



(12)发明专利

(10)授权公告号 CN 106778303 B

(45)授权公告日 2020.03.17

(21)申请号 201611115873.2

(22)申请日 2016.12.07

(65)同一申请的已公布的文献号
申请公布号 CN 106778303 A

(43)申请公布日 2017.05.31

(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市南山区高新区
科技中一路腾讯大厦35层

(72)发明人 袁哲

(74)专利代理机构 深圳翼盛智成知识产权事务
所(普通合伙) 44300

代理人 黄威

(51)Int.Cl.
G06F 21/60(2013.01)

(56)对比文件

CN 101339591 A,2009.01.07,
CN 103198361 A,2013.07.10,
CN 103810441 A,2014.05.21,
CN 104077532 A,2014.10.01,
CN 104462024 A,2015.03.25,
汤庆新 等.基于日志分析的数据资源授权
策略评估.《计算机系统应用》.2016,第25卷(第6
期),第265-268页.

审查员 王秋苹

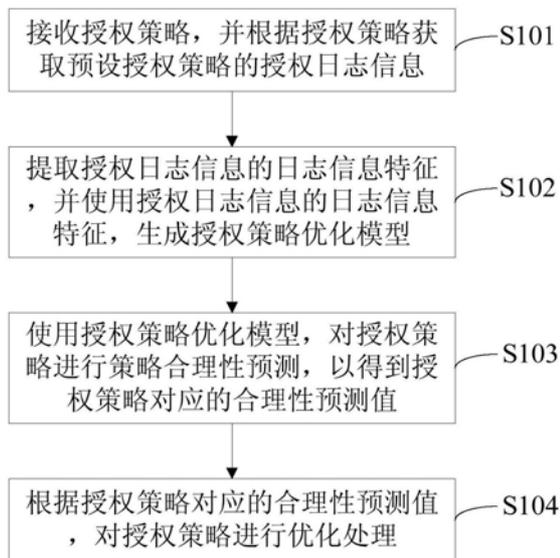
权利要求书2页 说明书11页 附图6页

(54)发明名称

授权策略优化方法及授权策略优化装置

(57)摘要

本发明提供一种授权策略优化方法,其包括:接收授权策略,并根据授权策略获取预设授权策略的授权日志信息;提取授权日志信息的日志信息特征,并使用授权日志信息的日志信息特征,生成授权策略优化模型;使用授权策略优化模型,对授权策略进行策略合理性预测,以得到授权策略对应的合理性预测值;以及根据授权策略对应的合理性预测值,对授权策略进行优化处理。本发明还提供一种授权策略优化装置,本发明的授权策略优化方法及授权策略优化装置实时生成授权策略优化模型对授权策略进行合理性预测,并使用推荐预设授权策略对授权策略进行优化处理,实现了授权策略优化的精细化处理。



1. 一种授权策略优化方法,其特征在于,包括:

接收用户输入的授权策略,并根据所述授权策略获取预设授权策略的授权日志信息,所述预设授权策略是指用来建立授权策略优化模型的授权策略;

提取所述授权日志信息的日志信息特征,对所述日志信息特征进行特征离散化处理或生成对应的组合特征,得到优化处理后的日志信息特征;

基于预设规则对所述优化处理后的日志信息特征进行训练样本选取;

根据所述训练样本的离散化或连续化特征属性,使用预设模型算法进行模型训练,以实时生成授权策略优化模型;

使用所述授权策略优化模型,对所述授权策略进行策略合理性预测,以得到所述授权策略对应的合理性预测值;以及

根据所述授权策略对应的合理性预测值,对所述授权策略进行优化处理。

2. 根据权利要求1所述的授权策略优化方法,其特征在于,所述根据所述授权策略对应的合理性预测值,对所述授权策略进行优化处理的步骤包括:

判断所述合理性预测值是否小于等于设定值;

如所述合理性预测值小于等于所述设定值,则提示用户对所述授权策略进行优化处理;

如所述合理性预测值大于所述设定值,则提示所述授权策略为合理性策略。

3. 根据权利要求1所述的授权策略优化方法,其特征在于,所述授权策略优化方法还包括步骤:

获取所述授权策略优化模型的至少一个推荐预设授权策略,其中所述推荐预设授权策略的合理性预测值大于所述授权策略优化模型中其他预设授权策略的合理性预测值;

所述根据所述授权策略对应的合理性预测值,对所述授权策略进行优化处理的步骤包括:

判断所述合理性预测值是否小于等于设定值;

如所述合理性预测值小于等于所述设定值,则发送所述至少一个推荐预设授权策略,以便用户对所述授权策略进行优化处理;

如所述合理性预测值大于所述设定值,则提示所述授权策略为合理性策略。

4. 根据权利要求1所述的授权策略优化方法,其特征在于,所述授权策略优化方法还包括步骤:

通过鉴权系统的鉴权日志以及业务服务器的业务关联日志,获取所述预设授权策略的授权日志信息。

5. 根据权利要求1所述的授权策略优化方法,其特征在于,所述日志信息特征包括用户特征、行为特征、授权策略特征以及鉴权目标值特征。

6. 一种授权策略优化装置,其特征在于,包括:

策略接收模块,用于接收用户输入的授权策略,并根据所述授权策略获取预设授权策略的授权日志信息,所述预设授权策略是指用来建立授权策略优化模型的授权策略;

模型生成模块,包括特征优化处理单元、训练样本选取单元以及模型生成单元;

所述特征优化处理单元,用于提取所述授权日志信息的日志信息特征,对所述日志信息特征进行特征离散化处理或生成对应的组合特征,得到优化处理后的日志信息特征;

所述训练样本选取单元,用于基于预设规则对优化处理后的日志信息特征进行训练样本选取;

所述模型生成单元,用于根据所述训练样本的离散化或连续化特征属性,使用预设模型算法进行模型训练,以实时生成授权策略优化模型;

策略合理性预测模块,用于使用所述授权策略优化模型,对所述授权策略进行策略合理性预测,以得到所述授权策略对应的合理性预测值;以及

优化处理模块,用于根据所述授权策略对应的合理性预测值,对所述授权策略进行优化处理。

7. 根据权利要求6所述的授权策略优化装置,其特征在于,所述优化处理模块包括:

判断单元,用于判断所述合理性预测值是否小于等于设定值;

优化处理单元,用于如所述合理性预测值小于等于所述设定值,则提示用户对所述授权策略进行优化处理;以及

合理策略提示单元,用于如所述合理性预测值大于所述设定值,则提示所述授权策略为合理性策略。

8. 根据权利要求6所述的授权策略优化装置,其特征在于,所述授权策略优化装置还包括:

推荐预设授权策略获取模块,用于获取所述授权策略优化模型的至少一个推荐预设授权策略,其中所述推荐预设授权策略的合理性预测值大于所述授权策略优化模型中其他预设授权策略的合理性预测值;

所述优化处理模块包括:

判断单元,用于判断所述合理性预测值是否小于等于设定值;

优化处理单元,用于如所述合理性预测值小于等于所述设定值,则发送所述至少一个推荐预设授权策略,以使用户对所述授权策略进行优化处理;

合理策略提示单元,用于如所述合理性预测值大于所述设定值,则提示所述授权策略为合理性策略。

9. 根据权利要求6所述的授权策略优化装置,其特征在于,所述授权策略优化装置还包括:

预设授权策略获取模块,用于通过鉴权系统的鉴权日志以及业务服务器的业务关联日志,获取所述预设授权策略的授权日志信息。

10. 根据权利要求6所述的授权策略优化装置,其特征在于,所述日志信息特征包括用户特征、行为特征、授权策略特征以及鉴权目标值特征。

11. 一种计算机可读存储介质,其存储有计算机程序,其中,所述计算机程序使得计算机执行如权利要求1至5任一项所述的方法。

12. 一种计算机设备,包括处理器和存储器,所述存储器存储有用于授权策略优化的计算机程序,其中,所述处理器加载所述存储器的计算机程序执行如权利要求1至5任一项所述的方法。

授权策略优化方法及授权策略优化装置

技术领域

[0001] 本发明涉及互联网领域,特别是涉及一种授权策略优化方法及授权策略优化装置。

背景技术

[0002] 为了便于对资源进行访问控制,资源服务器往往会授予不同用户以不同的权限,从而安全的控制不同用户的资源访问权限,即哪些用户可以访问哪些资源以及确认这些用户访问资源的访问方式等。

[0003] 因此资源服务器往往要通过鉴权系统管理用户对特定资源的具体访问行为。目前的亚马逊鉴权系统以及阿里云鉴权系统,有两种优化授权策略的方案。首先鉴权系统会将所有的鉴权行为作为日志记录下来,同时提供日志查询接口,由用户自己来分析历史鉴权;另外,鉴权系统会给出各个服务接口最近的访问记录,并筛选出没有被访问的服务及接口。通过这种粗粒度的分析,帮助用户进行决策。

[0004] 现有的鉴权系统在生成了完备的鉴权日志的基础上进行查询和基础的统计分析工作,来指导用户进行授权策略优化,虽然具有一定的指导意义,但是由于粒度过粗,因而只能发现和解决部分比较明显的问题,无法进行精细化的授权策略优化。

发明内容

[0005] 本发明实施例提供一种可进行精细化的授权策略优化的授权策略优化方法及授权策略优化装置,以解决现有的授权策略优化方法及授权策略优化装置的无法进行精细化的授权策略优化的技术问题。

[0006] 本发明实施例提供一种授权策略优化方法,其包括:

[0007] 接收授权策略,并根据所述授权策略获取预设授权策略的授权日志信息;

[0008] 提取所述授权日志信息的日志信息特征,并使用所述授权日志信息的日志信息特征,生成授权策略优化模型;

[0009] 使用所述授权策略优化模型,对所述授权策略进行策略合理性预测,以得到所述授权策略对应的合理性预测值;以及

[0010] 根据所述授权策略对应的合理性预测值,对所述授权策略进行优化处理。

[0011] 本发明实施例还提供一种授权策略优化装置,其包括:

[0012] 策略接收模块,用于接收授权策略,并根据所述授权策略获取预设授权策略的授权日志信息;

[0013] 模型生成模块,用于提取所述授权日志信息的日志信息特征,并使用所述授权日志信息的日志信息特征,生成授权策略优化模型;

[0014] 策略合理性预测模块,用于使用所述授权策略优化模型,对所述授权策略进行策略合理性预测,以得到所述授权策略对应的合理性预测值;以及

[0015] 优化处理模块,用于根据所述授权策略对应的合理性预测值,对所述授权策略进

行优化处理。

[0016] 相较于现有技术,本发明的授权策略优化方法及授权策略优化装置实时生成授权策略优化模型对授权策略进行合理性预测,并使用推荐预设授权策略对授权策略进行优化处理,实现了授权策略优化的精细化处理;解决了现有的授权策略优化方法及授权策略优化装置的无法进行精细化的授权策略优化的技术问题。

附图说明

[0017] 图1为本发明的授权策略优化方法的第一优选实施例的流程图;

[0018] 图2为本发明的授权策略优化方法的第二优选实施例的流程图;

[0019] 图3为本发明的授权策略优化方法的第二优选实施例的步骤S202的流程图;

[0020] 图4为本发明的授权策略优化方法的第二优选实施例的步骤S205的流程图;

[0021] 图5为本发明的授权策略优化装置的第一优选实施例的结构示意图;

[0022] 图6为本发明的授权策略优化装置的第二优选实施例的结构示意图;

[0023] 图7为本发明的授权策略优化装置的第二优选实施例的模型生成模块的结构示意图;

[0024] 图8为本发明的授权策略优化装置的第二优选实施例的优化处理模块的结构示意图;

[0025] 图9为本发明的授权策略优化方法及授权策略优化装置的具体实施例的使用流程图;

[0026] 图10为本发明的授权策略优化装置所在的电子设备的工作环境结构示意图。

具体实施方式

[0027] 请参照图式,其中相同的组件符号代表相同的组件,本发明的原理是以实施在一适当的运算环境中来举例说明。以下的说明是基于所例示的本发明具体实施例,其不应被视为限制本发明未在此详述的其它具体实施例。

[0028] 在以下的说明中,本发明的具体实施例将参考由一部或多部计算机所执行之作业的步骤及符号来说明,除非另有说明。因此,其将可了解到这些步骤及操作,其中有数次提到为由计算机执行,包括了由代表了以一结构化型式中的数据之电子信号的计算机处理单元所操纵。此操纵转换该数据或将其维持在该计算机之内存系统中的位置处,其可重新配置或另外以本领域技术人员所熟知的方式来改变该计算机之运作。该数据所维持的数据结构为该内存之实体位置,其具有由该数据格式所定义的特定特性。但是,本发明原理以上述文字来说明,其并不代表为一种限制,本领域技术人员将可了解到以下所述的多种步骤及操作亦可实施在硬件当中。

[0029] 本发明的授权策略优化装置可用于各种数据云平台的鉴权电子装置中,该鉴权电子装置包括但不限于可穿戴设备、个人计算机、服务器计算机、手持式或膝上型设备、移动设备、多处理器系统、小型计算机、大型计算机、包括上述任意系统或设备的分布式计算环境。本发明的鉴权电子装置可实现对用户访问数据资源的授权策略的合理性预测以及授权策略优化的精细化处理,从而提高了鉴权电子装置的授权操作成功率。

[0030] 请参照图1,图1为本发明的授权策略优化方法的第一优选实施例的流程图;本优

选实施例的授权策略优化方法可使用上述的鉴权电子装置进行实施,本优选实施例的授权策略优化方法包括:

[0031] 步骤S101,接收授权策略,并根据授权策略获取预设授权策略的授权日志信息;

[0032] 步骤S102,提取授权日志信息的日志信息特征,并使用授权日志信息的日志信息特征,生成授权策略优化模型;

[0033] 步骤S103,使用授权策略优化模型,对授权策略进行策略合理性预测,以得到授权策略对应的合理性预测值;

[0034] 步骤S104,根据授权策略对应的合理性预测值,对授权策略进行优化处理;

[0035] 下面详细说明本优选实施例的授权策略优化方法的各步骤的具体流程。

[0036] 在步骤S101中,授权策略优化装置接收用户输入的授权策略,该授权策略为用户想要使用对用户数据访问权限进行鉴权操作的策略,但是用户并不知道该授权策略是否合理,是否会产生过多的误判或漏判。

[0037] 随后授权策略优化装置根据接收的授权策略获取预设授权策略的授权日志信息;这里的预设授权策略是指用来建立授权策略优化模型的授权策略,这些预设授权策略的授权日志信息的来源可以是鉴权系统的鉴权日志,即以当前的鉴权电子装置历史以及当前的鉴权日志作为参考;也可以是业务服务器的业务关联日志,即业务服务器对最终授权情况的反馈,如业务服务器的业务关联日志中的某项业务数据访问异常,可能是由于授权策略设置不合理导致的。随后转到步骤S102。

[0038] 在步骤S102中,授权策略优化装置提取步骤S101中获取的预设授权策略的日志信息特征,该日志信息特征是指是指可用于表示预设授权策略的信息特征,该日志信息特征包括用户特征、行为特征、授权策略特征以及鉴权目标值特征等。

