(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114567678 A
(43)申请公布日 2022.05.31

(21)申请号 202210191837.3

(22)申请日 2022.02.28

(71)申请人 天翼安全科技有限公司
地址 100010 北京市东城区朝阳门北大街19号中国电信大厦

(72)发明人 刘紫千 常力元 孙福兴 李金伟 余启明 顾庆崴 陈林 刘长波

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
专利代理师 刘醒晗

(51)Int.Cl.
H04L 67/60(2022.01)
H04L 67/51(2022.01)
H04L 9/40(2022.01)
H04L 67/12(2022.01)

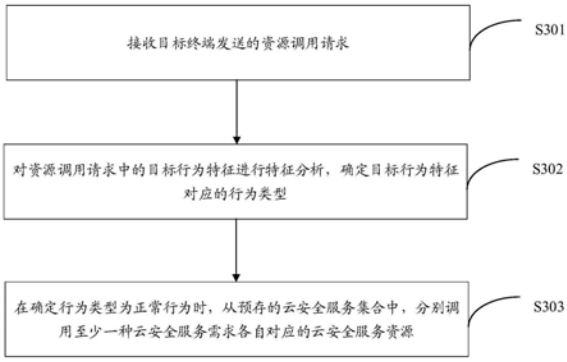
权利要求书2页 说明书11页 附图7页

(54)发明名称

一种云安全服务的资源调用方法、装置及电子设备

(57)摘要

本申请实施例提供了一种云安全服务的资源调用方法、装置及电子设备，涉及网络安全技术领域。本申请中，接收目标终端发送的资源调用请求之后，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型，从而在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源。采用本申请，通过对目标行为特征进行特征分析，确定目标行为特征对应的行为类型，从而根据目标行为特征的行为类型，判断是否调用至少一种云安全服务需求各自对应的云安全服务资源，提高了云安全服务资源调用的准确性。



CN 114567678 A

1.一种云安全服务的资源调用方法,其特征在于,包括:

接收目标终端发送的资源调用请求;其中,所述资源调用请求至少包括:目标对象的目标行为特征以及至少一种云安全服务需求;

对所述资源调用请求中的目标行为特征进行特征分析,确定所述目标行为特征对应的行为类型;

在确定所述行为类型为正常行为时,从所述预存的云安全服务集合中,分别调用所述至少一种云安全服务需求各自对应的云安全服务资源。

2.如权利要求1所述的方法,其特征在于,所述接收目标终端发送的资源调用请求之后,还包括:

从所述资源调用请求中,获取所述目标对象对应的目标哈希值;其中,所述目标哈希值表征:所述目标对象的特征信息,以及相应的至少一个云安全服务资源各自的特征信息;

在确定预设的哈希值集合中,存在所述目标哈希值时,对所述资源调用请求中的目标行为特征进行特征分析,确定所述目标行为特征对应的行为类型。

3.如权利要求1或2所述的方法,其特征在于,所述接收目标终端发送的资源调用请求之后,还包括:

获取所述目标对象对应的至少一种权限认证因子;其中,每种权限认证因子表征:相应权限认证方式认证通过的概率;

在确定所述至少一种权限认证因子,满足各自对应的权限认证条件时,对所述资源调用请求中的目标行为特征进行特征分析,确定所述目标行为特征对应的行为类型。

4.如权利要求1所述的方法,其特征在于,所述对所述资源调用请求中的目标行为特征进行特征分析,确定所述目标行为特征对应的行为类型,包括:

获取日志文件中记录的各个历史对象各自对应的历史行为特征;其中,每个历史对象拥有:所述至少一种云安全服务需求各自对应的云安全服务资源的资源调用权限;

基于所述目标行为特征与各个历史行为特征之间的特征相似度,确定所述目标特征行为的行为类型。

5.如权利要求4所述的方法,其特征在于,所述基于所述目标行为特征与各个历史行为特征之间的特征相似度,确定所述目标特征行为的行为类型,包括:

若获得的各个特征相似度均小于设定的相似度阈值,则确定所述目标特征行为的行为类型为异常行为;

若所述各个特征相似度中,存在大于所述相似度阈值的特征相似度,则确定所述目标特征行为的行为类型为正常行为。

6.一种云安全服务的资源调用装置,其特征在于,包括:

接收模块,用于接收目标终端发送的资源调用请求;其中,所述资源调用请求至少包括:目标对象的目标行为特征以及至少一种云安全服务需求;

分析模块,用于对所述资源调用请求中的目标行为特征进行特征分析,确定所述目标行为特征对应的行为类型;

调用模块,用于在确定所述行为类型为正常行为时,从所述预存的云安全服务集合中,分别调用所述至少一种云安全服务需求各自对应的云安全服务资源。

7.如权利要求6所述的装置,其特征在于,在所述接收目标终端发送的资源调用请求之

后,所述接收模块还用于:

从所述资源调用请求中,获取所述目标对象对应的目标哈希值;其中,所述目标哈希值表征:所述目标对象的特征信息,以及相应的至少一个云安全服务资源各自的特征信息;

在确定预设的哈希值集合中,存在所述目标哈希值时,对所述资源调用请求中的目标行为特征进行特征分析,确定所述目标行为特征对应的行为类型。

8.如权利要求6或7所述的装置,其特征在于,在所述接收目标终端发送的资源调用请求之后,所述接收模块还用于:

获取所述目标对象对应的至少一种权限认证因子;其中,每种权限认证因子表征:相应权限认证方式认证通过的概率;

在确定所述至少一种权限认证因子,满足各自对应的权限认证条件时,对所述资源调用请求中的目标行为特征进行特征分析,确定所述目标行为特征对应的行为类型。

9.如权利要求6所述的装置,其特征在于,在所述对所述资源调用请求中的目标行为特征进行特征分析,确定所述目标行为特征对应的行为类型时,所述分析模块具体用于:

获取日志文件中记录的各个历史对象各自对应的历史行为特征;其中,每个历史对象拥有:所述至少一种云安全服务需求各自对应的云安全服务资源的资源调用权限;

基于所述目标行为特征与各个历史行为特征之间的特征相似度,确定所述目标特征行为的行为类型。

10.如权利要求9所述的装置,其特征在于,在所述基于所述目标行为特征与各个历史行为特征之间的特征相似度,确定所述目标特征行为的行为类型时,所述分析模块具体用于:

若获得的各个特征相似度均小于设定的相似度阈值,则确定所述目标特征行为的行为类型为异常行为;

若所述各个特征相似度中,存在大于所述相似度阈值的特征相似度,则确定所述目标特征行为的行为类型为正常行为。

11.一种电子设备,包括存储器,处理器及存储在存储器上并可在处理器运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现如权利要求1-5中任一项所述的方法。

12.一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如权利要求1-5中任一所述方法的步骤。

13.一种计算机程序产品,其特征在于,所述计算机程序产品在被计算机调用时,使得所述计算机执行如权利要求1-5中任一项所述的方法。

一种云安全服务的资源调用方法、装置及电子设备

技术领域

[0001] 本申请涉及网络安全技术领域，尤其涉及一种云安全服务的资源调用方法、装置及电子设备。

背景技术

[0002] 随着互联网技术的飞速发展，零信任网络框架概念的普及、到通用协议的制定，对云边界访问安全提供了一种崭新的视角；进一步地，基于零信任网络访问(Zero-Trust Network Access，ZTNA)的资源共享业务也逐渐增加。

[0003] 例如，为了实现资源数据的安全共享，根据预设的路径映射关系，对终端发送的资源访问请求进行映射处理，获得相应的映射结果；接着，从预设的云安全服务集合中，选取出映射结果所对应的目标云安全服务资源；进一步地，在确定资源访问请求携带，调用目标云安全服务资源所需的配置参数时，建立与终端之间的安全通信通道；最终，通过安全通信通道将目标云安全服务资源发送给终端。

