(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116595573 A
(43)申请公布日 2023.08.15

(21)申请号 202310404735.X

(22)申请日 2023.04.14

(71)申请人 敦源信息科技(广州)有限公司
地址 510000 广东省广州市高新技术产业开发区揽月路8号自编1栋238房间

(72)发明人 黄晓生 韦天贵

(74)专利代理机构 广州专理知识产权代理事务所(普通合伙) 44493
专利代理师 曲超

(51)Int.Cl.
G06F 21/62(2013.01)

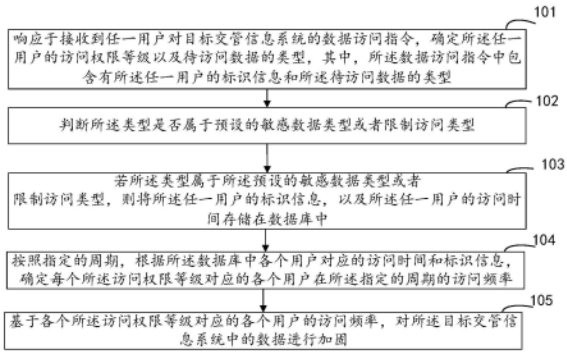
权利要求书2页 说明书10页 附图2页

(54)发明名称

交管信息系统的数据安全加固方法及装置

(57)摘要

本公开提出了一种交管信息系统的数据安全加固方法及装置,包括:响应于接收到任一用户对目标交管信息系统的数据访问指令,确定任一用户的访问权限等级以及待访问数据的类型;判断类型是否属于预设的敏感数据类型或者限制访问类型;若属于,则将任一用户的标识信息,以及任一用户的访问时间存储在数据库中;按照指定的周期,根据数据库中各个用户对应的访问时间和标识信息,确定每个访问权限等级对应的各个用户在指定的周期的访问频率;基于各个访问权限等级对应的各个用户的访问频率,对目标交管信息系统中的数据进行加固。由此,可以自适应的对交管信息系统的数据进行安全加固,降低用户访问过程中对交管信息系统所造成的安全威胁。



CN 116595573 A

1.一种交管信息系统的数据安全加固方法,其特征在于,包括:

响应于接收到任一用户对目标交管信息系统的数据访问指令,确定所述任一用户的访问权限等级以及待访问数据的类型,其中,所述数据访问指令中包含有所述任一用户的标识信息和所述待访问数据的类型;

判断所述类型是否属于预设的敏感数据类型或者限制访问类型;

若所述类型属于所述预设的敏感数据类型或者限制访问类型,则将所述任一用户的标识信息,以及所述任一用户的访问时间存储在数据库中;

按照指定的周期,根据所述数据库中各个用户对应的访问时间和标识信息,确定每个所述访问权限等级对应的各个用户在所述指定的周期的访问频率;

基于各个所述访问权限等级对应的各个用户的访问频率,对所述目标交管信息系统中的数据进行加固。

2.根据权利要求1所述的方法,其特征在于,所述响应于接收到任一用户对目标交管信息系统的数据访问指令,包括:

对所述任一用户进行生物识别,以判断所述任一用户是否为预先授权的用户,所述生物识别包含有人脸识别、指纹识别和活体检测;

在所述任一用户为预先授权的用户的情况下,对所述任一用户进行密码验证,并在验证通过的情况下,根据所述任一用户对所述目标交管信息系统的操作,生成数据访问指令。

3.根据权利要求1所述的方法,其特征在于,所述基于各个所述访问权限等级对应的各个用户的访问频率,对所述目标交管信息系统中的数据进行加固,包括:

获取与每个所述访问权限等级关联的第一数量;

响应与确定任一访问权限等级对应的各个用户中有所述第一数量的用户对应的所述访问频率大于第一阈值,对所述目标交管信息系统中的数据进行加固。

4.根据权利要求1所述的方法,其特征在于,所述基于各个所述访问权限等级对应的各个用户的访问频率,对所述目标交管信息系统中的数据进行加固,包括:

