(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117978471 A
(43)申请公布日 2024.05.03

(21)申请号 202410075822.X

(22)申请日 2024.01.18

(71)申请人 南方电网数字电网集团信息通信科技有限公司
地址 510000 广东省广州市黄埔区光谱中路11号2栋3单元12层全层

(72)发明人 金浩 曾子峰 邹洪 张佳发 许伟杰 陈锋 江家伟

(74)专利代理机构 北京品源专利代理有限公司 11332
专利代理师 赵迎迎

(51)Int.Cl.
*H04L 9/40*(2022.01)

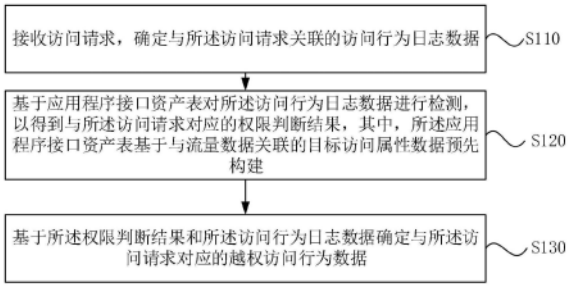
权利要求书2页 说明书10页 附图2页

(54)发明名称

访问请求的越权检测方法、装置、设备及存储介质

(57)摘要

本发明公开了一种访问请求的越权检测方法、装置、设备及存储介质。该方法包括:接收访问请求,确定与所述访问请求关联的访问行为日志数据;基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建;基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据。取到了准确地检测越权行为,提高了安全风险检测的准确性和效率有益效果。




CN 117978471 A

1.一种访问请求的越权检测方法,其特征在于,包括:

接收访问请求,确定与所述访问请求关联的访问行为日志数据;

基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建;

基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据。

2.根据权利要求1所述的方法,其特征在于,所述接收访问请求,确定与所述访问请求关联的访问行为日志数据,包括:

确定与访问请求关联的应用程序接口账号;

对与所述访问请求关联的应用程序接口账号进行验证,以得到目标应用程序接口账号;

确定与所述目标应用程序接口账号关联的初始访问属性数据,基于所述初始访问属性数据自动生成与所述访问请求关联的访问行为日志数据,其中,所述初始访问属性数据包括应用程序接口请求端点数据、访问时间数据和请求方法数据中的至少一种。

3.根据权利要求1所述的方法,其特征在于,所述应用程序接口资产表基于目标访问属性数据预先构建,包括:

获取预设数量的流量数据,提取所述流量数据中的目标流量数据;

基于深度报文解析方法对所述目标流量数据进行深度解析,以得到与目标流量数据关联的目标访问属性数据,其中,所述目标访问属性数据包括目的网络协议数据、目的端口数据、主机数据、应用程序编程接口地址数据以及请求方法数据中的至少一种;

基于所述目标访问属性数构建所述应用程序接口资产表。

4.根据权利要求1所述的方法,其特征在于,所述基于预先构建的应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,包括:

在所述应用程序接口资产表中确定与所述访问行为日志数据对应的权限信息数据,其中,所述权限信息数据包括权限范围数据和/或可执行操作数据;

将所述访问行为日志数据和所述权限信息数据进行比对,以得到与所述访问请求对应的权限判断结果。

5.根据权利要求4所述的方法,其特征在于,所述在所述应用程序接口资产表中确定与所述访问行为日志数据对应的权限信息数据,包括:

基于所述访问行为日志数据中的所述初始访问属性数据在所述应用程序接口资产表中查找与所述初始访问属性数据对应的所述目标访问属性数据;

基于所述目标访问属性数据确定与所述访问行为日志数据对应的权限信息数据。

6.根据权利要求1所述的方法,其特征在于,所述基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据,包括:

基于越权检测算法对所述权限判断结果和访问行为日志数据进行分析,以得到越权访问行为数据。

7.根据权利要求1所述的方法,其特征在于,在所述基于所述权限判断结果确定与访问请求对应的越权访问行为数据之后,还包括:

基于所述越权访问行为数据确定与所述越权访问行为数据对应的安全响应方式,其中,所述安全响应方式包括警报提示、阻止访问和记录异常中的至少一种。

8.一种访问请求的越权检测装置,其特征在于,包括:

请求接收模块,用于接收访问请求,确定与所述访问请求关联的访问行为日志数据;

权限判断模块,用于基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建;

越权分析模块,用于基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据。

9.一种电子设备,其特征在于,所述电子设备包括:

至少一个处理器;以及

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的计算机程序,所述计算机程序被所述至少一个处理器执行,以使所述至少一个处理器能够执行权利要求1-7中任一项所述的访问请求的越权检测方法。

10.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有计算机指令,所述计算机指令用于使处理器执行时实现权利要求1-7中任一项所述的访问请求的越权检测方法。