[0004] 然而，采用上述的ZTNA方式，会因异常对象在终端发出的资源访问请求携带，调用相应的云安全服务资源所需的配置参数时，也可建立与终端之间的安全通信通道，从而进行异常的云安全服务资源调用。因此，采用上述方式，无法提高云安全服务资源调用的准确性。

发明内容

[0005] 本申请提供一种云安全服务的资源调用方法、装置及电子设备，用以提高云安全服务资源调用的准确性。

[0006] 第一方面，本申请实施例提供了一种云安全服务的资源调用方法，所述方法包括：

[0007] 接收目标终端发送的资源调用请求；其中，资源调用请求至少包括：目标对象的目标行为特征以及至少一种云安全服务需求。

[0008] 对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型。

[0009] 在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源。

[0010] 第二方面，本申请实施例还提供了一种云安全服务的资源调用装置，所述装置包括：

[0011] 接收模块，用于接收目标终端发送的资源调用请求；其中，资源调用请求至少包括：目标对象的目标行为特征以及至少一种云安全服务需求。

[0012] 分析模块，用于对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型。

[0013] 调用模块，用于在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源。

[0014] 一种可选的实施例中，在接收目标终端发送的资源调用请求之后，接收模块还用于：

[0015] 从资源调用请求中，获取目标对象对应的目标哈希值；其中，目标哈希值表征：目标对象的特征信息，以及相应的至少一个云安全服务资源各自的特征信息。

[0016] 在确定预设的哈希值集合中，存在目标哈希值时，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型。

[0017] 一种可选的实施例中，在接收目标终端发送的资源调用请求之后，接收模块还用于：

[0018] 获取目标对象对应的至少一种权限认证因子；其中，每种权限认证因子表征：相应权限认证方式认证通过的概率。

[0019] 在确定至少一种权限认证因子，满足各自对应的权限认证条件时，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型。

[0020] 一种可选的实施例中，在对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型时，分析模块具体用于：

[0021] 获取日志文件中记录的各个历史对象各自对应的历史行为特征；其中，每个历史对象拥有：至少一种云安全服务需求各自对应的云安全服务资源的资源调用权限。

[0022] 基于目标行为特征与各个历史行为特征之间的特征相似度，确定目标特征行为的行为类型。

[0023] 一种可选的实施例中，在基于目标行为特征与各个历史行为特征之间的特征相似度，确定目标特征行为的行为类型时，分析模块具体用于：

[0024] 若获得的各个特征相似度均小于设定的相似度阈值，则确定目标特征行为的行为类型为异常行为。

[0025] 若各个特征相似度中，存在大于相似度阈值的特征相似度，则确定目标特征行为的行为类型为正常行为。

[0026] 第三方面，本申请提供了一种电子设备，所述电子设备包括：

[0027] 存储器，用于存放计算机程序；

[0028] 处理器，用于执行所述存储器上所存放的计算机程序时，实现上述的一种云安全服务的资源调用方法步骤。

[0029] 第四方面，本申请提供了一种计算机可读存储介质，所述计算机可读存储介质内存储有计算机程序，所述计算机程序被处理器执行时实现上述的一种云安全服务的资源调用方法步骤。

[0030] 第五方面，提供一种计算机程序产品，所述计算机程序产品在被计算机调用时，使得所述计算机执行如第一方面所述的云安全服务的资源调用方法步骤。

[0031] 本申请实施例提供的云安全服务的资源调用方法，接收目标终端发送的资源调用请求之后，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型，从而在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源。采用这种方式，通过对目标行为特征进行特征分析，确定目标行为特征对应的行为类型，从而根据目标行为特征的行为类型，判断是否调用至少一种云安全服务需求各自对应的云安全服务资源，避免了传统方式中，异常对

象在目标终端发出的资源调用请求携带，调用相应的云安全服务资源所需的配置参数时，也可建立与终端之间的安全通信通道，从而进行异常的云安全服务资源调用的技术弊端，提高了云安全服务资源调用的准确性。

附图说明

[0032] 图1示例性示出了本申请实施例所适用的系统架构图；

[0033] 图2示例性示出了本申请实施例提供的一种区块链的结构示意图；

[0034] 图3示例性示出了本申请实施例提供的一种云安全服务的资源调用方法流程示意图；

[0035] 图4示例性示出了本申请实施例提供的一种接收资源调用请求的逻辑示意图；

[0036] 图5示例性示出了本申请实施例提供的一种确定目标特征行为的行为类型的逻辑示意图；

[0037] 图6示例性示出了本申请实施例提供的一种基于图5的逻辑示意图；

[0038] 图7示例性示出了本申请实施例提供的一种调用云安全服务资源的逻辑示意图；

[0039] 图8示例性示出了本申请实施例提供的一种基于图3的逻辑示意图；

[0040] 图9示例性示出了本申请实施例提供的一种云安全服务的资源调用装置的结构示意图；

[0041] 图10示例性示出了本申请实施例提供的一种电子设备的结构示意图。

具体实施方式

[0042] 为了提高云安全服务资源调用的准确性，本申请实施例中，接收目标终端发送的资源调用请求之后，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型，从而在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源。

[0043] 为了更好地理解本申请实施例，下面首先对本申请实施例中涉及的技术术语进行说明。

[0044] (1)Web应用防火墙，(Web Application Firewall，WAF)：又称为网站应用级入侵防御系统，是通过执行一系列针对超文本传输协议(Hyper Text Transfer Protocol，HTTP)/基于安全套接层的超文本传输协议(Hyper Text Transfer Protocol over Secure Socket Layer，HTTPS)的安全策略来专门为Web应用提供保护的一种云安全服务。

[0045] (2)终端检测与响应(Endpoint Detection and Response，EDR)：是一套终端安全解决方案，方案有云端、轻量级的端点安全软件和管理平台软件共同组成。其中，云端主要负责平台的升级、病毒库的升级、云查杀；MGR负责管理维护所有Agent终端，支持统一的终端资产管理、终端病毒查杀、终端合规检查、支持对安全事件的一键隔离处置，以及热点事件失陷指标(Indicators of Compromise，IOC)的全网威胁定位；Agent端点软件支持防病毒功能、入侵防御功能、防火墙隔离功能、数据信息采集上报、一键处置等。

[0046] (3)网络漏洞扫描：是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测(渗透攻击)行为。为了便于描述，本文中，以Vul Scanner作为一种网站漏洞扫描对应的云安全服务为例。

[0047] (4)区块链技术(Blockchain Technology,BT):是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式,用区块链技术所串接的分布式账本能让两方有效纪录交易,且可永久查验此交易。

[0048] 目前的区块链会先对各数据进行分片处理,然后对每个分片中的数据,采用安全哈希算法,分别进行相应哈希运算,再基于每个分片的哈希值构建默克尔树,得到各默克尔根,该默克尔根各数据可作为在区块链中的标识(例如ID值);在构建默克尔树的过程中,一方面需要存储树中间节点,另一方面哈希运算次数多,该区块链中的哈希值存储结构是按照二叉树或*叉树的方式进行构建,这种交易数据的有序性可影响区块链的性能,从而增加了空间存储的负载量,降低了运算速度。

[0049] (5)安全哈希算法(Secure Hash Algorithm,SHA):是一种数据加密算法,该算法的思想是接收一段明文,然后以一种不可逆的方式将它转换成一段(通常更小)密文,也可以简单的理解为取一串输入码(称为预映射或信息),并把它们转化为长度较短、位数固定的输出序列即散列值(也称为信息摘要或信息认证代码)的过程。

[0050] (6)角色的访问控制模型(Role-Based Access Control,RBAC):角色的访问控制模型支持三个著名的安全原则:最小权限原则,责任分离原则和数据抽象原则。在角色的访问控制模型中,权限与角色相关联,用户通过成为适当角色的成员而得到这些角色的权限。这就极大地简化了权限的管理。在一个组织中,角色是为了完成各种工作而创造,用户则依据它的责任和资格来被指派相应的角色,用户可以很容易地从一个角色被指派到另一个角色。角色可依新的需求和系统的合并而赋予新的权限,而权限也可根据需要而从某角色中回收。角色与角色的关系可以建立起来以囊括更广泛的客观情况。