获取与至少一个目标访问权限等级关联的第二数量;

响应于确定所述至少一个目标访问权限等级对应的各个用户中有所述第二数量的用户对应的所述访问频率大于第一阈值,对所述目标交管信息系统中的数据进行加固。

5.根据权利要求1所述的方法,其特征在于,所述基于各个所述访问权限等级对应的各个用户的访问频率,对所述目标交管信息系统中的数据进行加固,包括:

响应于所述访问频率均大于所述第一阈值的用户数量在各个授权用户中的占比满足预设条件,对所述目标交管信息系统中的数据进行加固。

6.根据权利要求1所述的方法,其特征在于,所述对所述目标交管信息系统中的数据进行加固,包括:

对所述目标交管信息系统中的关键数据进行加密和备份,并将备份好的所述关键数据的数据包发送到多个关联的交管信息系统中进行存储;

启动更新维护程序,对所述目标交管信息系统进行更新维护。

7.根据权利要求1所述的方法,其特征在于,还包括:

按照预设的频率,对每个所述用户在所述目标交管信息系统中的事件日志进行分析,以获取所述用户的行为特征,其中,所述行为特征包括登录时间、访问路径、时间间隔、交互

行为；

获取与所述用户的标识信息关联的参考行为特征；

比较所述用户的行为特征和对应的所述参考行为特征之间的相似度；

在所述相似度小于预设阈值的情况下，对所述目标交管信息系统中的数据进行加固。

8.一种交管信息系统的数据安全加固装置，其特征在于，包括：

第一确定模块，用于响应于接收到任一用户对目标交管信息系统的数据访问指令，确定所述任一用户的访问权限等级以及待访问数据的类型，其中，所述数据访问指令中包含有所述任一用户的标识信息和所述待访问数据的类型；

判断模块，用于判断所述类型是否属于预设的敏感数据类型或者限制访问类型；

存储模块，用于若所述类型属于所述预设的敏感数据类型或者限制访问类型，则将所述任一用户的标识信息，以及所述任一用户的访问时间存储在数据库中；

第二确定模块，用于按照指定的周期，根据所述数据库中各个用户对应的访问时间和标识信息，确定每个所述访问权限等级对应的各个用户在所述指定的周期的访问频率；

加固模块，用于基于各个所述访问权限等级对应的各个用户的访问频率，对所述目标交管信息系统中的数据进行加固。

9.根据权利要求8所述的装置，其特征在于，所述第一确定模块，具体用于：

对所述任一用户进行生物识别，以判断所述任一用户是否为预先授权的用户，所述生物识别包含有人脸识别、指纹识别和活体检测；

在所述任一用户为预先授权的用户的情况下，对所述任一用户进行密码验证，并在验证通过的情况下，根据所述任一用户对所述目标交管信息系统的操作，生成数据访问指令。

10.根据权利要求8所述的装置，其特征在于，所述加固模块，具体用于：

获取与每个所述访问权限等级关联的第一数量；

响应与确定任一访问权限等级对应的各个用户中有所述第一数量的用户对应的所述访问频率大于第一阈值，对所述目标交管信息系统中的数据进行加固。

交管信息系统的数据安全加固方法及装置

技术领域

[0001] 本公开涉及数据处理技术领域，尤其涉及一种交管信息系统的数据安全加固方法及装置。

背景技术

[0002] 交管信息系统在现代社会中已经无处不在，我们通过交管信息系统进行的各种业务活动都离不开数据。然而，随着互联网和移动设备的普及，信息泄露、黑客攻击等安全威胁也愈加严重，对交管信息系统的数据安全提出了更高的要求。在用户对交管信息系统的访问过程中，极易出现数据的机密性泄露或者受到其他黑客攻击。如何对用户的行为进行监测，从而自适应的提高交管信息系统的数据安全是目前需要解决的问题。