# 访问请求的越权检测方法、装置、设备及存储介质

## 技术领域

[0001] 本发明涉及数据安全技术领域,尤其涉及一种访问请求的越权检测方法、装置、设备及存储介质。

## 背景技术

[0002] 随着信息技术的飞速发展,应用程序编程接口在各行各业中扮演着日益重要的角色。应用程序编程接口为不同系统之间的数据交流提供了标准化的接口。

[0003] 然而,随之而来的是应用程序编程接口安全性面临的挑战,尤其是账号越权访问问题。当恶意用户或未授权用户通过应用程序编程接口访问获取未授权的信息或执行未经授权的操作时,可能导致敏感数据泄露、系统瘫痪等严重后果。

## 发明内容

[0004] 本发明提供了一种访问请求的越权检测方法、装置、设备及存储介质,以解决越权访问检测准确性较低,导致敏感数据泄露、系统瘫痪的问题。

[0005] 根据本发明的一方面,提供了一种访问请求的越权检测方法,该方法包括:

[0006] 接收访问请求,确定与所述访问请求关联的访问行为日志数据;

[0007] 基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建;

[0008] 基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据。

[0009] 根据本发明的另一方面,提供了一种访问请求的越权检测装置,该装置包括:

[0010] 请求接收模块,用于接收访问请求,确定与所述访问请求关联的访问行为日志数据;

[0011] 权限判断模块,用于基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建;

[0012] 越权分析模块,用于基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据。

[0013] 根据本发明的另一方面,提供了一种电子设备,所述电子设备包括:

[0014] 至少一个处理器;以及

[0015] 与所述至少一个处理器通信连接的存储器;其中,

[0016] 所述存储器存储有可被所述至少一个处理器执行的计算机程序,所述计算机程序被所述至少一个处理器执行,以使所述至少一个处理器能够执行本发明任一实施例所述的访问请求的越权检测方法。

[0017] 根据本发明的另一方面,提供了一种计算机可读存储介质,所述计算机可读存储

介质存储有计算机指令,所述计算机指令用于使处理器执行时实现本发明任一实施例所述的访问请求的越权检测方法。

[0018] 本发明实施例的技术方案,通过接收访问请求,确定与所述访问请求关联的访问行为日志数据;建立访问请求和访问行为日志数据之间的关系;然后,基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建;构建应用程序接口资产表对每个应用程序接口资产的精细化管理,基于应用程序接口资产表对所述访问行为日志数据进行检测,确保了账号只能访问其具备合法权限的应用程序接口,最后,基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据,解决了越权访问检测准确性较低,导致敏感数据泄露、系统瘫痪的问题,取到了准确地检测越权行为,提高了安全风险检测的准确性和效率有益效果。

[0019] 应当理解,本部分所描述的内容并非旨在标识本发明的实施例的关键或重要特征,也不用于限制本发明的范围。本发明的其它特征将通过以下的说明书而变得容易理解。

## 附图说明

[0020] 为了更清楚地说明本发明实施例中的技术方案,下面将对实施例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。

[0021] 图1是根据本发明实施例一提供的一种访问请求的越权检测方法的流程图;

[0022] 图2是根据本发明实施例二提供的一种访问请求的越权检测方法的流程图;

[0023] 图3是根据本发明实施例三提供的一种访问请求的越权检测装置的结构示意图;

[0024] 图4是实现本发明实施例的访问请求的越权检测方法的电子设备的结构示意图。

## 具体实施方式

[0025] 为了使本技术领域的人员更好地理解本发明方案,下面将结合本发明实施例中的附图,对本发明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发明一部分的实施例,而不是全部的实施例。基于本发明中的实施例,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,都应当属于本发明保护的范围。

[0026] 需要说明的是,本发明的说明书和权利要求书及上述附图中的术语“目标”、“初始”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含,例如,包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0027] 实施例一

[0028] 图1为本发明实施例一提供了一种访问请求的越权检测方法的流程图,本实施例

可适用于访问请求检测情况,该方法可以由访问请求的越权检测装置来执行,该访问请求的越权检测装置可以采用硬件和/或软件的形式实现,该访问请求的越权检测装置可配置于电子设备中。如图1所示,该方法包括:

[0029] S110、接收访问请求,确定与所述访问请求关联的访问行为日志数据。

[0030] 其中,访问请求可以理解为API(Application Program Interface)访问请求。访问行为日志数据可以理解为应用程序接口账号的访问行为日志数据。

[0031] 具体的,接收账号访问应用程序接口的请求,确定与所述访问请求关联的访问行为日志数据。

[0032] 可选的,所述接收访问请求,确定与所述访问请求关联的访问行为日志数据,包括:确定与访问请求关联的应用程序接口账号;对与所述访问请求关联的应用程序接口账号进行验证,以得到目标应用程序接口账号;确定与所述目标应用程序接口账号关联的初始访问属性数据,基于所述初始访问属性数据自动生成与所述访问请求关联的访问行为日志数据,其中,所述初始访问属性数据包括应用程序接口请求端点数据、访问时间数据和请求方法数据中的至少一种。

[0033] 其中,应用程序接口账号可以理解为API账号。目标应用程序接口账号可以理解为登录成功的API账号。

[0034] 具体的,接收用户发起的访问请求,基于预设的账号识别规则,识别和验证访问请求中的API账号,以得到登录成功的目标应用程序接口账号。追踪并记录目标应用程序接口账号的访问行为,确定与所述目标应用程序接口账号关联的初始访问属性数据。根据初始访问属性数据自动生成与访问请求关联的访问行为日志数据。其中,账号识别规则可以根据经验预先设定,本实施例不对其进行限制。