[0051] 需要说明的是,上述技术术语命名方式仅为一种示例,本申请实施例对上述技术术语的命名方式不做限制。

[0052] 下面将结合本发明实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0053] 需要说明的是,在本申请的描述中“多个”理解为“至少两个”。“和/或”,描述关联对象的关联关系,表示可以存在三种关系,例如,A和/或B,可以表示:单独存在A,同时存在A和B,单独存在B这三种情况。A与B连接,可以表示:A与B直接连接和A与B通过C连接这两种情况。另外,在本申请的描述中,“第一”、“第二”等词汇,仅用于区分描述的目的,而不能理解为指示或暗示相对重要性,也不能理解为指示或暗示顺序。

[0054] 图1示例性示出了本申请实施例所适用的系统架构图,如图1所示,该系统架构包括:终端设备101、服务器102以及网络103。其中,终端设备101与服务器102之间可通过无线通信方式或有线通信方式进行信息交互。

[0055] 示例性的,终端设备101可通过蜂窝移动通信技术接入网络103,从而与服务器102进行通信,所述蜂窝移动通信技术,比如,包括第五代移动通信(5th Generation Mobile Networks,5G)技术。

[0056] 可选的，终端设备101可通过短距离无线通信方式接入网络103，从而与服务器102进行通信，所述短距离无线通信方式，比如，包括无线保真(Wireless Fidelity，Wi-Fi)技术。

[0057] 本申请实施例对服务器以及上述其他设备的数量不做限制，图1仅以一个服务器为例进行描述。

[0058] 终端设备101，是一种可以向用户提供语音和/或数据连通性的设备，包括具有无线连接功能的手持式终端设备、车载终端设备等。

[0059] 示例性的，终端设备可以是：手机、平板电脑、笔记本电脑、掌上电脑、移动互联网设备(Mobile Internet Device，MID)、可穿戴设备，虚拟现实(Virtual Reality，VR)设备、增强现实(Augmented Reality，AR)设备、工业控制中的无线终端设备、无人驾驶中的无线终端设备、智能电网中的无线终端设备、运输安全中的无线终端设备、智慧城市中的无线终端设备，或智慧家庭中的无线终端设备等。

[0060] 服务器102，用于接收目标终端发送的资源调用请求；其中，资源调用请求至少包括：目标对象的目标行为特征以及至少一种云安全服务需求；接着，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型；进一步地，在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源。

[0061] 需要说明的是，为了便于理解，本文中，终端设备也称为目标终端。服务器在云安全服务资源调用和数据传输过程中，采用区块链技术，用以保障目标对象的数据和隐私安全，如图2所示，为一种区块链的结构示意图，每个区块链节点包括：当前区块链节点的数据，以及根据当前区块链节点的数据生成的哈希值，以及上一区块链节点的哈希值中的至少一个。

[0062] 可选的，服务器可在预设的安全模块许可采用许可生成算法，根据相应对象的标识信息、云安全服务资源的标识信息、云安全服务资源的特征信息以及相应对象的权限时限，生成相应的哈希值，用于权限认证。其中，许可生成算法可包括：各种安全哈希算法，比如，SHA256算法或者Keccak256算法。

[0063] 进一步地，基于上述系统架构，根据至少一种云安全服务需求，分别进行各自对应的云安全服务资源的调用，参阅图3所示，本申请实施例中，云安全服务的资源调用方法流程，具体步骤如下：

[0064] S301：接收目标终端发送的资源调用请求。

[0065] 具体的，参阅图4所示，在执行步骤S301时，服务器接收目标终端发送的资源调用请求，通过信息解析模块，解析资源调用请求，进而从资源调用请求中，获得各种类型的数据包；进一步地，可根据数据分类模块，从获得的各种数据包中，获得目标对象的目标行为特征以及至少一种云安全服务需求。

[0066] 一种可能的实现方式中，服务站在获得目标对象的目标行为特征，以及至少一种云安全服务需求之后，还可根据数据分类模块，从获得的各种数据包中，获取目标对象的目标哈希值；进一步地，在确定预设的哈希值集合中，存在目标哈希值时，才能对资源调用请求中的目标行为特征进行特征分析，进而确定目标行为特征对应的行为类型；其中，目标哈希值表征：目标对象的特征信息，以及相应的至少一个云安全服务资源各自的特征信息。

[0067] 需要说明的是，服务器设定的哈希值集合中的每个候选哈希值，都是在构造相应区块链节点时，在访问控制模型中，采用安全哈希算法，对相应历史对象的特征信息，以及相应的各个历史云安全服务资源各自的特征信息，进行哈希运算生成的，因此，每个候选哈希值都可实现对相应历史对象身份信息认证。其中，当创建一个新的区块链节点时，需要在资源池中构造区块链节点并广播相应历史对象的特征信息，从而告知区块链已有的各个区块链节点，当前创建的新区块链节点，即将加入该区块链。

[0068] 显而易见的，服务器根据每个区块链节点中，每个候选哈希值与相应历史对象的特征信息，以及相应的各个历史云安全服务资源各自的特征信息之间的映射关系，解决云安全服务资源多个对象共享的问题，确保不同信息之间的隔离，保证了云安全服务资源能够正确分发到相应的目标终端，从而避免了资源抢占及数据泄露。

[0069] 一种可能的实现方式中，服务站在获得目标对象的目标行为特征，以及至少一种云安全服务需求之后，还可根据数据分类模块，从获得的各种数据包中，获取目标对象对应的至少一种权限认证因子；其中，每种权限认证因子表征：相应权限认证方式认证通过的概率，且为不同的权限认证方式，权限认证方式包括：登录密码、短信验证或邮箱验证等权限认证方式。可选的，服务器在确定目标对象多因子认证通过后，确认目标对象的操作权限和数据权限，从而确保准确的调用相应的云安全服务资源。

[0070] 需要说明的是，服务器需要确定至少一种权限认证因子，满足各自对应的权限认证条件时，才能对资源调用请求中的目标行为特征进行特征分析，进而确定目标行为特征对应的行为类型。

[0071] S302：对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型。

[0072] 具体的，参阅图5所示，在执行步骤S302时，服务器在接收目标终端发送的资源调用请求之后，可获取日志文件中记录的各个历史对象各自对应的历史行为特征；进一步地，基于目标行为特征与各个历史行为特征之间的特征相似度，确定目标特征行为的行为类型；其中，每个历史对象拥有：至少一种云安全服务需求各自对应的云安全服务资源的资源调用权限。

[0073] 示例性的，服务器可基于日志文件中记录的各个历史对象各自对应的历史行为特征进行机器学习建模，建立行为分析模型，进而获得目标行为特征与各个历史行为特征之间的特征相似度。该分析模型能够实时从各个历史行为特征各自对应的数据中进行自学习，以保证行为特征分析的准确性；其中，每个历史行为特征可包括：相应的源IP、终端设备信息、网络token、以及相应历史对象的使用习惯(登录时间、活跃度、使用时长等)。

[0074] 进一步地，参阅图6所示，若获得的各个特征相似度均小于设定的相似度阈值，则确定目标特征行为的行为类型为异常行为；若各个特征相似度中，存在大于相似度阈值的特征相似度，则确定目标特征行为的行为类型为正常行为。

[0075] 示例性的，假定日志文件中记录5个历史行为特征，以及设定的相似度阈值为92％，服务器通过分析模型对目标对象的目标行为特征T.M.C，进行特征分析，从而可获得5个历史行为特征，各自与目标行为特征T.M.C之间特征相似度，各历史行为特征各自对应的特征相似度如表1所示：

[0076] 表1

[0077]