发明内容

[0003] 本公开旨在至少在一定程度上解决相关技术中的技术问题之一。

[0004] 本公开第一方面实施例提出了一种交管信息系统的数据安全加固方法，包括：

[0005] 响应于接收到任一用户对目标交管信息系统的数据访问指令，确定所述任一用户的访问权限等级以及待访问数据的类型，其中，所述数据访问指令中包含有所述任一用户的标识信息和所述待访问数据的类型；

[0006] 判断所述类型是否属于预设的敏感数据类型或者限制访问类型；

[0007] 若所述类型属于所述预设的敏感数据类型或者限制访问类型，则将所述任一用户的标识信息，以及所述任一用户的访问时间存储在数据库中；

[0008] 按照指定的周期，根据所述数据库中各个用户对应的访问时间和标识信息，确定每个所述访问权限等级对应的各个用户在所述指定的周期的访问频率；

[0009] 基于各个所述访问权限等级对应的各个用户的访问频率，对所述目标交管信息系统中的数据进行加固。

[0010] 本公开第二方面实施例提出了一种交管信息系统的数据安全加固方法装置，包括：

[0011] 第一确定模块，用于响应于接收到任一用户对目标交管信息系统的数据访问指令，确定所述任一用户的访问权限等级以及待访问数据的类型，其中，所述数据访问指令中包含有所述任一用户的标识信息和所述待访问数据的类型；

[0012] 判断模块，用于判断所述类型是否属于预设的敏感数据类型或者限制访问类型；

[0013] 存储模块，用于若所述类型属于所述预设的敏感数据类型或者限制访问类型，则将所述任一用户的标识信息，以及所述任一用户的访问时间存储在数据库中；

[0014] 第二确定模块，用于按照指定的周期，根据所述数据库中各个用户对应的访问时间和标识信息，确定每个所述访问权限等级对应的各个用户在所述指定的周期的访问频率；

[0015] 加固模块，用于基于各个所述访问权限等级对应的各个用户的访问频率，对所述

目标交管信息系统中的数据进行加固。

[0016] 本公开第三方面实施例提出了一种电子设备，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时，实现如本公开第一方面实施例提出的交管信息系统的数据安全加固方法。

[0017] 本公开第四方面实施例提出了一种非临时性计算机可读存储介质，存储有计算机程序，所述计算机程序被处理器执行时实现如本公开第一方面实施例提出的交管信息系统的数据安全加固方法。

[0018] 本公开提供的交管信息系统的数据安全加固方法及装置，存在如下有益效果：

[0019] 本公开实施例中，该装置首先响应于接收到任一用户对目标交管信息系统的数据访问指令，确定所述任一用户的访问权限等级以及待访问数据的类型，其中，所述数据访问指令中包含有所述任一用户的标识信息和所述待访问数据的类型，之后判断所述类型是否属于预设的敏感数据类型或者限制访问类型，若所述类型属于所述预设的敏感数据类型或者限制访问类型，则将所述任一用户的标识信息，以及所述任一用户的访问时间存储在数据库中，之后按照指定的周期，根据所述数据库中各个用户对应的访问时间和标识信息，确定每个所述访问权限等级对应的各个用户在所述指定的周期的访问频率，然后基于各个所述访问权限等级对应的各个用户的访问频率，对所述目标交管信息系统中的数据进行加固。由此，能够结合每个用户的访问频率和访问时间，来判断是否对交管信息系统中的数据进行加固，从而可以自适应的对交管信息系统的数据进行安全加固，降低用户访问过程中对交管信息系统所造成的安全威胁。

[0020] 本公开附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本公开的实践了解到。

附图说明

[0021] 本公开上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0022] 图1为本公开实施例所提供的一种交管信息系统的数据安全加固方法的流程示意图；