[0035] S120、基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建。

[0036] 其中,应用程序接口资产表可以理解为API资产表。权限判断结果可以理解为越权判断结果,权限判断结果包括未越权和越权。

[0037] 具体的,基于预先构建的API资产表对所述访问行为日志数据进行检测,以得到访问请求的权限判断结果是否越权。

[0038] 可选的,所述应用程序接口资产表基于目标访问属性数据预先构建,包括:获取预设数量的流量数据,提取所述流量数据中的目标流量数据;基于深度报文解析方法对所述目标流量数据进行深度解析,以得到与目标流量数据关联的目标访问属性数据,其中,所述目标访问属性数据包括目的网络协议数据、目的端口数据、主机数据、应用程序编程接口地址数据以及请求方法数据中的至少一种;基于所述目标访问属性数构建所述应用程序接口资产表。

[0039] 其中,流量数据可以理解为网络流量数据。目标流量数据可以是HTTP(HyperText Transfer Protocol)流量数据。目标访问属性数据可以理解为与HTTP流量中API流量关联的访问属性数据。

[0040] 具体的,通过部署实时监测系统,对网络流量数据进行实时捕获和记录。并对预设数量的流量数据进行解析,提取网络流量中的HTTP流量。通过深度报文解析方法对HTTP流

量进行深度解析,在HTTP流量中存在的API流量的情况下,确定API流量的目标访问属性数据。基于API流量的目标访问属性数据中的目的网络协议数据、目的端口数据、主机数据、应用程序编程接口地址数据以及请求方法数据构建API资产表。

[0041] 在本发明实施例中,通过解析捕获的网络流量,提取出其中的HTTP流量。然后,对这些HTTP流量进行深度解析,判断其中存在的API流量。基于目的网络协议数据、目的端口数据、主机数据、应用程序编程接口地址数据以及请求方法数据五个字段构建API资产表。对网络中存在的API资产的全面识别。

[0042] S130、基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据。

[0043] 具体的,在所述权限判断结果为越权的情况下,基于与访问请求对应的权限判断结果和访问行为日志数据,确定与访问请求对应的具体越权访问行为数据。

[0044] 可选的,所述基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据,包括:基于越权检测算法对所述权限判断结果和访问行为日志数据进行分析,以得到越权访问行为数据。

[0045] 具体的,基于上下文内容关联分析的越权检测算法对权限判断结果和访问行为日志数据进行分析,进一步分析访问请求的具体越权访问行为数据。

[0046] 在本发明实施例中,在权限判断结果为越权的情况下,基于上下文内容关联分析的越权检测算法对权限判断结果和访问行为日志数据进行进一步分析,可准确确定访问请求存在的具体越权访问行为数据,提高越权检测的准确性。

[0047] 可选的,在所述基于所述权限判断结果确定与访问请求对应的越权访问行为数据之后,还包括:

[0048] 基于所述越权访问行为数据确定与所述越权访问行为数据对应的安全响应方式,其中,所述安全响应方式包括警报提示、阻止访问和记录异常中的至少一种。

[0049] 具体的,可预先针对不同越权访问行为设定对应安全响应等级(例如低级、中级和高级),并针对不同的安全响应等级设置不同安全响应方式,例如:低级越权访问行为可警报提示并阻止访问;中级越权访问行为可记录异常并阻止访问;高级越权访问行为可警报提示、记录异常并阻止访问等。也可直接针对不同的越权访问行为预设对应的安全响应方式。在确定与所述越权访问行为数据对应的安全响应方式后,可生成安全响应指令发送至系统端触发相应的安全响应机制。

[0050] 在本发明实施例中,通过系统采用先进的算法,结合账号访问行为和API资产权限,实现对越权访问行为的实时、准确检测。一旦检测到越权行为,系统将迅速发出警报,防范潜在的安全风险。

[0051] 本发明实施例的技术方案,通过接收访问请求,确定与所述访问请求关联的访问行为日志数据;建立访问请求和访问行为日志数据之间的关系;然后,基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建;构建应用程序接口资产表对每个应用程序接口资产的精细化管理,基于应用程序接口资产表对所述访问行为日志数据进行检测,确保了账号只能访问其具备合法权限的应用程序接口,最后,基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问

行为数据,解决了越权访问检测准确性较低,导致敏感数据泄露、系统瘫痪的问题,取到了准确地检测越权行为,提高了安全风险检测的准确性和效率有益效果。

[0052] 实施例二

[0053] 图2为本发明实施例二提供的一种访问请求的越权检测方法的流程图,本实施例是对上述实施例之间的关系如何基于预先构建的应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果的进一步的细化。可选的,所述基于预先构建的应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,包括:在所述应用程序接口资产表中确定与所述访问行为日志数据对应的权限信息数据,其中,所述权限信息数据包括权限范围数据和/或可执行操作数据;将所述访问行为日志数据和所述权限信息数据进行比对,以得到与所述访问请求对应的权限判断结果。