[0039] 其中用户特征可包括用户类别以及用户活跃度等;该用户类别可为如普通用户、外部用户、跨账户以及子账户等,用户活跃度可为用户的数据访问频率。行为特征可包括操作行为接口、操作行为地理位置、操作行为类别以及鉴权类别等。操作行为类别可为操作资源所属项目或操作资源所属云服务等。鉴权类别包括鉴权是否通过。授权策略特征包括授权策略变更频率、授权策略数量、策略用户匹配关系以及策略资源匹配关系等。策略用户匹配关系可为用户与策略的对应关系,策略资源匹配关系可为资源和策略的对应关系。鉴权目标值特征包括鉴权结果是否正确以及鉴权结果是否发生变更等。

[0040] 随后授权策略优化装置使用提取的授权日志信息的日志信息特征,训练生成授权策略优化模型;该授权策略优化模型可对其他的授权策略进行策略合理性预测。随后转到步骤S103。

[0041] 在步骤S103中,授权策略优化装置使用步骤S102生成的授权策略优化模型,对授权策略进行策略合理性预测,从而得到量化的策略有效性概率,即具有指导作用的授权策略对应的合理性预测值。本优选实施例中的授权策略优化模型可实时生成,因此该授权策略优化模型可结合时间衰减随着预设授权策略的积累不断优化。随后转到步骤S104。

[0042] 在步骤S104中,授权策略优化装置根据步骤S103获取的授权策略对应的合理性预测值,对授权策略进行优化处理。具体为:如合理性预测值小于等于设定值,则提示用户对该授权策略进行优化处理,如修改授权策略中的某个特征,以提高该授权策略的合理性预测值。如合理性预测值大于设定值,则提示该授权策略为合理性策略,鉴权电子装置可直接

采用该授权策略对用户进行鉴权操作。

[0043] 这样即完成了本优选实施例的授权策略优化方法的授权策略优化过程。

[0044] 本优选实施例的授权策略优化方法实时生成授权策略模型对授权策略进行合理性预测,并根据授权策略的合理性预测值对授权策略进行优化处理,实现了授权策略优化的精细化处理。

[0045] 请参照图2,图2为本发明的授权策略优化方法的第二优选实施例的流程图;本优选实施例的授权策略优化方法可使用上述的鉴权电子装置进行实施,本优选实施例的授权策略优化方法包括:

[0046] 步骤S201,接收授权策略,并根据授权策略获取预设授权策略的授权日志信息;

[0047] 步骤S202,提取授权日志信息的日志信息特征,并使用授权日志信息的日志信息特征,生成授权策略优化模型;

[0048] 步骤S203,获取授权策略优化模型的至少一个推荐预设授权策略,其中推荐预设授权策略的合理性预测值大于授权策略优化模型中其他预设授权策略的合理性预测值;

[0049] 步骤S204,使用授权策略优化模型,对授权策略进行策略合理性预测,以得到授权策略对应的合理性预测值;

[0050] 步骤S205,根据授权策略对应的合理性预测值,对授权策略进行优化处理。

[0051] 下面详细说明本优选实施例的授权策略优化方法的各步骤的具体流程。

[0052] 在步骤S201中,授权策略优化装置接收用户输入的授权策略,该授权策略为用户想要使用对用户数据访问权限进行鉴权操作的策略,但是用户并不知道该授权策略是否合理,是否会产生过多的误判或漏判。

[0053] 随后授权策略优化装置根据接收的授权策略获取预设授权策略的授权日志信息;这里的预设授权策略是指用来建立授权策略优化模型的授权策略,这些预设授权策略的授权日志信息的来源可以是鉴权系统的鉴权日志,即以当前的鉴权电子装置历史以及当前的鉴权日志作为参考;也可以是业务服务器的业务关联日志,即业务服务器对最终授权情况的反馈,如业务服务器的业务关联日志中的某项业务数据访问异常,可能是由于授权策略设置不合理导致的。随后转到步骤S202。

[0054] 在步骤S202中,授权策略优化装置提取步骤S201中获取的预设授权策略的日志信息特征,该日志信息特征是指是指可用于表示预设授权策略的信息特征,该日志信息特征包括用户特征、行为特征、授权策略特征以及鉴权目标值特征等。

[0055] 随后授权策略优化装置使用提取的授权日志信息的日志信息特征,训练生成授权策略优化模型;该授权策略优化模型可对其他的授权策略进行策略合理性预测。具体的生成授权策略优化模型的步骤请参照如图3,图3为本发明的授权策略优化方法的第二优选实施例的步骤S202的流程图。该步骤S202包括:

[0056] 步骤S301,授权策略优化装置对日志信息特征进行特征优化处理,如特征离散化处理或生成对应的组合特征等。组合特征主要是指用户、资源以及策略的关系特征,组合特征可以丰富和约束上述日志信息特征。

[0057] 步骤S302,授权策略优化装置基于预设规则对优化处理后的日志信息特征进行训练样本选取;如正训练样本以及负训练样本等。这里的预设规则可为日志信息特征的选取规则或加权规则等,如某个授权策略的使用时间较长,则对该授权策略设置较高的加权值;

如某个授权策略的使用时间较短或经常被更新,则可不选取该授权策略,或设置较低的加权值。

[0058] 步骤S303,授权策略优化装置根据步骤S302获取的训练样本的离散化或连续化特征属性,使用预设模型算法(如Logistic Regression,逻辑回归线性模型算法或Gradient Boosting Decision Tree,梯度提升决策树非线性模型算法)进行模型训练,以生成授权策略优化模型。随后转到步骤S203。

[0059] 在步骤S203中,授权策略优化装置获取步骤S202中的授权策略优化模型的至少一个推荐预设授权策略,其中推荐预设授权策略的合理性预测值大于授权策略优化模型中其他预设授权策略的合理性预测值。即授权策略优化装置获取授权策略优化模型中具有较高合理性预测值的正样本,以对合理性预测值较低的授权策略进行优化操作。随后转到步骤S204。

[0060] 在步骤S204中,授权策略优化装置使用步骤S202生成的授权策略优化模型,对授权策略进行策略合理性预测,从而得到量化的策略有效性概率,即具有指导作用的授权策略对应的合理性预测值。本优选实施例中的授权策略优化模型可实时生成,因此该授权策略优化模型可结合时间衰减随着预设授权策略的积累不断优化。随后转到步骤S205。

[0061] 在步骤S205中,授权策略优化装置根据步骤S204获取的授权策略对应的合理性预测值,对授权策略进行优化处理。具体为请参照图4,图4为本发明的授权策略优化方法的第二优选实施例的步骤S205的流程图。该步骤S205包括:

[0062] 步骤S401,授权策略优化装置判断授权策略的合理性预测值是否小于等于设定值;如小于等于设定值,则转到步骤S402;如大于设定值,则转到步骤S403。

[0063] 步骤S402,如合理性预测值小于等于设定值,则授权策略优化装置发送至少一个步骤S203中获取的推荐预设授权策略至用户,以使用户对授权策略进行优化处理。

[0064] 步骤S403,如合理性预测值大于设定值,则提示该授权策略为合理性策略,鉴权电子装置可直接采用该授权策略对用户进行鉴权操作。

[0065] 这样即完成了本优选实施例的授权策略优化方法的授权策略优化过程。

[0066] 在第一优选实施例的基础上,本优选实施例的授权策略优化方法实时生成授权策略优化模型对授权策略进行合理性预测,并使用推荐预设授权策略对授权策略进行优化处理,实现了授权策略优化的精细化处理。同时对日志信息特征进行特征优化处理,以及使用预设规则对训练样本进行选取,进一步提高了授权策略优化的有效性。