[0023] 图2为本公开实施例所提供的一种交管信息系统的数据安全加固方法装置的结构框图；

[0024] 图3示出了适于用来实现本公开实施方式的示例性计算机设备的框图。

具体实施方式

[0025] 下面详细描述本公开的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本公开，而不能理解为对本公开的限制。

[0026] 下面参考附图描述本公开实施例的交管信息系统的数据安全加固方法、装置、计算机设备和存储介质。

[0027] 需要说明的是，本公开实施例中的交管信息系统的数据安全加固方法的执行主体为交管信息系统的数据安全加固方法装置，该装置可以由软件和/或硬件的方式实现，该装

置可以配置在任意电子设备中，或者也可以是服务器。在本公开提出的场景中，下面将以“交管信息系统的数据安全加固方法装置”作为执行主体对本公开实施例中提出的交管信息系统的数据安全加固方法进行说明，在此不进行限定。

[0028] 图1为本公开实施例所提供的交管信息系统的数据安全加固方法的流程示意图。

[0029] 如图1所示，该交管信息系统的数据安全加固方法可以包括以下步骤：

[0030] 步骤101，响应于接收到任一用户对目标交管信息系统的数据访问指令，确定任一用户的访问权限等级以及待访问数据的类型，其中，数据访问指令中包含有任一用户的标识信息和待访问数据的类型。

[0031] 可选的，可以首先对任一用户进行生物识别，以判断任一用户是否为预先授权的用户，生物识别包含有人脸识别、指纹识别和活体检测。

[0032] 可以理解的是，可以预先存储有授权用户的指纹信息、人脸信息，从而在任一用户触发了对目标交管信息系统的访问请求之后，该装置可以对任一用户进行生物识别。其中，生物识别可以是一种用于识别人类特征的技术，包括生物特征和行为特征。生物特征可能包括指纹、虹膜、声纹、面部识别等，行为特征则可以包含如敲击模式、手写模式等。为了对个体进行生物识别，交管信息系统通常需要先收集并存储特定的生物数据样本。例如，采用指纹识别技术时，系统可能需要先使用设备扫描用户的指纹，并将其存储在数据库中，然后在需要验证用户身份时比对实际的指纹样本。在生物识别期间，系统会比对当前获取到的生物数据与已存储在数据库中的数据，从而确定是否匹配。如果匹配成功，则交管信息系统将确认该用户的身份，并提供适当的访问权限或其他操作权限。

[0033] 其中，访问权限等级可以根据安全需要和操作权限来分为不同的级别，本公开实施例中，访问权限至少包括：全部访问权限(Full Access)：拥有所有文件、文件夹、系统配置和管理员权限，可以执行任何任务。可写访问权限(Write Access)：允许用户创建、修改和删除文件、文件夹和其他资源。读取访问权限(Read Access)：允许用户查看和阅读任何数据、文档或资源，但不允许对其进行任何更改。执行访问权限(Execute Access)：运行可执行文件、命令行脚本等程序的权限。添加、编辑和删除访问权限(Add,Edit and Delete Access)：提供修改数据和添加新数据的权限。访问某些文件或文件夹的访问权限(Access to Some Files or Folders)：仅限于能够访问指定的文件或文件夹。没有访问权限(No Access)：不具备查看、编辑或管理资源的权限。需要说明的是，访问权限等级可能会因系统或组织的需求而略有不同。在敏感或特殊环境中，可以设置更高或更严格的权限级别以保护重要信息的安全性。

[0034] 其中，全部访问权限对应的权限等级最高为1级，没有访问权限对应的权限等级最低，为6级，其中，可写访问权限、读取访问权限、执行访问权限、添加、编辑和删除访问权限这四种访问权限可以分为2级、3级、4级、5级这4个等级。

[0035] 需要说明的是，对于不同的访问权限等级的数据，加密的策略也是不相同的，因而用户在进行解密时也需要按照对应的解密方式进行解密。

[0036] 进一步地，在任一用户为预先授权的用户的情况下，对任一用户进行密码验证，并在验证通过的情况下，根据任一用户对目标交管信息系统的操作，生成数据访问指令。