历史行为特征	H.M.C1	H.M.C2	H.M.C3	H.M.C4	H.M.C5
特征相似度	T.d1	T.d2	T.d3	T.d4	T.d5
相似度数值	93%	85%	97%	75%	89%

[0078] 由上述表格可知,服务器通过分析模型对目标对象的目标行为特征T.M.C,以及各个历史行为特征进行特征比对分析,从而可获得5个历史行为特征,各自与目标行为特征T.M.C之间特征相似度。例如,服务器通过分析模型对目标行为特征T.M.C,以及历史行为特征H.M.C1进行特征比对分析,可获得目标行为特征T.M.C与历史行为特征H.M.C1之间的特征相似度为T.d1,即,93%,依此类推,不再赘述。

[0079] 进一步地,服务器根据获得各个特征相似度,以及设定的相似度阈值为92%,可知:各个特征相似度中,存在大于相似度阈值的特征相似度,即,93%与97%,则确定目标特征行为T.M.C的行为类型为正常行为。

[0080] 示例性的,仍以表1中的5个历史行为特征和目标行为特征T.M.C为例,服务器可通过各个历史行为特征,各自与目标行为特征T.M.C之间的特征相似度,以及预设的相似度阈值92%,获得各个历史行为特征与目标行为特征T.M.C之间的相似度结果。

[0081] 需要说明的是,相似度结果表征:相应历史行为特征是否与目标行为特征T.M.C相似;若某个历史行为特征与目标行为特征T.M.C之间的特征相似度,大于或等于预设的相似度阈值92%时,则可判定该历史行为特征与目标行为特征T.M.C相似;若某个历史行为特征与目标行为特征T.M.C之间的特征相似度,小于预设的相似度阈值92%时,则可判定该历史行为特征与目标行为特征T.M.C不相似。

[0082] 显而易见的,5个历史行为特征,各自与目标行为特征T.M.C的相似度结果如表2所示:

[0083] 表2

[0084]

历史行为特征	H.M.C1	H.M.C2	H.M.C3	H.M.C4	H.M.C5
相似度数值	93%	85%	97%	75%	89%
相似度结果	相似	不相似	相似	不相似	不相似

[0085] 由上述表格可知,服务器可根据各个历史行为特征,各自与目标行为特征T.M.C的相似度数值,以及预设的相似度阈值92%,分别确定相应的历史行为特征,是否与目标行为特征T.M.C。例如,以历史行为特征H.M.C1为例,通过对比可知,历史行为特征H.M.C1与目标行为特征T.M.C之间的相似度数值为93%,大于预设的相似度阈值92%,则可判定历史行为特征H.M.C1与目标行为特征T.M.C相似;再以历史行为特征H.M.C2为例,通过对比可知,历史行为特征H.M.C2与目标行为特征T.M.C之间的相似度数值为85%,小于预设的相似度阈值92%,则可判定历史行为特征H.M.C2与目标行为特征T.M.C不相似,依此类推。

[0086] 进一步地,服务器可基于上述表2中,5个历史行为特征各自与目标行为特征T.M.C之间的相似度结果,可知:5个历史行为特征中,存在2个与目标行为特征T.M.C的相似度结果为相似的历史行为特征;因此,可判定目标特征行为T.M.C的行为类型属于正常行为。

[0087] 需要说明的是,假设各个历史行为特征中,不存在与目标行为特征之间的相似度结果为相似的历史行为特征,则可判定目标特征行为T.M.C的行为类型属于异常行为。

[0088] 可选的,服务器可直接从目标行为特征与各个历史行为特征之间的特征相似度中,筛选出最大的特征相似度,从而将最大的特征相似度所对应的历史对象,作为目标对

象，进而许可目标对象进行相应的云安全服务资源的调用；其中，最大的特征相似度需大于设定的相似度阈值。

[0089] S303：在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源。

[0090] 具体的，在执行步骤S303时，服务器在确定行为类型为正常行为时，从相应区块链节点预存的云安全服务集合中，根据资源调用请求中的至少一个云安全服务需求，分别调用相应云安全服务需求对应的云安全服务资源。

[0091] 示例性的，参阅图7所示，假定预存的云安全服务集合包括：WAF、EDR以及Vul Scanner三种云安全服务资源，服务器在确定目标行为特征的行为类型为正常行为时，根据资源调用请求中的云安全服务需求，以及预设的对照关系表，从预存的云安全服务集合中，分别调用相应云安全服务需求对应的云安全服务资源。

[0092] 参阅表3所示，为区块链的各个区块链节点各自调用的云安全服务资源。

[0093] 表3

[0094]

区块链节点	Node1	Node2	Node3	Node4	Node5
云安全服务资源	WAF	EDR	WAF、Vul Scanner	WAF、EDR、Vul Scanner	EDR、Vul Scanner

[0095] 由上述表格可知，服务器所采用的区块链中，不同的区块链节点可实现对不同云安服务资源的调用，区块链节点Node1拥有云安全服务资源WAF的资源调度权限；区块链节点Node3拥有云安全服务资源WAF，以及云安全服务资源Vul Scanner的资源调度权限。

[0096] 需要说明的是，区块链具有去中心化、数据透明、不易篡改、可追溯等技术特点，适用于目标对象的身份验证、访问控制，以及对云安全服务资源分发进行全周期的记录。

[0097] 可选的，区块链节点除了记录云安全服务资源与相应对象的信息，还可携带相应的基于角色的访问控制模型，并角色的访问控制模型基于用于目标对象的行为分析和权限认证。

[0098] 基于上述的方法步骤，参阅图8所示，服务器可以根据接收目标终端发送的资源调用请求，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型，在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源；其中，资源调用请求至少包括：目标对象的目标行为特征，以及至少一种云安全服务需求。

[0099] 本申请实施例提供的云安全服务的资源调用方法，接收目标终端发送的资源调用请求之后，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型，从而在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源。采用这种方式，通过对目标行为特征进行特征分析，确定目标行为特征对应的行为类型，从而根据目标行为特征的行为类型，判断是否调用至少一种云安全服务需求各自对应的云安全服务资源，避免了传统方式中，异常对象在目标终端发出的资源调用请求携带，调用相应的云安全服务资源所需的配置参数时，也可建立与终端之间的安全通信通道，从而进行异常的云安全服务资源调用的技术弊端，

提高了云安全服务资源调用的准确性。

[0100] 基于相同的技术构思，本申请实施例还提供了一种云安全服务的资源调用装置，该云安全服务的资源调用装置可以实现本申请实施例的上述方法流程。如图9所示，该云安全服务的资源调用装置包括：接收模块901、分析模块902以及调用模块903，其中：

[0101] 接收模块901，用于接收目标终端发送的资源调用请求；其中，资源调用请求至少包括：目标对象的目标行为特征以及至少一种云安全服务需求。

[0102] 分析模块902，用于对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型。

[0103] 调用模块903，用于在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源。

[0104] 一种可选的实施例中，在接收目标终端发送的资源调用请求之后，接收模块901还用于：

[0105] 从资源调用请求中，获取目标对象对应的目标哈希值；其中，目标哈希值表征：目标对象的特征信息，以及相应的至少一个云安全服务资源各自的特征信息。

[0106] 在确定预设的哈希值集合中，存在目标哈希值时，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型。

[0107] 一种可选的实施例中，在接收目标终端发送的资源调用请求之后，接收模块901还用于：

[0108] 获取目标对象对应的至少一种权限认证因子；其中，每种权限认证因子表征：相应权限认证方式认证通过的概率。

[0109] 在确定至少一种权限认证因子，满足各自对应的权限认证条件时，对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型。

[0110] 一种可选的实施例中，在对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型时，分析模块902具体用于：