[0067] 本发明还提供一种授权策略优化装置,请参照图5,图5为本发明的授权策略优化装置的第一优选实施例的结构示意图。本优选实施例的授权策略优化装置可使用上述的授权策略优化方法的第一优选实施例进行实施,本优选实施例的授权策略优化装置50包括策略接收模块51、模型生成模块52、策略合理性预测模块53以及优化处理模块54。

[0068] 策略接收模块51用于接收授权策略,并根据授权策略获取预设授权策略的授权日志信息;模型生成模块52用于提取授权日志信息的日志信息特征,并使用授权日志信息的日志信息特征,生成授权策略优化模型;策略合理性预测模块53用于使用授权策略优化模型,对授权策略进行策略合理性预测,以得到授权策略对应的合理性预测值;优化处理模块54用于根据授权策略对应的合理性预测值,对授权策略进行优化处理。

[0069] 本优选实施例的授权策略优化装置50使用时,首先策略接收模块51接收用户输入

的授权策略,该授权策略为用户想要使用对用户数据访问权限进行鉴权操作的策略,但是用户并不知道该授权策略是否合理,是否会产生过多的误判或漏判。

[0070] 随后策略接收模块51根据接收的授权策略获取预设授权策略的授权日志信息;这里的预设授权策略是指用来建立授权策略优化模型的授权策略,这些预设授权策略的授权日志信息的来源可以是鉴权系统的鉴权日志,即以当前的鉴权电子装置历史以及当前的鉴权日志作为参考;也可以是业务服务器的业务关联日志,即业务服务器对最终授权情况的反馈,如业务服务器的业务关联日志中的某项业务数据访问异常,可能是由于授权策略设置不合理导致的。

[0071] 然后模型生成模块52提取策略接收模块51获取的预设授权策略的日志信息特征,该日志信息特征是指是指可用于表示预设授权策略的信息特征,该日志信息特征包括用户特征、行为特征、授权策略特征以及鉴权目标值特征等。

[0072] 其中用户特征可包括用户类别以及用户活跃度等;该用户类别可为如普通用户、外部用户、跨账户以及子账户等,用户活跃度可为用户的数据访问频率。行为特征可包括操作行为接口、操作行为地理位置、操作行为类别以及鉴权类别等。操作行为类别可为操作资源所属项目或操作资源所属云服务等。鉴权类别包括鉴权是否通过。授权策略特征包括授权策略变更频率、授权策略数量、策略用户匹配关系以及策略资源匹配关系等。策略用户匹配关系可为用户与策略的对应关系,策略资源匹配关系可为资源和策略的对应关系。鉴权目标值特征包括鉴权结果是否正确以及鉴权结果是否发生变更等。

[0073] 随后模型生成模块52使用提取的授权日志信息的日志信息特征,训练生成授权策略优化模型;该授权策略优化模型可对其他的授权策略进行策略合理性预测。

[0074] 然后策略合理性预测模块53使用模型生成模块52生成的授权策略优化模型,对授权策略进行策略合理性预测,从而得到量化的策略有效性概率,即具有指导作用的授权策略对应的合理性预测值。本优选实施例中的授权策略优化模型可实时生成,因此该授权策略优化模型可结合时间衰减随着预设授权策略的积累不断优化。

[0075] 最后优化处理模块54根据策略合理性预测模块53获取的授权策略对应的合理性预测值,对授权策略进行优化处理。具体为:如合理性预测值小于等于设定值,则提示用户对该授权策略进行优化处理,如修改授权策略中的某个特征,以提高该授权策略的合理性预测值。如合理性预测值大于设定值,则提示该授权策略为合理性策略,鉴权电子装置可直接采用该授权策略对用户进行鉴权操作。

[0076] 这样即完成了本优选实施例的授权策略优化装置50的授权策略优化过程。

[0077] 本优选实施例的授权策略优化装置实时生成授权策略模型对授权策略进行合理性预测,并根据授权策略的合理性预测值对授权策略进行优化处理,实现了授权策略优化的精细化处理。

[0078] 请参照图6,图6为本发明的授权策略优化装置的第二优选实施例的结构示意图。本优选实施例的授权策略优化装置可使用上述的授权策略优化方法的第二优选实施例进行实施,本优选实施例的授权策略优化装置60包括推荐预设授权策略获取模块62、策略接收模块61、模型生成模块63、推荐预设授权策略获取模块64、策略合理性预测模块65以及优化处理模块66。

[0079] 预设授权策略获取模块62用于通过鉴权系统的鉴权日志以及业务服务器的业务

关联日志,获取预设授权策略的授权日志信息。策略接收模块61用于接收授权策略,并根据授权策略获取预设授权策略的授权日志信息。模型生成模块63用于提取授权日志信息的日志信息特征,并使用授权日志信息的日志信息特征,生成授权策略优化模型。推荐预设授权策略获取模块64用于获取授权策略优化模型的至少一个推荐预设授权策略,其中推荐预设授权策略的合理性预测值大于授权策略优化模型中其他预设授权策略的合理性预测值。策略合理性预测模块65用于使用授权策略优化模型,对授权策略进行策略合理性预测,以得到授权策略对应的合理性预测值。优化处理模块66用于根据授权策略对应的合理性预测值,对授权策略进行优化处理。

[0080] 请参照图7,图7为本发明的授权策略优化装置的第二优选实施例的模型生成模块的结构示意图。该模型生成模块63包括特征优化处理单元71、训练样本选取单元72以及模型生成单元73。

[0081] 特征优化处理单元71用于对日志信息特征进行特征优化处理;训练样本选取单元72用于基于预设规则对优化处理后的日志信息特征进行训练样本选取;模型生成单元73用于根据训练样本的离散化或连续化特征属性,使用预设模型算法进行模型训练,以生成授权策略优化模型。

[0082] 请参照图8,图8为本发明的授权策略优化装置的第二优选实施例的优化处理模块的结构示意图。该优化处理模块66包括判断单元81、优化处理单元82以及合理策略提示单元83。

[0083] 判断单元81用于判断合理性预测值是否小于等于设定值;优化处理单元82用于如合理性预测值小于等于设定值,则提示用户对授权策略进行优化处理;具体的,可发送至少一个推荐预设授权策略,以使用户对授权策略进行优化处理。合理策略提示单元83用于如合理性预测值大于设定值,则提示授权策略为合理性策略。

[0084] 本优选实施例的授权策略优化装置60使用时,首先策略接收模块61接收用户输入的授权策略,该授权策略为用户想要使用对用户数据访问权限进行鉴权操作的策略,但是用户并不知道该授权策略是否合理,是否会产生过多的误判或漏判。

[0085] 随后推荐预设授权策略获取模块62通过鉴权系统的鉴权日志以及业务服务器的业务关联日志,获取预设授权策略的授权日志信息。策略接收模块61根据接收的授权策略获取预设授权策略的授权日志信息。

[0086] 然后模型生成模块63提取策略接收模块61获取的预设授权策略的日志信息特征,该日志信息特征是指是指可用于表示预设授权策略的信息特征,该日志信息特征包括用户特征、行为特征、授权策略特征以及鉴权目标值特征等。

[0087] 随后模型生成模块63使用提取的授权日志信息的日志信息特征,训练生成授权策略优化模型;该授权策略优化模型可对其他的授权策略进行策略合理性预测。具体的生成授权策略优化模型的步骤包括:

[0088] 模型生成模块63的特征优化处理单元71对日志信息特征进行特征优化处理,如特征离散化处理或生成对应的组合特征等。组合特征主要是指用户、资源以及策略的关系特征,组合特征可以丰富和约束上述日志信息特征。

