访问。无论是漏洞攻击还是传统的木马攻击，其都需要进行大量的访问来实现对可能的攻击点进行检测。由于访问需要大量重复扫描才可确定攻击点，因此，通常采用程序来实现对服务器的扫描，进而通过漏洞或者植入木马对服务器产生攻击。而程序访问与正常访问在访问频率和时间上会存在不同，利用该特点可以对攻击行为进行初步识别。

[0038] 在本实施例中，根据程序扫描或者盗取植入木马相关信息的与服务器建立连接的时间参数进行采集。示例性的，可以通过查看日志等方式收集与直接暴露于互联网的服务器的访问时间间隔。

[0039] 步骤S2、根据所述访问时间间隔计算网络访问行为的连接时间频谱，根据所述连接时间频谱判定所述第三方终端的网络访问行为是正常网络访问行为或异常网络访问行为；

[0040] 具体而言，目前部分木马或者扫描程序可以对连接时间进行调整，但由于其必须在规定的时间内完成扫描次数，即一定时间内必须与所述服务器建立多次连接。因此，其与所述服务器建立连接的时间相对于普通用户来说相对具有规律性，虽然目前可以通过扫描程序或者木马程序中的随机函数来对访问时间进行控制，但由于受到各种访问条件约束，例如上述提到的在一定时长内完成扫描次数等，其与所述服务器建立连接的时长仍然具有一定规律性。但该种规律不便于直接识别。因此，在本实施例中，根据所述连接时间参数计算连接时间图谱。即将所述每次连接时间的间隔(访问时间间隔)作为时序序列，对所述时序序列进行离散傅里叶变换，得到相应的时间频谱图，根据所述频谱图中的频谱范围确定是否为异常网络访问行为。进一步的，在所述频谱范围小于预设的范围时，确定为异常网络访问行为。

[0041] 步骤S3、若是异常网络访问行为，则获取每次访问的上行和下行的数据包量，每次访问的上行和下行的数据包量建立访问参数数据集，根据所述参数数据集进行聚类分析，并根据聚类分析结果识别所述异常网络访问行为是否为攻击风险；若是正常网络访问行为，则结束当前服务器攻击访问识别。

[0042] 具体而言，通过上述步骤S1-S2可以初步判断可能存在被攻击风险，还需通过后续处理对其进行确认。在本实施例中，在通过上述步骤确定为异常网络访问行为时，可以获取与所述服务器建立连接的其它信息对其是否为攻击行为进行识别。

[0043] 对服务器的漏洞扫描或者木马通信过程中，其中每次的通信内容基本保持不变，其每次发送的数据包的数量基本一致，并且其在应用层通信的内容也基本相同。且流量和数据包的数量都较小，利用此特点，可以上述步骤判断的异常网络访问行为是否为攻击风险进行准确判别。示例性的，所述参数可以包括：访问的间隔时长、每次访问的上行数据包量、下行数据包量、数据流量。根据上述参数建立相应的集合，生成访问参数数据集。

[0044] 在本实施例中，所述对将所述参数数据集加入网络访问行为聚类分析图，可以包括：根据所有与网络暴露服务器的建立连接的参数建立网络访问行为聚类分析图；根据所述参数数据集在所述聚类分析图中设定对应点。将物理或抽象对象的集合分成由类似的对象组成的多个类的过程被称为聚类。由聚类所生成的簇是一组数据对象的集合，这些对象与同一个簇中的对象彼此相似，与其他簇中的对象相异。

[0045] 在本实施例中，可以采用K-MEANS算法实现聚类，其原来为给定一个有N个元组或者纪录的数据集，分裂法将构造K个分组，每一个分组就代表一个聚类，K<N。而且这K个分组满足下列条件：(1)每一个分组至少包含一个数据纪录；(2)每一个数据纪录属于且仅属于一个分组(注意：这个要求在某些模糊聚类算法中可以放宽)；对于给定的K，算法首先给出一个初始的分组方法，以后通过反复迭代的方法改变分组，使得每一次改进之后的分组方案都较前一次好，而所谓好的标准就是：同一分组中的记录越近越好，而不同分组中的纪录越远越好。大部分划分方法是基于距离的。给定要构建的分区数k，划分方法首先创建一个初始化划分。然后，它采用一种迭代的重定位技术，通过把对象从一个组移动到另一个组来进行划分。一个好的划分的一般准备是：同一个簇中的对象尽可能相互接近或相关，而不同