[0111] 获取日志文件中记录的各个历史对象各自对应的历史行为特征；其中，每个历史对象拥有：至少一种云安全服务需求各自对应的云安全服务资源的资源调用权限。

[0112] 基于目标行为特征与各个历史行为特征之间的特征相似度，确定目标特征行为的行为类型。

[0113] 一种可选的实施例中，在基于目标行为特征与各个历史行为特征之间的特征相似度，确定目标特征行为的行为类型时，分析模块902具体用于：

[0114] 若获得的各个特征相似度均小于设定的相似度阈值，则确定目标特征行为的行为类型为异常行为。

[0115] 若各个特征相似度中，存在大于相似度阈值的特征相似度，则确定目标特征行为的行为类型为正常行为。

[0116] 基于相同的技术构思，本申请实施例还提供了一种电子设备，该电子设备可实现本申请上述实施例提供的方法流程。在一种实施例中，该电子设备可以是服务器，也可以是终端设备或其他电子设备。如图10所示，该电子设备可包括：

[0117] 至少一个处理器1001，以及与至少一个处理器1001连接的存储器1002，本申请实施例中不限定处理器1001与存储器1002之间的具体连接介质，图10中是以处理器1001和存

储器1002之间通过总线1000连接为例。总线1000在图10中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。总线1000可以分为地址总线、数据总线、控制总线等，为便于表示，图10中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。或者，处理器1001也可以称为控制器，对于名称不做限制。

[0118] 在本申请实施例中，存储器1002存储有可被至少一个处理器1001执行的指令，至少一个处理器1001通过执行存储器1002存储的指令，可以执行前文论述的一种云安全服务的资源调用方法。处理器1001可以实现图9所示的装置中各个模块的功能。

[0119] 其中，处理器1001是该装置的控制中心，可以利用各种接口和线路连接整个该控制设备的各个部分，通过运行或执行存储在存储器1002内的指令以及调用存储在存储器1002内的数据，该装置的各种功能和处理数据，从而对该装置进行整体监控。

[0120] 在一种可能的设计中，处理器1001可包括一个或多个处理单元，处理器1001可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器1001中。在一些实施例中，处理器1001和存储器1002可以在同一芯片上实现，在一些实施例中，它们也可以在独立的芯片上分别实现。

[0121] 处理器1001可以是通用处理器，例如CPU(CPU)、数字信号处理器、专用集成电路、现场可编程门阵列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，可以实现或者执行本申请实施例中公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的一种云安全服务的资源调用方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

[0122] 存储器1002作为一种非易失性计算机可读存储介质，可用于存储非易失性软件程序、非易失性计算机可执行程序以及模块。存储器1002可以包括至少一种类型的存储介质，例如可以包括闪存、硬盘、多媒体卡、卡型存储器、随机访问存储器(Random Access Memory,RAM)、静态随机访问存储器(Static Random Access Memory,SRAM)、可编程只读存储器(Programmable Read Only Memory,PROM)、只读存储器(Read Only Memory,ROM)、带电可擦除可编程只读存储器(Electrically Erasable Programmable Read-Only Memory,EEPROM)、磁性存储器、磁盘、光盘等等。存储器1002是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。本申请实施例中的存储器1002还可以是电路或者其它任意能够实现存储功能的装置，用于存储程序指令和/或数据。

[0123] 通过对处理器1001进行设计编程，可以将前述实施例中介绍的一种云安全服务的资源调用方法所对应的代码固化到芯片内，从而使芯片在运行时能够执行图3所示的实施例的一种云安全服务的资源调用方法的步骤。如何对处理器1001进行设计编程为本领域技术人员所公知的技术，这里不再赘述。

[0124] 基于同一发明构思，本申请实施例还提供一种存储介质，该存储介质存储有计算机指令，当该计算机指令在计算机上运行时，使得计算机执行前文论述的一种云安全服务的资源调用方法。

[0125] 在一些可能的实施方式中，本申请提供一种云安全服务的资源调用方法的各个方

面还可以实现为一种程序产品的形式，其包括程序代码，当程序产品在装置上运行时，程序代码用于使该控制设备执行本说明书上述描述的根据本申请各种示例性实施方式的一种云安全服务的资源调用方法中的步骤。

[0126] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0127] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0128] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0129] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

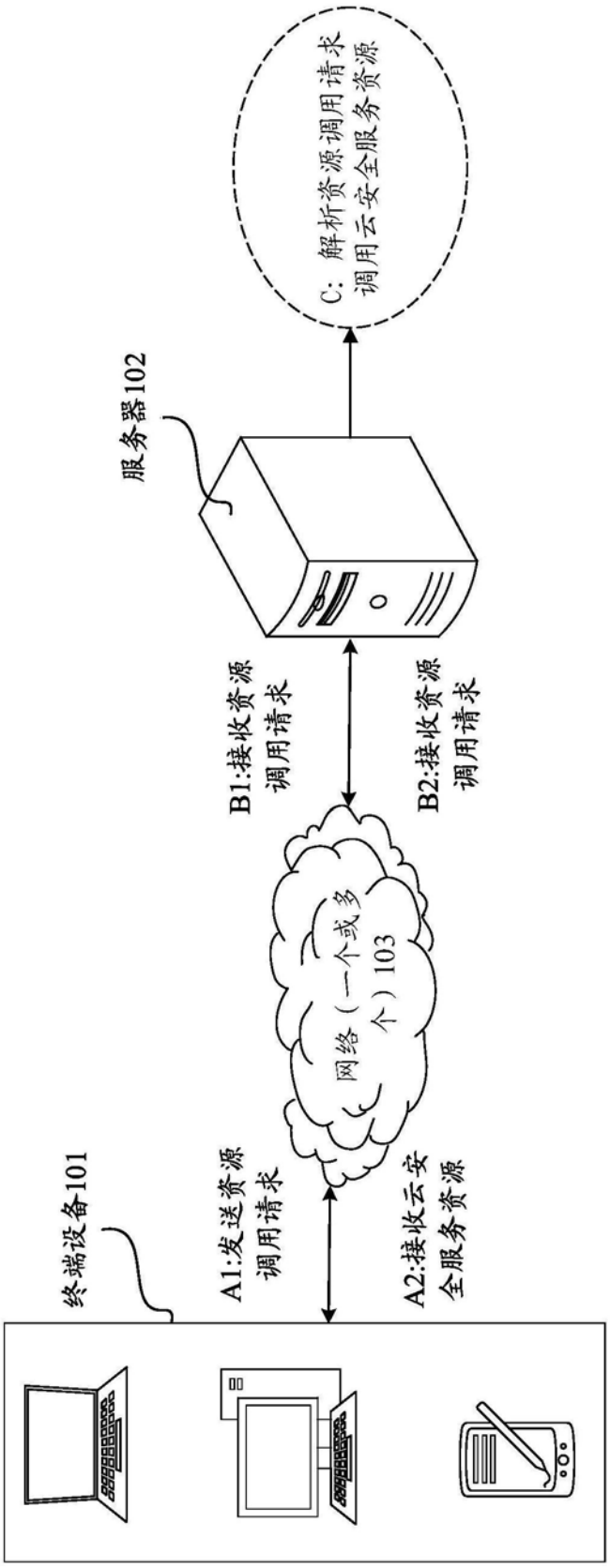

C：解析资源调用请求
调用云安全服务资源
服务器102
B1:接收资源
调用请求
B2:接收资源
调用请求
网络（一个或多
个）103
终端设备101
A1:发送资源
调用请求
A2:接收云安
全服务资源