[0089] 模型生成模块63的训练样本选取单元72基于预设规则对优化处理后的日志信息特征进行训练样本选取;如正训练样本以及负训练样本等。这里的预设规则可为日志信息

特征的选取规则或加权规则等,如某个授权策略的使用时间较长,则对该授权策略设置较高的加权值;如某个授权策略的使用时间较短或经常被更新,则可不选取该授权策略,或设置较低的加权值。

[0090] 模型生成模块63的模型生成单元73根据训练样本选取单元72获取的训练样本的离散化或连续化特征属性,使用预设模型算法(如Logistic Regression,逻辑回归线性模型算法或Gradient Boosting Decision Tree,梯度提升决策树非线性模型算法)进行模型训练,以生成授权策略优化模型。

[0091] 然后推荐预设授权策略获取模块64获取模型生成模块63生成的授权策略优化模型的至少一个推荐预设授权策略,其中推荐预设授权策略的合理性预测值大于授权策略优化模型中其他预设授权策略的合理性预测值。即推荐预设授权策略获取模块64获取授权策略优化模型中具有较高合理性预测值的正样本,以对合理性预测值较低的授权策略进行优化操作。

[0092] 随后策略合理性预测模块65使用模型生成模块63生成的授权策略优化模型,对授权策略进行策略合理性预测,从而得到量化的策略有效性概率,即具有指导作用的授权策略对应的合理性预测值。本优选实施例中的授权策略优化模型可实时生成,因此该授权策略优化模型可结合时间衰减随着预设授权策略的积累不断优化。

[0093] 最后优化处理模块66根据策略合理性预测模块65获取的授权策略对应的合理性预测值,对授权策略进行优化处理。具体为:

[0094] 优化处理模块66的判断单元81判断授权策略的合理性预测值是否小于等于设定值;如合理性预测值小于等于设定值,则优化处理单元82发送至少一个推荐预设授权策略至用户,以使用户对授权策略进行优化处理。如合理性预测值大于设定值,则合理策略提示单元83提示该授权策略为合理性策略,鉴权电子装置可直接采用该授权策略对用户进行鉴权操作。

[0095] 这样即完成了本优选实施例的授权策略优化装置60的授权策略优化过程。

[0096] 在第一优选实施例的基础上,本优选实施例的授权策略优化装置实时生成授权策略优化模型对授权策略进行合理性预测,并使用推荐预设授权策略对授权策略进行优化处理,实现了授权策略优化的精细化处理。同时对日志信息特征进行特征优化处理,以及使用预设规则对训练样本进行选取,进一步提高了授权策略优化的有效性。

[0097] 下面通过一具体实施例说明本发明的授权策略优化方法及授权策略优化装置的具体工作原理。请参照图9,图9为本发明的授权策略优化方法及授权策略优化装置的具体实施例的使用流程图。本具体实施例的授权策略优化装置设置在鉴权服务器中,以对访问云服务器的用户进行授权验证。本具体实施例的授权策略优化流程包括:

[0098] 步骤S901,鉴权服务器接收待验证的授权策略;

[0099] 步骤S902,鉴权服务器从鉴权系统读取鉴权日志,并从业务服务器读取业务关联日志,并根据鉴权日志以及业务关联日志获取预设授权策略的授权日志信息;

[0100] 步骤S903,鉴权服务器提取授权日志信息的日志信息特征(策略特征),并对上述日志信息特征进行训练,生成授权策略优化模型;

[0101] 步骤S904,鉴权服务器提取待验证的授权策略的策略特征,并在授权策略优化模型中使用上述待验证的授权策略的策略特征,对授权策略进行策略合理性预测,以得到授

权策略对应的合理性预测值；

[0102] 步骤S905,判断合理性预测值是否小于等于设定值;如小于等于设定值,则转到步骤S906;如大于设定值,则转到步骤S907;

[0103] 步骤S906,从授权策略优化模型中获取至少一个具有较高合理性预测值的推荐预设授权策略,并将该推荐预设授权策略发送至用户以进行授权策略优化。

[0104] 步骤S907,提示该授权策略为合理性策略。

[0105] 这样即完成了本具体实施例的,授权策略优化方法及授权策略优化装置的授权策略优化过程。

[0106] 本发明的授权策略优化方法及授权策略优化装置实时生成授权策略优化模型对授权策略进行合理性预测,并使用推荐预设授权策略对授权策略进行优化处理,实现了授权策略优化的精细化处理;解决了现有的授权策略优化方法及授权策略优化装置无法进行精细化的授权策略优化的技术问题。

[0107] 如本申请所使用的术语“组件”、“模块”、“系统”、“接口”、“进程”等等一般地旨在指计算机相关实体:硬件、硬件和软件的组合、软件或执行中的软件。例如,组件可以是但不限于是运行在处理器上的进程、处理器、对象、可执行应用、执行的线程、程序和/或计算机。通过图示,运行在控制器上的应用和该控制器二者都可以是组件。一个或多个组件可以有在于执行的进程和/或线程内,并且组件可以位于一个计算机上和/或分布在两个或更多计算机之间。

[0108] 图10和随后的讨论提供了对实现本发明所述的授权策略优化装置所在的电子设备的工作环境的简短、概括的描述。图10的工作环境仅仅是适当的工作环境的一个实例并且不旨在建议关于工作环境的用途或功能的范围的任何限制。实例电子设备1012包括但不限于可穿戴设备、头戴设备、医疗健康平台、个人计算机、服务器计算机、手持式或膝上型设备、移动设备(比如移动电话、个人数字助理(PDA)、媒体播放器等等)、多处理器系统、消费型电子设备、小型计算机、大型计算机、包括上述任意系统或设备的分布式计算环境,等等。

[0109] 尽管没有要求,但是在“计算机可读指令”被一个或多个电子设备执行的通用背景下描述实施例。计算机可读指令可以经由计算机可读介质来分布(下文讨论)。计算机可读指令可以实现为程序模块,比如执行特定任务或实现特定抽象数据类型的功能、对象、应用编程接口(API)、数据结构等等。典型地,该计算机可读指令的功能可以在各种环境中随意组合或分布。

[0110] 图10图示了包括本发明的授权策略优化装置中的一个或多个实施例的电子设备1012的实例。在一种配置中,电子设备1012包括至少一个处理单元1016和存储器1018。根据电子设备的确切配置和类型,存储器1018可以是易失性的(比如RAM)、非易失性的(比如ROM、闪存等)或二者的某种组合。该配置在图10中由虚线1014图示。

[0111] 在其他实施例中,电子设备1012可以包括附加特征和/或功能。例如,设备1012还可以包括附加的存储装置(例如可移除和/或不可移除的),其包括但不限于磁存储装置、光存储装置等等。这种附加存储装置在图10中由存储装置1020图示。在一个实施例中,用于实现本文所提供的一个或多个实施例的计算机可读指令可以在存储装置1020中。存储装置1020还可以存储用于实现操作系统、应用程序等的其他计算机可读指令。计算机可读指令可以载入存储器1018中由例如处理单元1016执行。

[0112] 本文所使用的术语“计算机可读介质”包括计算机存储介质。计算机存储介质包括以用于存储诸如计算机可读指令或其他数据之类的信息的任何方法或技术实现的易失性和非易失性、可移除和不可移除介质。存储器1018和存储装置1020是计算机存储介质的实例。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字通用盘(DVD)或其他光存储装置、盒式磁带、磁带、磁盘存储装置或其他磁存储设备、或可以用于存储期望信息并可以被电子设备1012访问的任何其他介质。任意这样的计算机存储介质可以是电子设备1012的一部分。