[0054] 如图2所示,该方法包括:

[0055] S210、接收访问请求,确定与所述访问请求关联的访问行为日志数据。

[0056] S220、在所述应用程序接口资产表中确定与所述访问行为日志数据对应的权限信息数据,其中,所述权限信息数据包括权限范围数据和/或可执行操作数据。

[0057] 其中,权限范围数据可以理解为访问特定API的权限数据。可执行操作数据可以理解为可访问的API接口数据。

[0058] 具体的,在API资产表中确定与访问行为日志数据对应的可访问的API接口数据和/或访问特定API的权限数据。

[0059] 在本发明实施例中,结合API账号的访问行为和API资产表,判断每个API资产的权限是否匹配,确定账号是否有权访问特定API。实现了对API访问的精细化管理,确保只有具备相应权限的账号才能访问相应的API。

[0060] 可选的,所述在所述应用程序接口资产表中确定与所述访问行为日志数据对应的权限信息数据,包括:基于所述访问行为日志数据中的所述初始访问属性数据在所述应用程序接口资产表中查找与所述初始访问属性数据对应的所述目标访问属性数据;基于所述目标访问属性数据确定与所述访问行为日志数据对应的权限信息数据。

[0061] 其中,初始访问属性数据可以理解为访问行为日志数据中的所有访问属性数据。

[0062] 具体的,基于初始访问属性数据检索API资产表,在API资产表中查找与所述初始访问属性数据对应的所述目标访问属性数据;基于目标访问属性数据中的目的网络协议数据、目的端口数据、主机数据、应用程序编程接口地址数据以及请求方法数据确定与所述访问行为日志数据对应的权限信息数据。

[0063] S230、将所述访问行为日志数据和所述权限信息数据进行比对,以得到与所述访问请求对应的权限判断结果。

[0064] 具体的,将访问行为日志数据与所述访问行为日志数据对应的权限信息数据进行比对,判断访问请求的权限信息是否匹配一级确定应用程序接口账号是否有权访问特定的API。基于比对结果确定与所述访问请求对应的权限判断结果。

[0065] 在本实施例中,通过对API资产表的细致解析,系统能够准确判断每个API资产的权限范围,包括读取、写入、删除等操作,为系统提供了细粒度的权限控制。

[0066] S240、基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应

的越权访问行为数据。

[0067] 本发明实施例的技术方案,通过在所述应用程序接口资产表中确定与所述访问行为日志数据对应的权限信息数据,其中,所述权限信息数据包括权限范围数据和/或可执行操作数据;准确确定访问请求对应的权限范围和/或可执行操作。然后,将所述访问行为日志数据和所述权限信息数据进行比对,以得到与所述访问请求对应的权限判断结果,实现了对应用程序接口访问的精细化管理,确保只有具备相应权限的账号才能访问相应的应用程序接口。

[0068] 作为本发明实施例一可选实例,本实施例的访问请求的越权检测具体包括以下步骤:

[0069] 步骤1.数据接入:

[0070] 实时流量监测:部署实时监测系统,对网络流量进行实时捕获和记录。

[0071] 步骤2.API资产识别

[0072] 通过对流网络量进行解析,提取出流量中的HTTP流量,并对HTTP流量进行深度解析,判断其中存在的API流量,基于API流量的目的网络协议数据、目的端口数据、主机数据、应用程序编程接口地址数据以及请求方法数据五个字段构建API资产表。

[0073] 步骤3.API账号识别:

[0074] 输入:访问请求。

[0075] 处理:系统通过预设账号识别规则,识别和验证请求中的应用程序接口账号。其中,账号识别规则可以自定义配置账号识别规则,本实施例不对其进行限制。

[0076] 输出:被识别和验证的应用程序接口账号信息。

[0077] 步骤4.访问行为记录:

[0078] 输入:通过应用程序接口账号识别后的至少一个应用程序接口账号信息。

[0079] 处理:确定与所述目标应用程序接口账号关联的初始访问属性数据,基于所述初始访问属性数据自动生成与所述访问请求关联的访问行为日志数据,其中,所述初始访问属性数据包括应用程序接口请求端点数据、访问时间数据和请求方法数据中的至少一种。

[0080] 输出:访问行为日志数据。

[0081] 步骤5.API资产表检索:

[0082] 输入:至少一个与所述访问请求关联的访问行为日志数据。

[0083] 处理:系统根据访问行为日志数据检索API资产表,获取每个API资产的权限信息数据,包括权限范围数据和/或可执行操作数据。

[0084] 输出:API资产表中与访问行为相关的网络协议数据、目的端口数据、主机数据、应用程序编程接口地址数据以及请求方法数据。

[0085] 步骤6.权限判断:

[0086] 输入:应用程序接口账号的访问行为日志数据和API资产表中与访问行为相关的网络协议数据、目的端口数据、主机数据、应用程序编程接口地址数据以及请求方法数据。

[0087] 处理:系统根据访问请求关联的访问行为日志数据和API资产表,判断每个API资产的权限是否匹配,确定应用程序接口账号是否有权访问特定应用程序接口。

[0088] 输出:与所述访问请求对应的权限判断结果。

[0089] 步骤7.越权检测:

[0090] 输入:访问请求关联的访问行为日志数据和访问请求对应的权限判断结果。

[0091] 处理:系统基于上下文内容关联分析实现的越权检测算法对所述权限判断结果和访问行为日志数据进行分析。

[0092] 输出:越权访问行为数据。

[0093] 步骤8.安全响应:

[0094] 输入:越权访问行为数据。

[0095] 处理:基于所述越权访问行为数据确定与所述越权访问行为数据对应的安全响应方式。

[0096] 输出:安全响应指令。

[0097] 本发明实施例的技术方案,通过实时跟踪和记录每个API账号的访问行为,包括请求的API端点、访问时间、请求方法等,形成全面的访问行为日志。通过API资产表检索,获取每个API资产的详细信息,包括权限范围、可执行操作等,为后续权限判断提供充足的依据。结合API账号的访问行为和API资产表,系统实现对每个API资产的权限判断,确保账号只能访问其具备合法权限的API。利用先进的越权检测算法,对账号的访问行为和权限判断结果进行实时分析,准确检测是否存在越权访问行为。提高了对非法访问行为的检测准确率,及时发现潜在的安全风险,提高了系统的安全防护能力。

[0098] 实施例三

[0099] 图3为本发明实施例三提供的一种访问请求的越权检测装置的结构示意图。如图3所示,该装置包括:请求接收模块310、权限判断模块320和越权分析模块330。

[0100] 其中,请求接收模块310,用于接收访问请求,确定与所述访问请求关联的访问行为日志数据;权限判断模块320,用于基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建;越权分析模块330,用于基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据。

[0101] 本发明实施例的技术方案,通过请求接收模块,接收访问请求,确定与所述访问请求关联的访问行为日志数据;建立访问请求和访问行为日志数据之间的关系;然后,通过权限判断模块,基于应用程序接口资产表对所述访问行为日志数据进行检测,以得到与所述访问请求对应的权限判断结果,其中,所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建;构建应用程序接口资产表对每个应用程序接口资产的精细化管理,基于应用程序接口资产表对所述访问行为日志数据进行检测,确保了账号只能访问其具备合法权限的应用程序接口,最后,通过权限判断模块,基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据,解决了越权访问检测准确性较低,导致敏感数据泄露、系统瘫痪的问题,取到了准确地检测越权行为,提高了安全风险检测的准确性和效率有益效果。

[0102] 可选的,所述请求接收模块包括:

[0103] 账号确定单元,用于确定与访问请求关联的应用程序接口账号;

[0104] 账号验证单元,用于对与所述访问请求关联的应用程序接口账号进行验证,以得到目标应用程序接口账号;

[0105] 日志生成单元,用于确定与所述目标应用程序接口账号关联的初始访问属性数

据,基于所述初始访问属性数据自动生成与所述访问请求关联的访问行为日志数据,其中,所述初始访问属性数据包括应用程序接口请求端点数据、访问时间数据和请求方法数据中的至少一种。

[0106] 可选的,所述权限判断模块包括:

[0107] 流量获取单元,用于获取预设数量的流量数据,提取所述流量数据中的目标流量数据;

[0108] 属性数据获取单元,用于基于深度报文解析方法对所述目标流量数据进行深度解析,以得到与目标流量数据关联的目标访问属性数据,其中,所述目标访问属性数据包括目的网络协议数据、目的端口数据、主机数据、应用程序编程接口地址数据以及请求方法数据中的至少一种;

[0109] 资产表构建单元,用于基于所述目标访问属性数构建所述应用程序接口资产表。

[0110] 可选的,所述权限判断模块包括:

[0111] 权限确定单元,用于在所述应用程序接口资产表中确定与所述访问行为日志数据对应的权限信息数据,其中,所述权限信息数据包括权限范围数据和/或可执行操作数据;

[0112] 权限判断单元,用于将所述访问行为日志数据和所述权限信息数据进行比对,以得到与所述访问请求对应的权限判断结果。

[0113] 可选的,所述权限确定单元包括:

[0114] 属性数据查找子单元,用于基于所述访问行为日志数据中的所述初始访问属性数据在所述应用程序接口资产表中查找与所述初始访问属性数据对应的所述目标访问属性数据;

[0115] 权限信息确定子单元,用于基于所述目标访问属性数据确定与所述访问行为日志数据对应的权限信息数据。

[0116] 可选的,所述越权分析模块具体用于:

[0117] 基于越权检测算法对所述权限判断结果和访问行为日志数据进行分析,以得到越权访问行为数据。

[0118] 可选的,所述装置还包括安全响应模块。

[0119] 所述安全响应模块,用于在所述基于所述权限判断结果确定与访问请求对应的越权访问行为数据之后,基于所述越权访问行为数据确定与所述越权访问行为数据对应的安全响应方式,其中,所述安全响应方式包括警报提示、阻止访问和记录异常中的至少一种。