图1

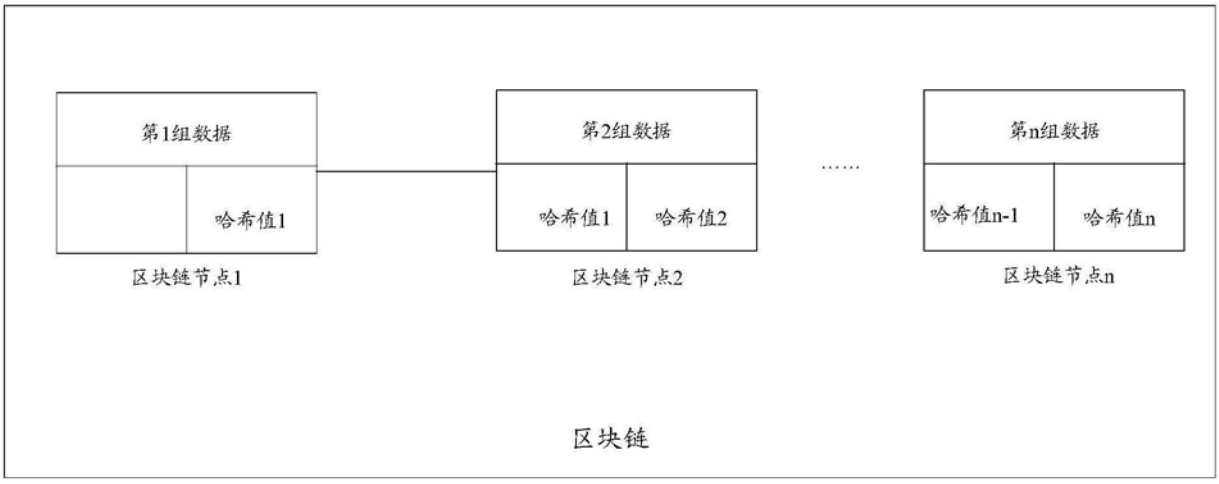

第1组数据
哈希值1
区块链节点1
第2组数据
哈希值1
哈希值2
区块链节点2
……
第n组数据
哈希值n-1
哈希值n
区块链节点n
区块链

图2

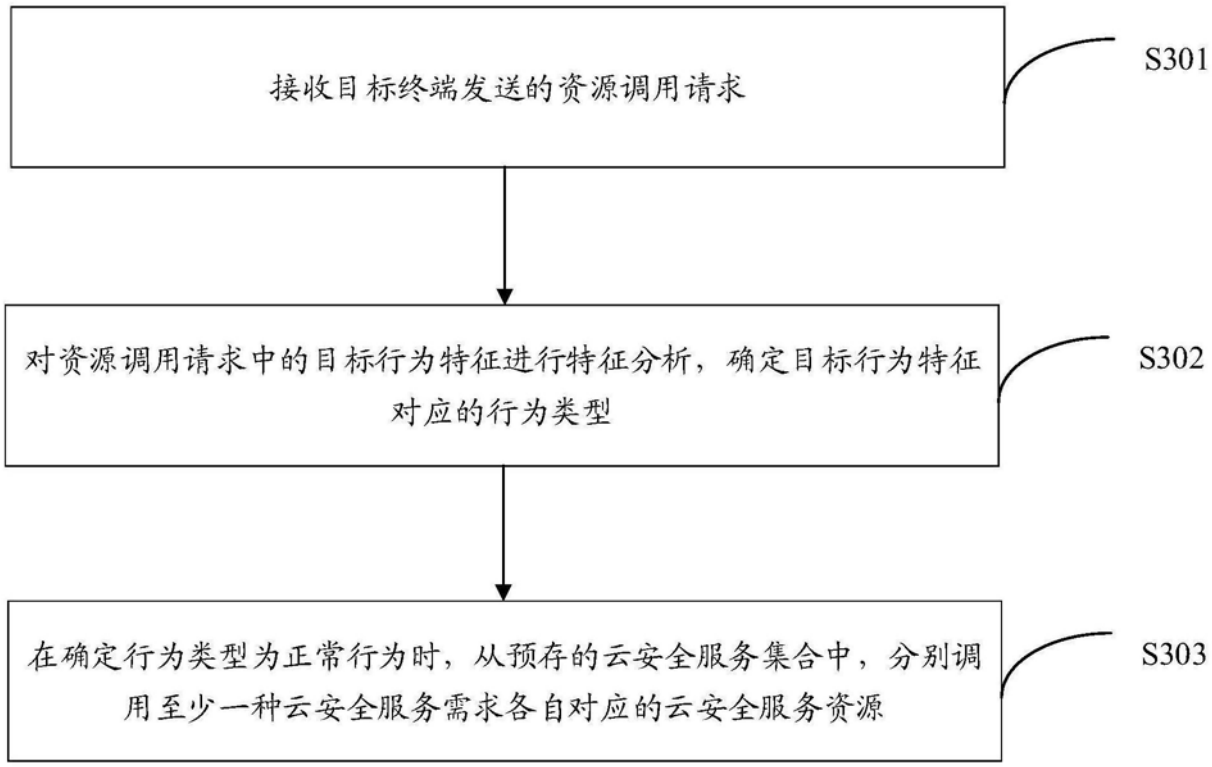

接收目标终端发送的资源调用请求
S301
对资源调用请求中的目标行为特征进行特征分析，确定目标行为特征对应的行为类型
S302
在确定行为类型为正常行为时，从预存的云安全服务集合中，分别调用至少一种云安全服务需求各自对应的云安全服务资源
S303