[0113] 电子设备1012还可以包括允许电子设备1012与其他设备通信的通信连接1026。通信连接1026可以包括但不限于调制解调器、网络接口卡(NIC)、集成网络接口、射频发射器/接收器、红外端口、USB连接或用于将电子设备1012连接到其他电子设备的其他接口。通信连接1026可以包括有线连接或无线连接。通信连接1026可以发射和/或接收通信媒体。

[0114] 术语“计算机可读介质”可以包括通信介质。通信介质典型地包含计算机可读指令或诸如载波或其他传输机构之类的“已调制数据信号”中的其他数据,并且包括任何信息递送介质。术语“已调制数据信号”可以包括这样的信号:该信号特性中的一个或多个按照将信息编码到信号中的方式来设置或改变。

[0115] 电子设备1012可以包括输入设备1024,比如键盘、鼠标、笔、语音输入设备、触摸输入设备、红外相机、视频输入设备和/或任何其他输入设备。设备1012中也可以包括输出设备1022,比如一个或多个显示器、扬声器、打印机和/或任意其他输出设备。输入设备1024和输出设备1022可以经由有线连接、无线连接或其任意组合连接到电子设备1012。在一个实施例中,来自另一个电子设备的输入设备或输出设备可以被用作电子设备1012的输入设备1024或输出设备1022。

[0116] 电子设备1012的组件可以通过各种互连(比如总线)连接。这样的互连可以包括外围组件互连(PCI)(比如快速PCI)、通用串行总线(USB)、火线(IEEE1394)、光学总线结构等等。在另一个实施例中,电子设备1012的组件可以通过网络互连。例如,存储器1018可以由位于不同物理位置中的、通过网络互连的多个物理存储器单元构成。

[0117] 本领域技术人员将认识到,用于存储计算机可读指令的存储设备可以跨越网络分布。例如,可经由网络1028访问的电子设备1030可以存储用于实现本发明所提供的的一个或多个实施例的计算机可读指令。电子设备1012可以访问电子设备1030并且下载计算机可读指令的一部分或所有以供执行。可替代地,电子设备1012可以按需要下载多条计算机可读指令,或者一些指令可以在电子设备1012处执行并且一些指令可以在电子设备1030处执行。

[0118] 本文提供了实施例的各种操作。在一个实施例中,所述的一个或多个操作可以构成一个或多个计算机可读介质上存储的计算机可读指令,其在被电子设备执行时将使得计算设备执行所述操作。描述一些或所有操作的顺序不应当被解释为暗示这些操作必需是顺序相关的。本领域技术人员将理解具有本说明书的益处的可替代的排序。而且,应当理解,不是所有操作必需在本文所提供的每个实施例中存在。

[0119] 而且,尽管已经相对于一个或多个实现方式示出并描述了本公开,但是本领域技术人员基于对本说明书和附图的阅读和理解将会想到等价变型和修改。本公开包括所有这样的修改和变型,并且仅由所附权利要求的范围限制。特别地关于由上述组件(例如元件、

资源等)执行的各种功能,用于描述这样的组件的术语旨在对应于执行所述组件的指定功能(例如其在功能上是等价的)的任意组件(除非另外指示),即使在结构上与执行本文所示的本公开的示范性实现方式中的功能的公开结构不等同。此外,尽管本公开的特定特征已经相对于若干实现方式中的仅一个被公开,但是这种特征可以与如可以对给定或特定应用而言是期望和有利的其他实现方式的一个或多个其他特征组合。而且,就术语“包括”、“具有”、“含有”或其变形被用在具体实施方式或权利要求中而言,这样的术语旨在以与术语“包含”相似的方式包括。

[0120] 本发明实施例中的各功能单元可以集成在一个处理模块中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现,也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用,也可以存储在一个计算机可读存储介质中。上述提到的存储介质可以是只读存储器,磁盘或光盘等。上述的各装置或系统,可以执行相应方法实施例中的方法。

[0121] 综上所述,虽然本发明已以实施例揭露如上,实施例前的序号,如“第一”、“第二”等仅为描述方便而使用,对本发明各实施例的顺序不造成限制。并且,上述实施例并非用以限制本发明,本领域的普通技术人员,在不脱离本发明的精神和范围内,均可作各种更动与润饰,因此本发明的保护范围以权利要求界定的范围为准。