的簇中的对象尽可能远离或不同。还有许多评判划分质量的其他准则。传统的划分方法可以扩展到子空间聚类，而不是搜索整个数据空间。当存在很多属性并且数据稀疏时，这是有用的。为了达到全局最优，基于划分的聚类可能需要穷举所有可能的划分，计算量极大。实际上，大多数应用都采用了流行的启发式方法，如k-均值和k-中心算法，渐近的提高聚类质量，逼近局部最优解。这些启发式聚类方法很适合发现中小规模的数据库中小规模的数据库中的球状簇。为了发现具有复杂形状的簇和对超大型数据集进行聚类，需要进一步扩展基于划分的方法。利用上述方式实现对所述参数数据集在所述聚类分析图中的定位。由于所述聚类分析图中包括所有网络访问的相应数据对应的点，其自动针对特征对正常网络访问行为和攻击风险行为进行判别，对生成对应的簇，根据参数数据集对应的定位点与各簇之间的位置关系，可判断其是否为攻击风险。

[0046] 可选的，可以根据所述参数数据集在所述聚类分析图中设定对应点与所述异常网络行为簇的距离判断是否为攻击风险。示例性的，可以判断所述设定对应点与异常网络行为簇之间的距离是否小于设定的安全距离阈值，在小于设定的安全距离阈值时，确定其可能为攻击风险。

[0047] 通过以上实施例的描述可知，本实施例方法可以利用网络攻击工具访问的自动性，确定对应的访问时间间隔，并将访问时间间隔转换为连接时间频谱，并利用连接时间频谱判断是否为异常网络访问行为，进而实现对可能的网络攻击行为进行初步筛查，在确定其可能为网络攻击行为时，利用访问数据特征进一步进行聚类分析，进而判断是否为攻击风险。由于采用访问时序特征对可能的攻击行为进行初步排查，可以有效减少后期判断的运算量，同时，聚类分析相对于规则匹配等方法运算量交底，可以较快的得到判断结果，并且能够保证判断的准确性。从而解决了目前对暴露于互联网络中的服务器进行攻击访问识别无法兼顾时效性和准确性的技术问题。

[0048] 基于上述实施例方法，本发明还提出了一些更为具体的实施例，下面对该些具体的实施例进行描述。

[0049] 在一具体的实施例中，所述获取暴露于互联网中的服务器的访问时间间隔，包括：

[0050] 获取与暴露于互联网中的服务器建立连接的地址，并判定该地址为白名单地址或非白名单地址；若为非白名单地址，则采集非白名单地址的第三方终端与所述暴露于互联网中的服务器的访问时间间隔。

[0051] 具体而言，通过白名单机制能够快速地排除非网络攻击可能的连接行为，进一步减少了运算的数据量。在满足识别精确度的要求下，减少了判别所需要的时间。

[0052] 在一具体的实施例中，所述根据所述参数数据集进行聚类分析，包括：

[0053] 步骤S311、根据所有与所述暴露于互联网中的服务器建立连接的参数建立网络访问行为聚类分析图；

[0054] 步骤S312、根据所述参数数据集在所述聚类分析图中设定对应点，得到聚类分析结果。

[0055] 在一具体的实施例中，所述根据聚类分析结果识别所述异常网络访问行为是否为攻击风险，包括：

[0056] 步骤S321、根据所述参数数据集在所述聚类分析图中设定对应点与所述异常网络行为簇的距离判断是否为攻击风险。

[0057] 在一具体的实施例中，所述根据聚类分析结果识别所述异常网络访问行为是否为攻击风险，包括：

[0058] 步骤S331、在所述对应点与所述异常网络行为簇的距离超出预设阈值时，判断所述对应点为离群点；

[0059] 示例性的，可以包括找到各簇质心；计算单对象到最近质心的距离；计算各对象到它的最近质心的相对距离；将其与给定的阈值作比较，选出离群点。

[0060] 步骤S332、获取所述离群点在当前时间节点之前预设次数会话的会话时长，以及与所述会话时长对应的小包数量；

[0061] 具体而言，聚类分析中各簇充分反映了不同安全状况，而离群点则可能由于其网络访问方式不同于以往的网络访问方式，造成在聚类分析中无法将其进行归类。为避免该种情况，在本实施例中，利用所述会话时长及其对应的小包数量来进行判断。示例性的，所述在当前时间节点之前预设次数会话的会话时长，以及与所述会话时长对应的小包数量。通常在进行攻击之前几次通信或者在展开攻击时，攻击端与服务器会建立较长时间的会话连接，并交互大量数据。并且该数据通常是以大量小流量包实现，以避免由于网络原因导致的传输错误，或者减少被沙箱检测到的几率。基于上述特点，可以对其进行识别。