图3

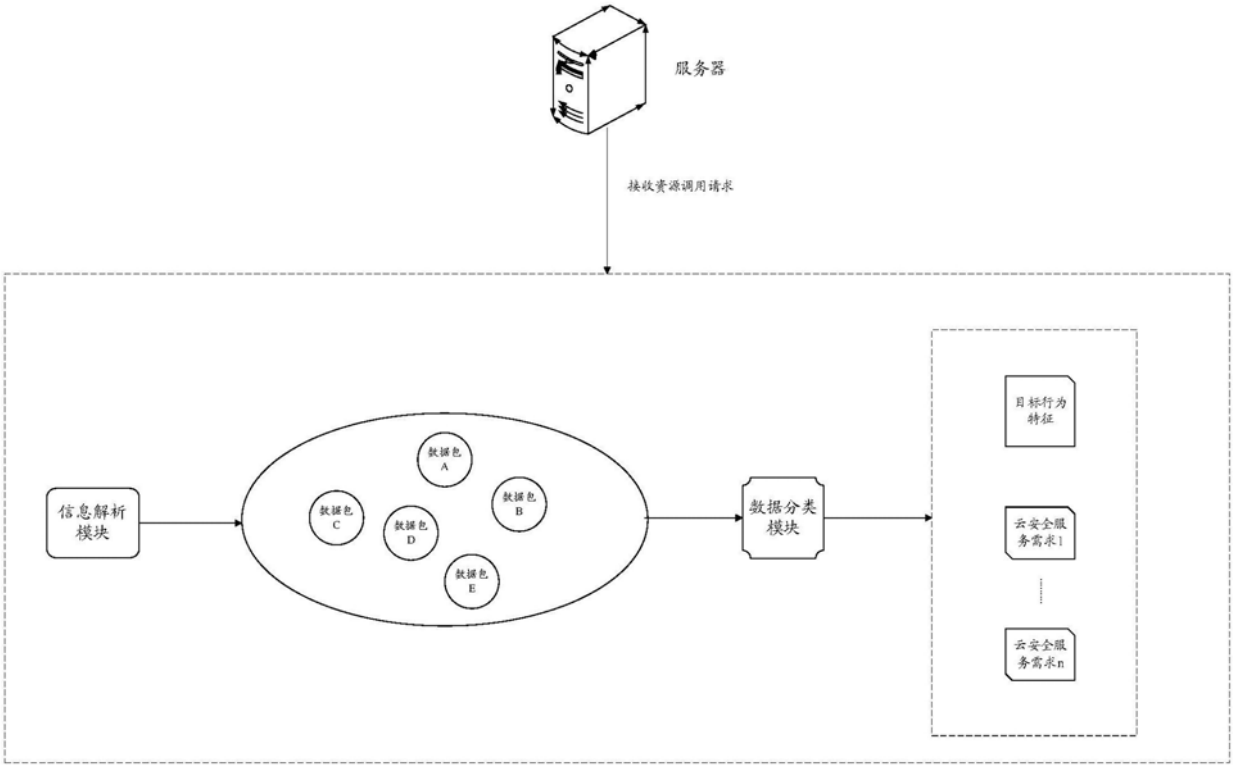

服务器
接收资源调用请求
信息解析模块
数据包A
数据包B
数据包C
数据包D
数据包E
数据分类模块
目标行为特征
云安全服务需求1
云安全服务需求n

图4

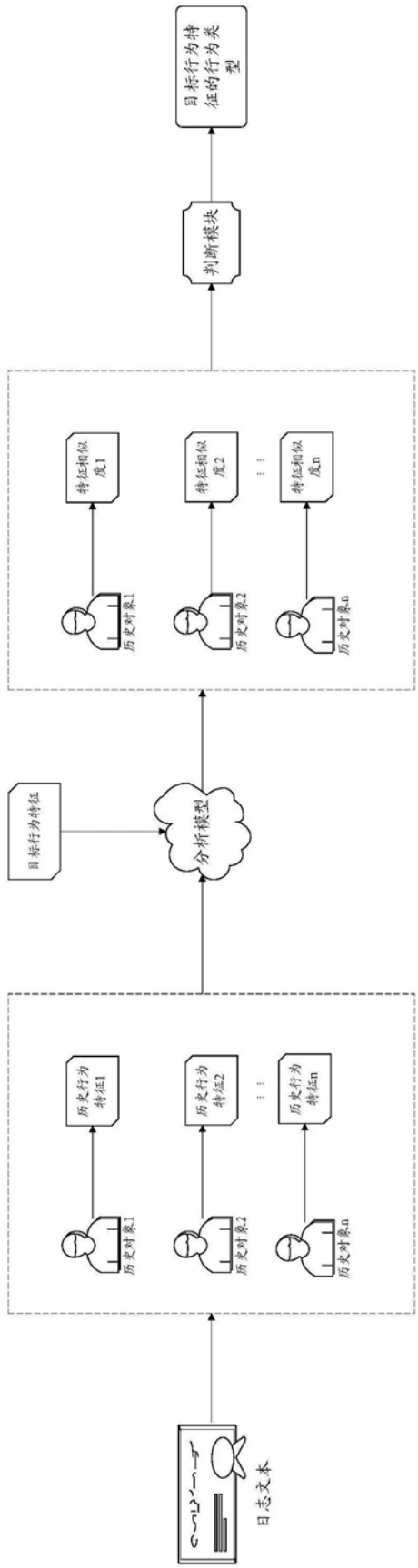

目标行为特征的行为类型
判断模块
特征相似度1
特征相似度2
特征相似度n
历史对象1
历史对象2
历史对象n
目标行为特征
分析模型
历史行为特征1
历史行为特征2
历史行为特征n
历史对象1
历史对象2
历史对象n
日志文本

图5

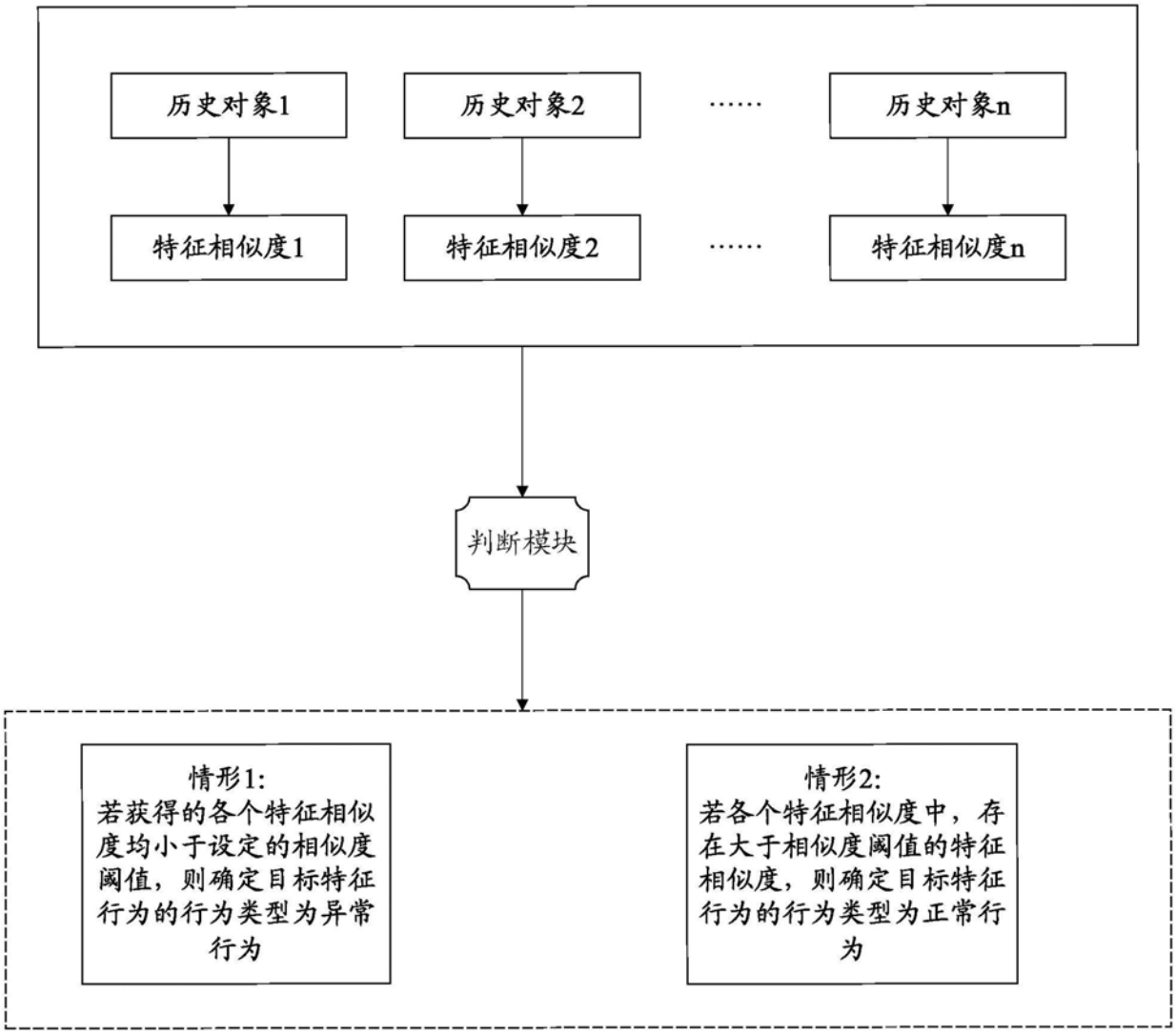

历史对象1
历史对象2
……
历史对象n
特征相似度1
特征相似度2
……
特征相似度n
判断模块
情形1:
若获得的各个特征相似度均小于设定的相似度阈值，则确定目标特征行为的行为类型为异常行为
情形2:
若各个特征相似度中，存在大于相似度阈值的特征相似度，则确定目标特征行为的行为类型为正常行为