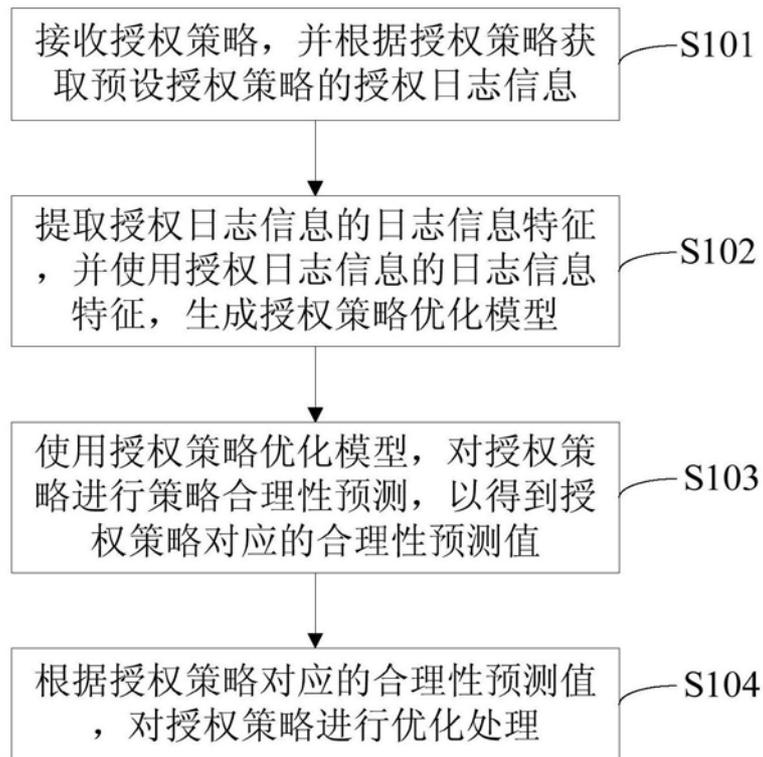


图1

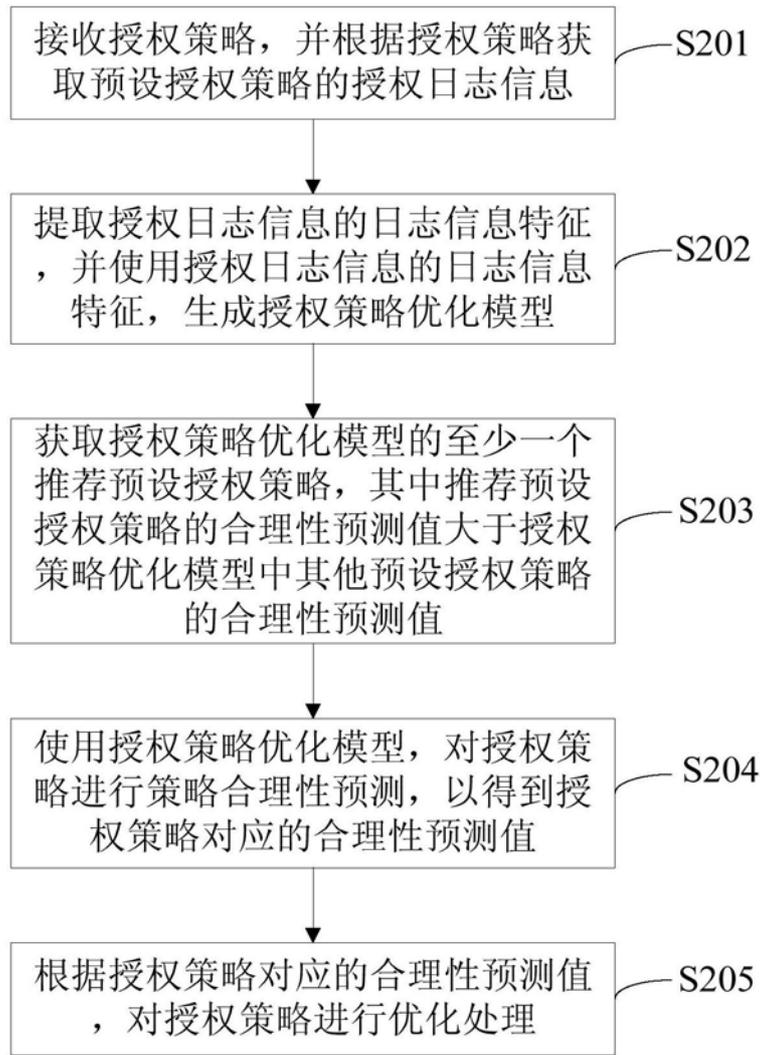


图2

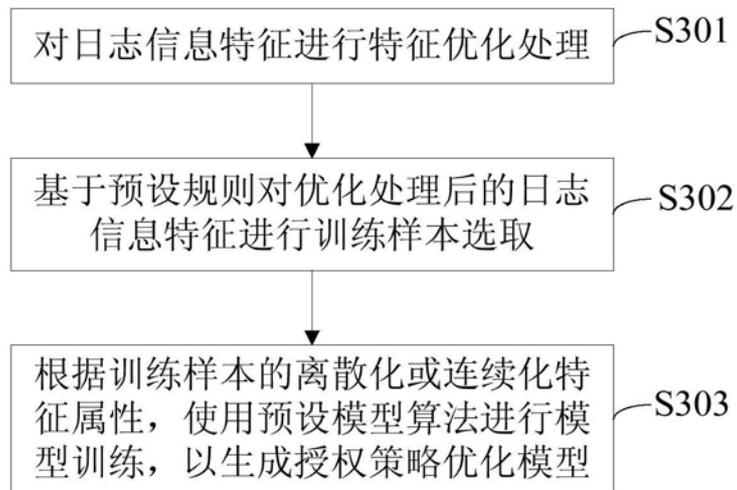


图3

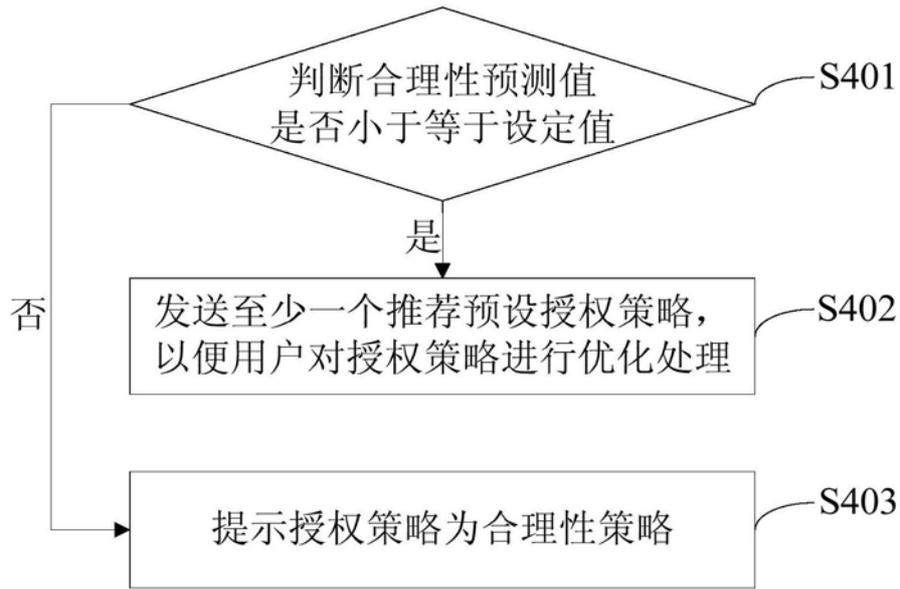


图4



图5