[0120] 本发明实施例所提供的访问请求的越权检测装置可执行本发明任意实施例所提供的访问请求的越权检测方法,具备执行方法相应的功能模块和有益效果。

[0121] 实施例四

[0122] 图4示出了可以用来实施本发明的实施例的电子设备10的结构示意图。电子设备旨在表示各种形式的数字计算机,诸如,膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动装置,诸如,个人数字处理、蜂窝电话、智能电话、可穿戴设备(如头盔、眼镜、手表等)和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例,并且不意在限制本文中描述的和/或者要求的本发明的实现。

[0123] 如图4所示,电子设备10包括至少一个处理器11,以及与至少一个处理器11通信连

接的存储器,如只读存储器(ROM)12、随机访问存储器(RAM)13等,其中,存储器存储有可被至少一个处理器执行的计算机程序,处理器11可以根据存储在只读存储器(ROM)12中的计算机程序或者从存储单元18加载到随机访问存储器(RAM)13中的计算机程序,来执行各种适当的动作和处理。在RAM 13中,还可存储电子设备10操作所需的各种程序和数据。处理器11、ROM 12以及RAM 13通过总线14彼此相连。输入/输出(I/O)接口15也连接至总线14。

[0124] 电子设备10中的多个部件连接至I/O接口15,包括:输入单元16,例如键盘、鼠标等;输出单元17,例如各种类型的显示器、扬声器等;存储单元18,例如磁盘、光盘等;以及通信单元19,例如网卡、调制解调器、无线通信收发机等。通信单元19允许电子设备10通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

[0125] 处理器11可以是各种具有处理和计算能力的通用和/或专用处理组件。处理器11的一些示例包括但不限于中央处理单元(CPU)、图形处理单元(GPU)、各种专用的人工智能(AI)计算芯片、各种运行机器学习模型算法的处理器、数字信号处理器(DSP)、以及任何适当的处理器、控制器、微控制器等。处理器11执行上文所描述的各个方法和处理,例如方法访问请求的越权检测。

[0126] 在一些实施例中,方法访问请求的越权检测可被实现为计算机程序,其被有形地包含于计算机可读存储介质,例如存储单元18。在一些实施例中,计算机程序的部分或者全部可以经由ROM 12和/或通信单元19而被载入和/或安装到电子设备10上。当计算机程序加载到RAM 13并由处理器11执行时,可以执行上文描述的方法访问请求的越权检测的一个或多个步骤。备选地,在其他实施例中,处理器11可以通过其他任何适当的方式(例如,借助于固件)而被配置为执行方法访问请求的越权检测。

[0127] 本文中以上描述的系统和技术的各种实施方式可以在数字电子电路系统、集成电路系统、场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、芯片上系统的系统(SOC)、负载可编程逻辑设备(CPLD)、计算机硬件、固件、软件、和/或它们的组合中实现。这些各种实施方式可以包括:实施在一个或者多个计算机程序中,该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释,该可编程处理器可以是专用或者通用可编程处理器,可以从存储系统、至少一个输入装置、和至少一个输出装置接收数据和指令,并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至少一个输出装置。

[0128] 用于实施本发明的方法的计算机程序可以采用一个或多个编程语言的任何组合来编写。这些计算机程序可以提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器,使得计算机程序当由处理器执行时使流程图和/或框图中所规定的功能/操作被实施。计算机程序可以完全在机器上执行、部分地在机器上执行,作为独立软件包部分地在机器上执行且部分地在远程机器上执行或完全在远程机器或服务器上执行。

[0129] 在本发明的上下文中,计算机可读存储介质可以是有形的介质,其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合地使用的计算机程序。计算机可读存储介质可以包括但不限于电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备,或者上述内容的任何合适组合。备选地,计算机可读存储介质可以是机器可读信号介质。机器可读存储介质的更具体示例会包括基于一个或多个线的电气连接、便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只

读存储器(EPROM或快闪存储器)、光纤、便捷式紧凑盘只读存储器(CD-ROM)、光学储存设备、磁储存设备、或上述内容的任何合适组合。

[0130] 为了提供与用户的交互,可以在电子设备上实施此处描述的系统和技术,该电子设备具有:用于向用户显示信息的显示装置(例如,CRT(阴极射线管)或者LCD(液晶显示器)监视器);以及键盘和指向装置(例如,鼠标或者轨迹球),用户可以通过该键盘和该指向装置来将输入提供给电子设备。其它种类的装置还可以用于提供与用户的交互;例如,提供给用户的反馈可以是任何形式的传感反馈(例如,视觉反馈、听觉反馈、或者触觉反馈);并且可以用任何形式(包括声输入、语音输入或者、触觉输入)来接收来自用户的输入。

[0131] 可以将此处描述的系统和技术实施在包括后台部件的计算系统(例如,作为数据服务器)、或者包括中间件部件的计算系统(例如,应用服务器)、或者包括前端部件的计算系统(例如,具有图形用户界面或者网络浏览器的用户计算机,用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如,通信网络)来将系统的部件相互连接。通信网络的示例包括:局域网(LAN)、广域网(WAN)、区块链网络和互联网。