[0062] 步骤S333、将所述会话时长输入和小包数量进行预处理得到预处理信息，利用预先训练好的异常行为判断神经网络模型对所述预处理信息进行识别确定所述异常网络访问行为是否为攻击风险。

[0063] 在本实施例中，可以利用卷积神经网络模型对其是否为攻击风险进行识别，卷积神经网络(Convolutional Neural Networks,CNN)是一类包含卷积计算且具有深度结构的前馈神经网络，是深度学习的代表算法之一。卷积神经网络具有表征学习(representation learning)能力，能够按其阶层结构对输入信息进行平移不变分类。在本实施例中，可以将包括不同预处理信息和对应的判断结果的大量样本数据输入到卷积神经网络模型中进行训练，采用端到端学习，在训练完成后，将离群点对应的预处理信息输入到神经网络模型，即可输出相应的识别结果。

[0064] 在一具体的实施例中，所述将所述会话时长输入和小包数量进行预处理得到预处理信息，包括：

[0065] 将所述会话时长输入和小包数量通过傅里叶变换转化为相应的频谱图像。

[0066] 具体而言，由于卷积神经网络对于图像识别特别适用，而对于数组或者矩阵其处理时间较长，因此，在本实施例中，由于所述会话时长输入和小包数量是与时间序列相关的参数，利用傅里叶变换可以将其转换为频谱图像，并且频率变化较快的频谱图像在边缘处会有明显区别，利用卷积神经网络能够更快的得到较为准确的识别结果。

[0067] 本发明另一实施例还提出一种服务器攻击访问识别系统，用于实施上述实施例所述的服务器攻击访问识别方法，包括：

[0068] 访问间隔获取单元1，用于获取第三方终端与暴露于互联网中的服务器的访问时间间隔；

[0069] 访问行为判定单元2，用于根据所述访问时间间隔计算网络访问行为的连接时间频谱，根据所述连接时间频谱判定所述第三方终端的网络访问行为是正常网络访问行为或异常网络访问行为；以及

[0070] 攻击风险识别单元3,用于若是异常网络访问行为,则获取每次访问的上行和下行的数据包量,每次访问的上行和下行的数据包量建立访问参数数据集,根据所述参数数据集进行聚类分析,并根据聚类分析结果识别所述异常网络访问行为是否为攻击风险;若是正常网络访问行为,则结束当前服务器攻击访问识别。

[0071] 以上所描述的系统实施例仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

[0072] 需说明的是,上述实施例所述系统与上述实施例所述方法对应,因此,上述实施例所述系统未详述部分可以参阅上述实施例所述方法的内容得到,此处不再赘述。

[0073] 并且,上述实施例所述服务器攻击访问识别系统如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。

[0074] 本发明另一实施例提出一种计算机设备,包括:根据上述实施例所述的服务器攻击访问识别系统;或者,存储器和处理器,所述存储器中存储有计算机可读指令,所述计算机可读指令被所述处理器执行时,使得所述处理器执行根据上述实施例所述的服务器攻击访问识别方法的步骤。

[0075] 当然,所述计算机设备还可以具有有线或无线网络接口、键盘以及输入输出接口等部件,以便进行输入输出,该计算机设备还可以包括其他用于实现设备功能的部件,在此不做赘述。

[0076] 示例性的,所述计算机程序可以被分割成一个或多个单元,所述一个或者多个单元被存储在所述存储器中,并由所述处理器执行,以完成本发明。所述一个或多个单元可以是能够完成特定功能的一系列计算机程序指令段,该指令段用于描述所述计算机程序在所述计算机设备中的执行过程。

[0077] 所述处理器可以是中央处理单元(Central Processing Unit,CPU),还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等,所述处理器是所述计算机设备的控制中心,利用各种接口和线路连接整个所述计算机设备的各个部分。