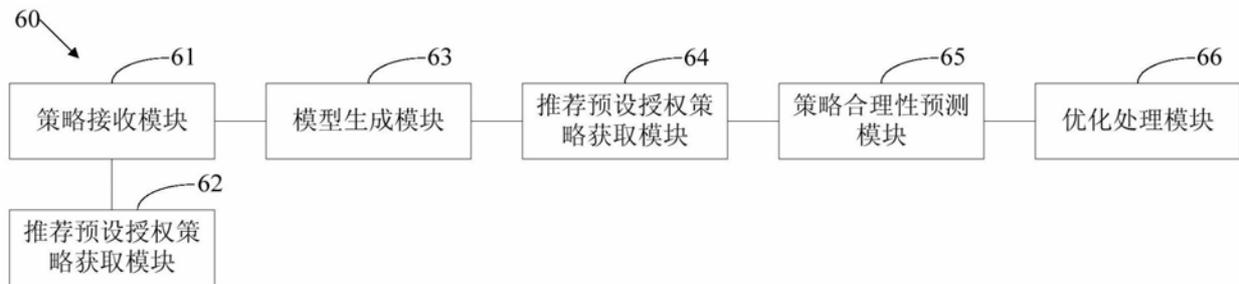


图6

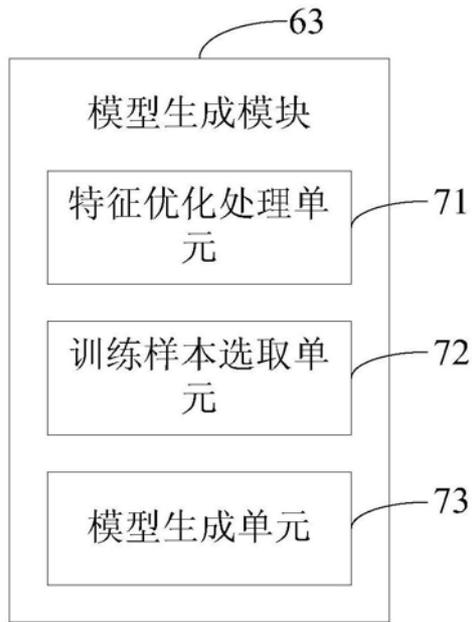


图7

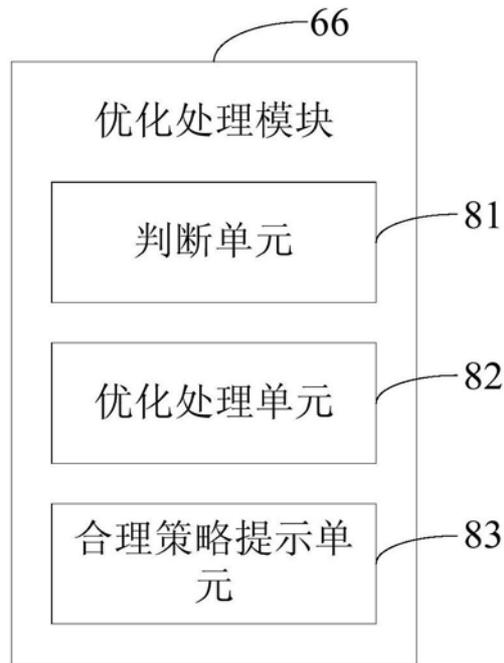


图8

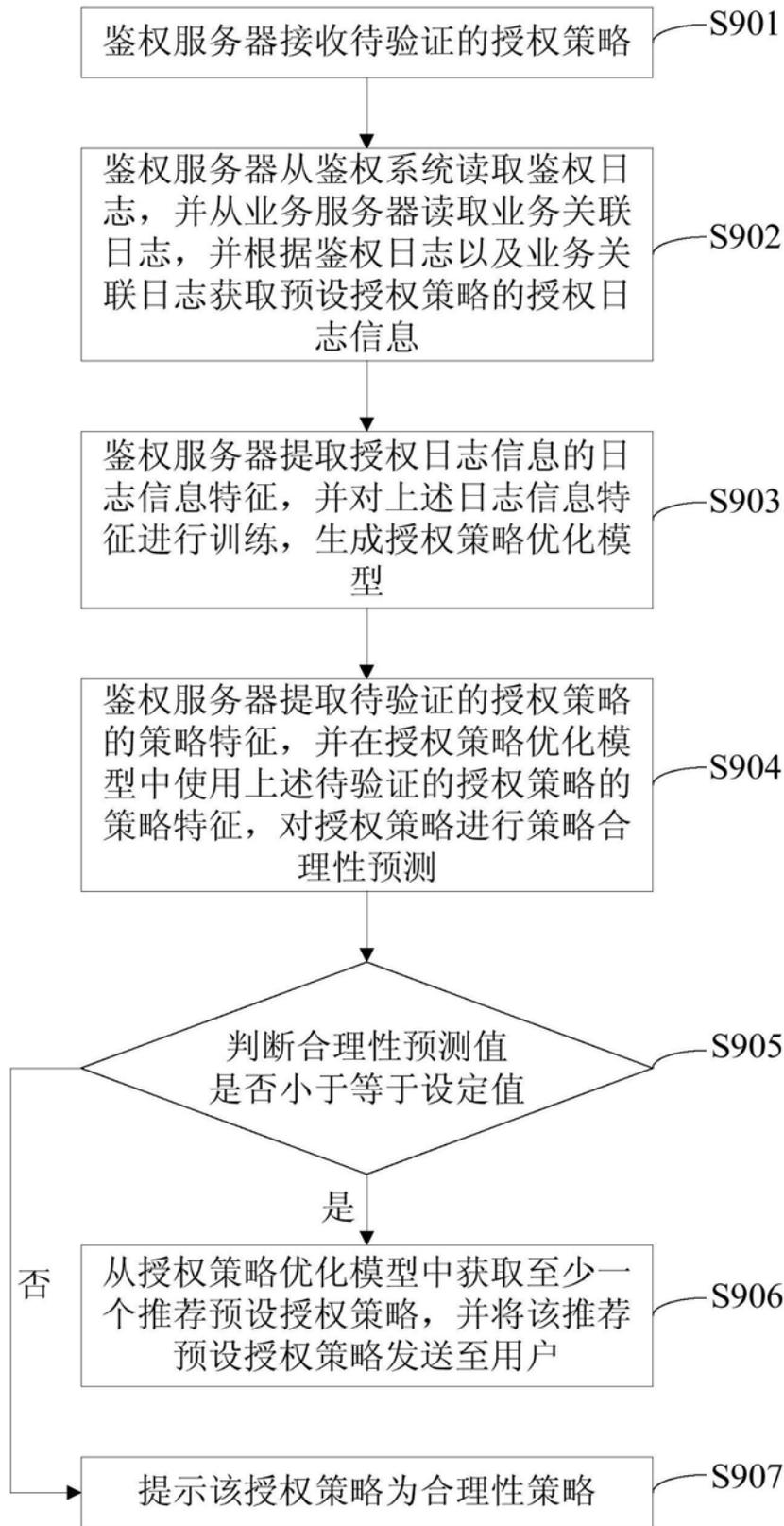


图9

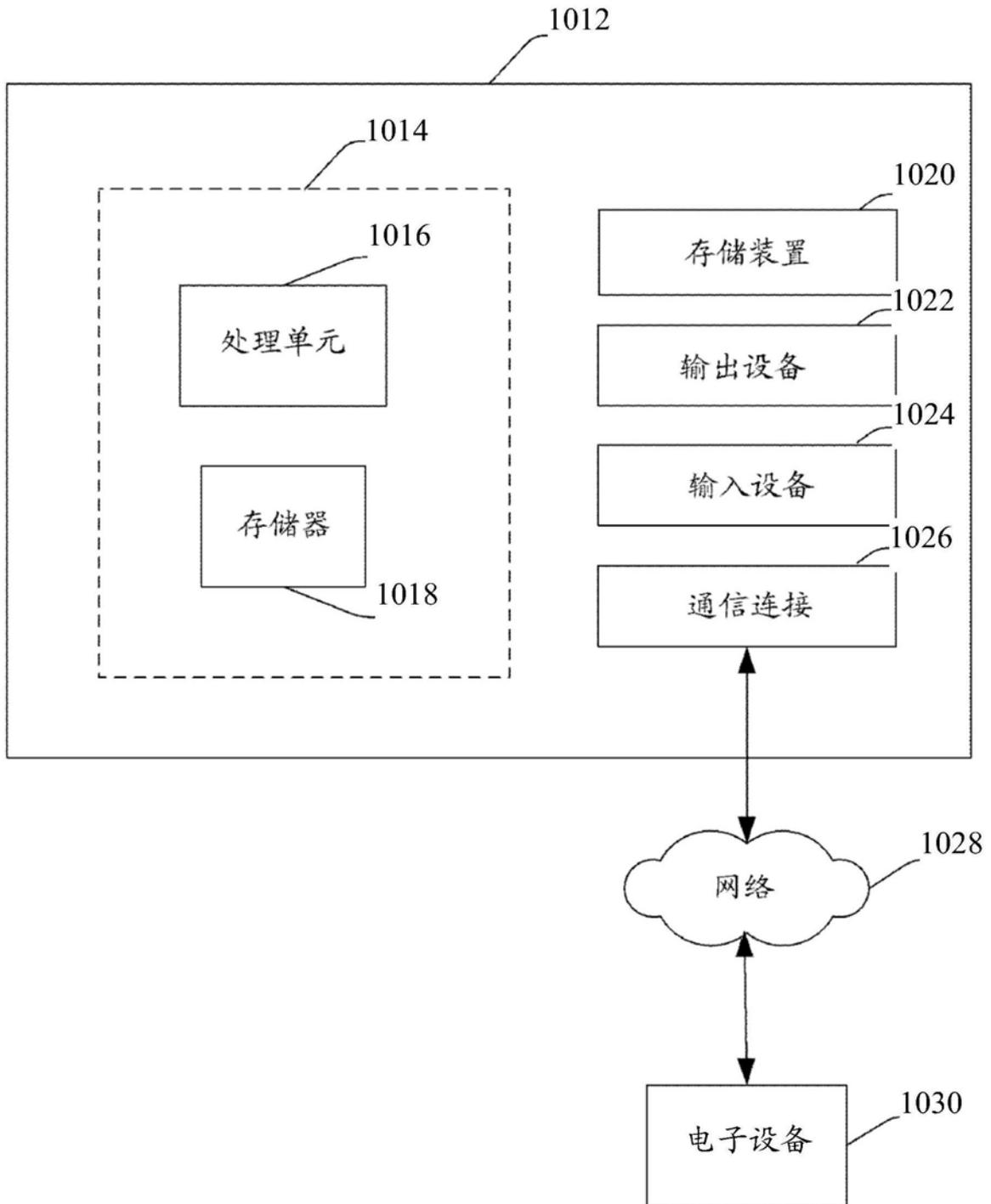


图10