[0132] 计算系统可以包括客户端和服务器。客户端和服务器一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。服务器可以是云服务器,又称为云计算服务器或云主机,是云计算服务体系中的一项主机产品,以解决了传统物理主机与VPS服务中,存在的管理难度大,业务扩展性弱的缺陷。

[0133] 应该理解,可以使用上面所示的各种形式的流程,重新排序、增加或删除步骤。例如,本发明中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行,只要能够实现本发明的技术方案所期望的结果,本文在此不进行限制。

[0134] 上述具体实施方式,并不构成对本发明保护范围的限制。本领域技术人员应该明白的是,根据设计要求和其他因素,可以进行各种修改、组合、子组合和替代。任何在本发明的精神和原则之内所作的修改、等同替换和改进等,均应包含在本发明保护范围之内。

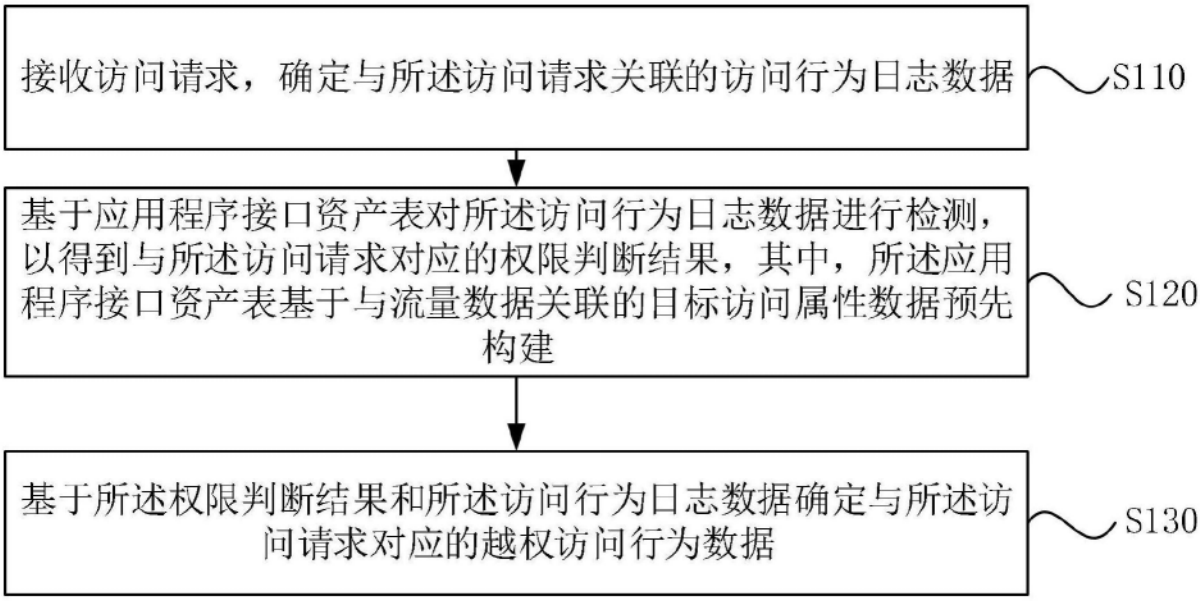

接收访问请求，确定与所述访问请求关联的访问行为日志数据
S110
基于应用程序接口资产表对所述访问行为日志数据进行检测，以得到与所述访问请求对应的权限判断结果，其中，所述应用程序接口资产表基于与流量数据关联的目标访问属性数据预先构建
S120
基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据
S130