[0078] 所述存储器可用于存储所述计算机程序和/或单元,所述处理器通过运行或执行存储在所述存储器内的计算机程序和/或单元,以及调用存储在存储器内的数据,实现所述计算机设备的各种功能。此外,存储器可以包括高速随机存取存储器,还可以包括非易失性存储器,例如硬盘、内存、插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字(Secure Digital,SD)卡,闪存卡(Flash Card)、至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0079] 本发明另一实施例提出一种计算机可读存储介质,其上存储有计算机程序,其特征在于:所述计算机程序被处理器执行时实现根据上述实施例所述的服务器攻击访问识别方法。

[0080] 示例性地,所述计算机可读存储介质可以包括:能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、电载波信号、电信信号以及软件分发介质等。

[0081] 以上已经描述了本发明的各实施例,上述说明是示例性的,并非穷尽性的,并且也不限于所披露的各实施例。在不偏离所说明的各实施例的范围和精神的情况下,对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择,旨在最好地解释各实施例的原理、实际应用或对市场中的技术改进,或者使本技术领域的其它普通技术人员能理解本文披露的各实施例。

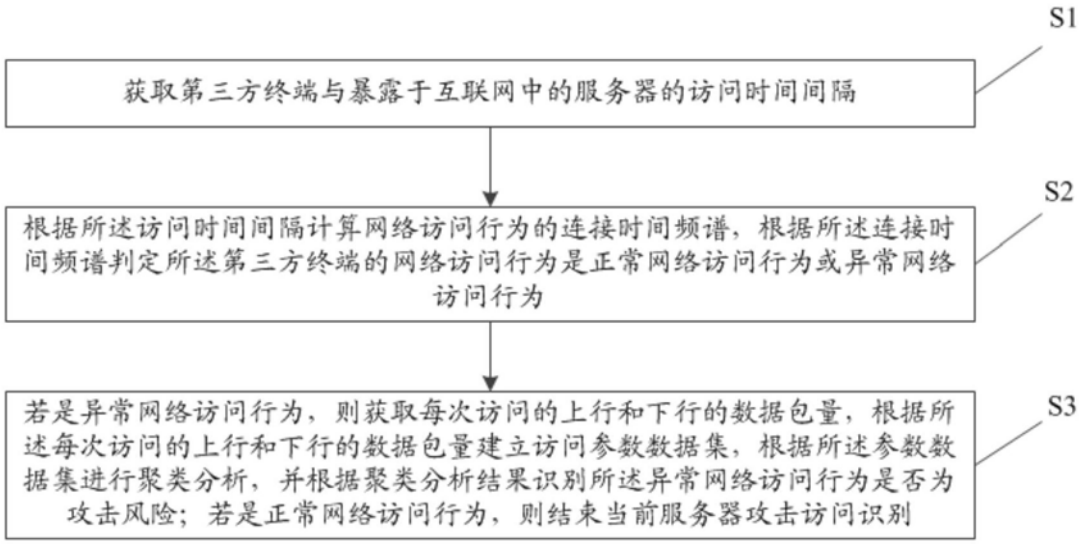

S1
获取第三方终端与暴露于互联网中的服务器的访问时间间隔
S2
根据所述访问时间间隔计算网络访问行为的连接时间频谱，根据所述连接时间频谱判定所述第三方终端的网络访问行为是正常网络访问行为或异常网络访问行为
S3
若是异常网络访问行为，则获取每次访问的上行和下行的数据包量，根据所述每次访问的上行和下行的数据包量建立访问参数数据集，根据所述参数数据集进行聚类分析，并根据聚类分析结果识别所述异常网络访问行为是否为攻击风险；若是正常网络访问行为，则结束当前服务器攻击访问识别

图1

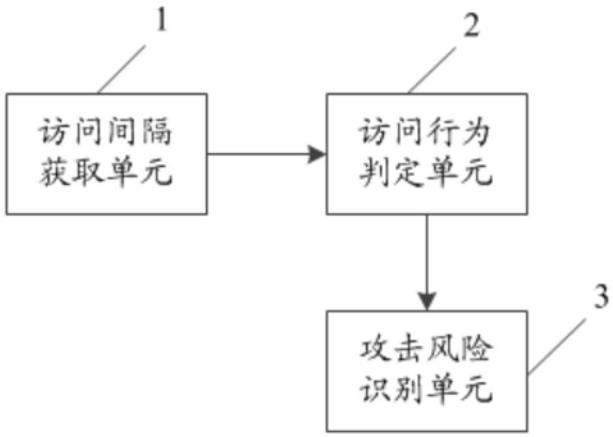

1
访问间隔获取单元
2
访问行为判定单元
3
攻击风险识别单元

图2