图6

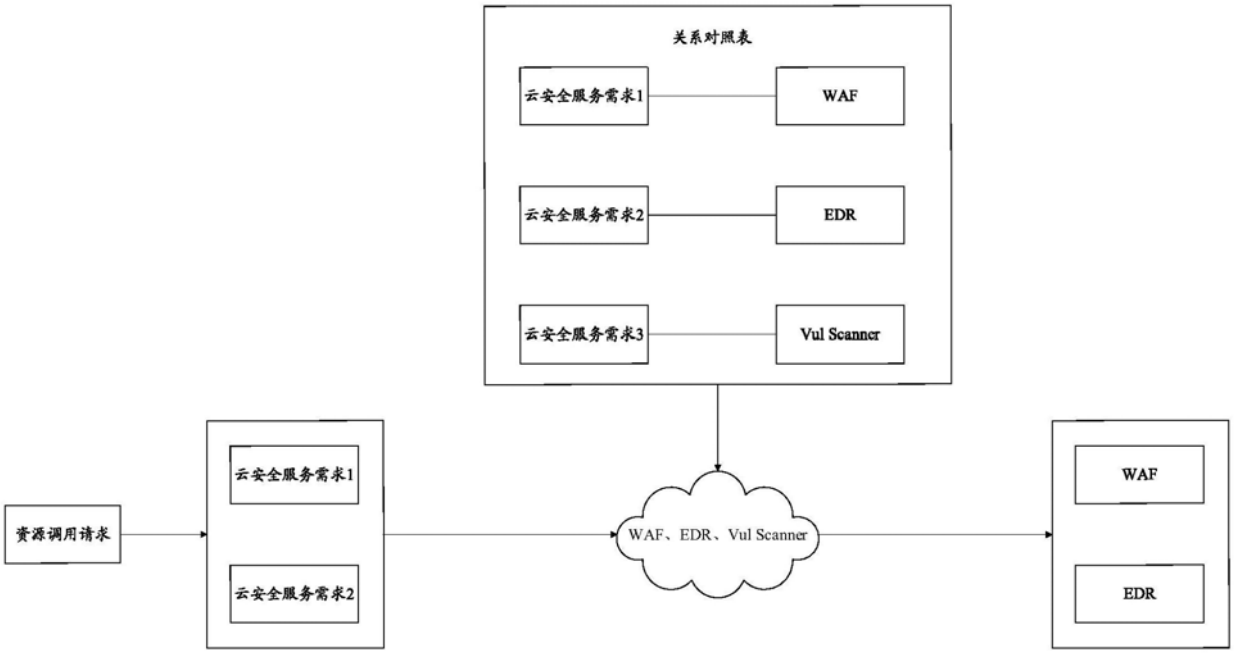

关系对照表
云安全服务需求1
WAF
云安全服务需求2
EDR
云安全服务需求3
Vul Scanner
资源调用请求
云安全服务需求1
云安全服务需求2
WAF、EDR、Vul Scanner
WAF
EDR

图7

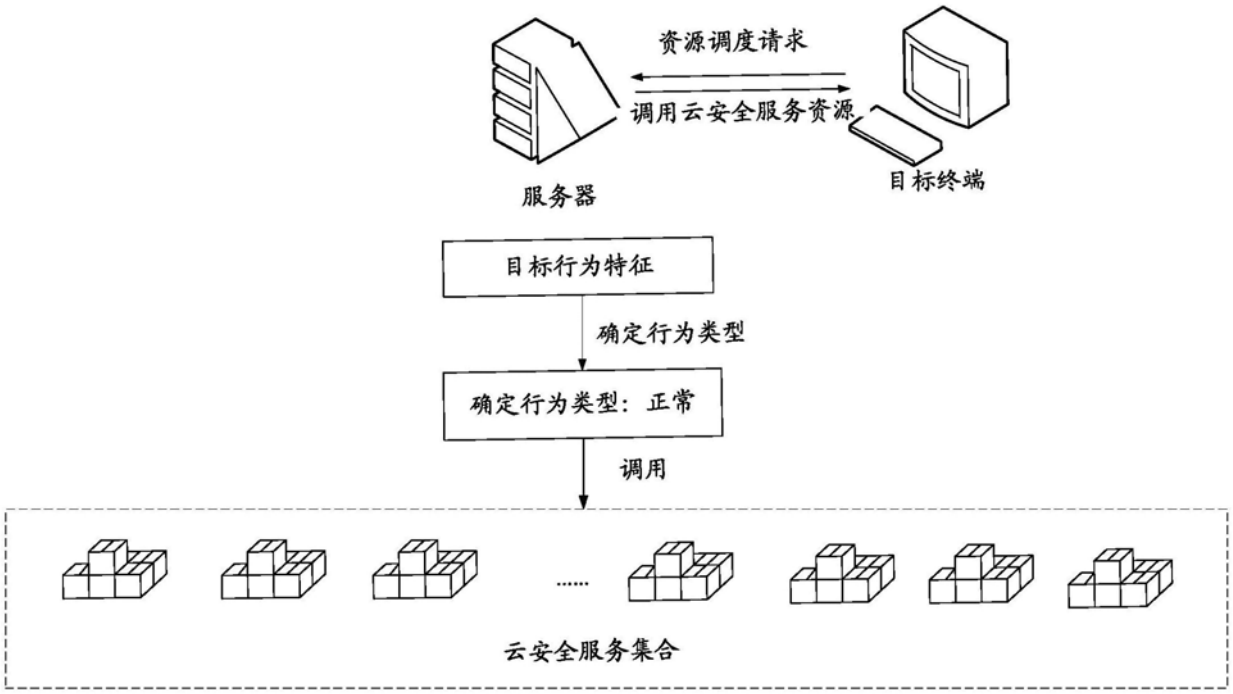

资源调度请求
调用云安全服务资源
服务器
目标终端
目标行为特征
确定行为类型
确定行为类型：正常
调用
.....
云安全服务集合

图8

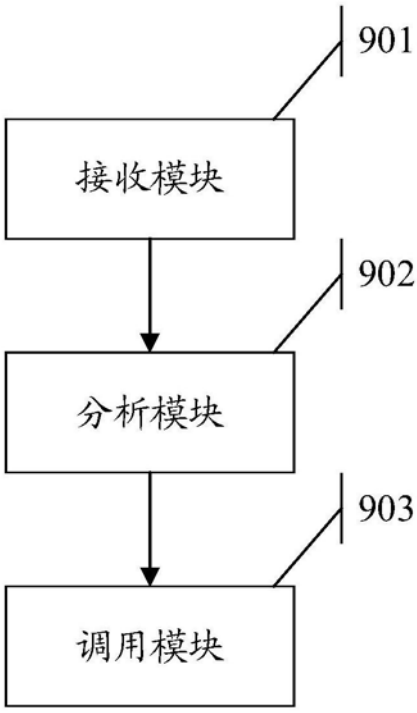


图9

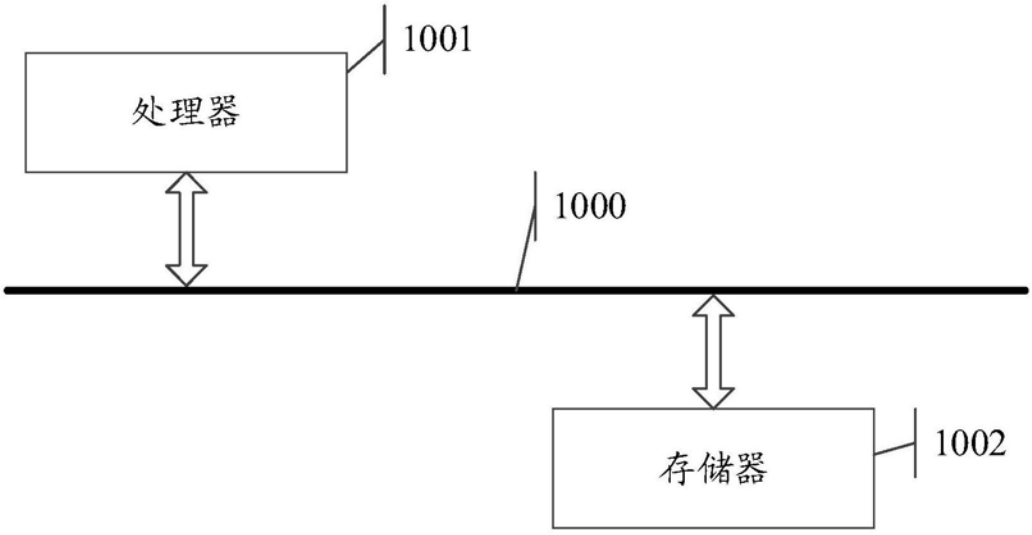


图10