图1

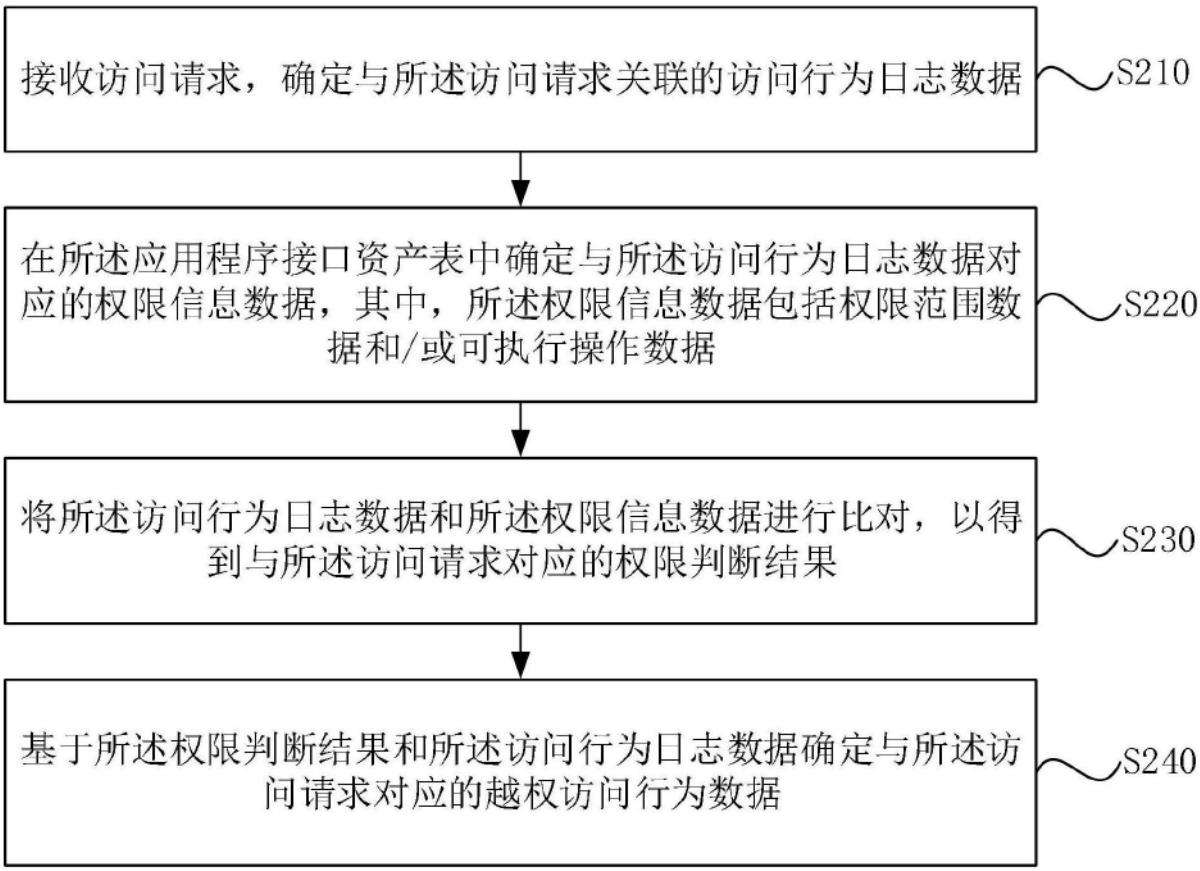

接收访问请求，确定与所述访问请求关联的访问行为日志数据
S210
在所述应用程序接口资产表中确定与所述访问行为日志数据对应的权限信息数据，其中，所述权限信息数据包括权限范围数据和/或可执行操作数据
S220
将所述访问行为日志数据和所述权限信息数据进行比对，以得到与所述访问请求对应的权限判断结果
S230
基于所述权限判断结果和所述访问行为日志数据确定与所述访问请求对应的越权访问行为数据
S240

图2

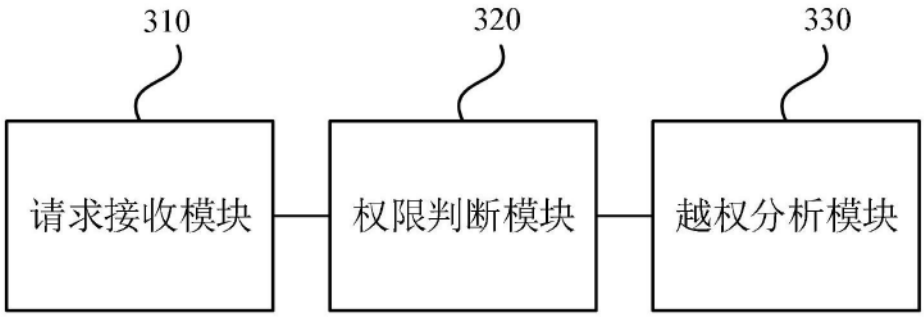

310
320
330
请求接收模块
权限判断模块
越权分析模块

图3

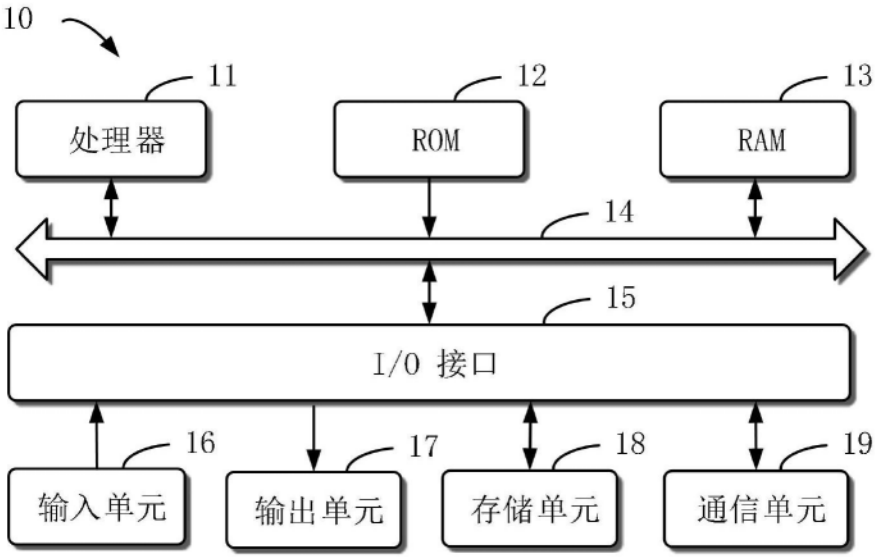

10
11
12
13
处理器
ROM
RAM
14
15
I/O 接口
16
17
18
19
输入单元
输出单元
存储单元
通信单元

图4