[0037] 需要说明的是，在对任一用户进行密码验证时需要根据任一用户所访问的数据的访问权限等级，确定对应的密码验证策略。进而可以在用户验证通过的情况下，生成对应的

数据访问指令。

[0038] 步骤102,判断类型是否属于预设的敏感数据类型或者限制访问类型。

[0039] 其中,敏感数据类型可以有个人身份信息:例如姓名、地址、社会安全号码、银行卡号码、医疗保健信息等。企业机密:例如商业计划、合同、财务报告、客户列表、专利、技术数据等,敏感数据:例如档案、安全信息、法律文件等,健康/医疗数据:例如医疗历史记录、诊断、治疗等等,在此不做限定。需要说明的是,不同的交管信息系统,对应的交管信息系统中的敏感数据类型或者限制访问类型也经常是不同的。本公开在此仅为一种示意性的说明。在不同行业的交管信息系统中,有对应不同的敏感数据类型或者限制访问类型。其中,限制访问类型可以为具有限制访问次数或者访问权限的数据类型,其可以为目标交管信息系统所属企业所预设的数据类型。

[0040] 步骤103,若类型属于预设的敏感数据类型或者限制访问类型,则将任一用户的标识信息,以及任一用户的访问时间存储在数据库中。

[0041] 其中,用户的标识可以为用户的姓名、或者ID,在此不做限定。其中,在该类型属于预设的敏感数据类型或者限制访问类型的情况下,则可以对本次用户的访问情况进行记录,也即可以记录好该任一用户的标识信息、访问时间、访问数据的类型,以及对访问数据的操作记录等等信息,并存储在数据库中。

[0042] 步骤104,按照指定的周期,根据数据库中各个用户对应的访问时间和标识信息,确定每个访问权限等级对应的各个用户在指定的周期的访问频率。

[0043] 其中,指定的周期可以为1天、或者2天,在此不做限定。

[0044] 其中,访问频率包含有第一访问频率,和第二访问频率。

[0045] 其中,第一访问频率是指用户对敏感数据类型或者限制访问类型的访问频率。

[0046] 其中,第二访问频率是指任一类型的敏感数据或者限制访问类型的被访问频率。

[0047] 举例来说,若在指定周期访问权限等级为S级的A类型敏感数据被70个用户访问了,则访问权限等级为S级的A类型敏感数据的第二访问频率即为70。

[0048] 若在指定周期内标识信息为009的用户X访问了敏感数据类型或者限制访问类型的数据的次数为150次,访问了非敏感数据类型和限制访问类型的数据的次数为25次,那么则用户X的第一访问频率可以为150。

[0049] 具体的,可以根据每个用户对应的标识信息和访问时间确定每个用户的访问次数,进而确定第一访问频率和第二访问频率。

[0050] 步骤105,基于各个访问权限等级对应的各个用户的访问频率,对目标交管信息系统中的数据进行加固。

[0051] 可选的,可以首先获取与每个访问权限等级关联的第一数量,之后响应与确定任一访问权限等级对应的各个用户中有第一数量的用户对应的访问频率大于第一阈值,对目标交管信息系统中的数据进行加固。

[0052] 需要说明的是,每个访问权限等级都对应有第一数量,其中,第一数量是对任一访问权限等级的数量的数量预警值,也即若在指定的周期内,有第一数量的用户访问了该任一访问权限等级的数据,则此时说明访问频率过高,因而需要对目标交管信息系统中的数据进行加固。举例来说,若访问权限等级为4级的数据有A、B、C、D,对应的第一数量为5000,其中,A、B、C、D被各个用户访问的人数为5000,且这5000个用户对应的第一访问频率均大于

第一阈值的情况下,则此时说明目标交管信息系统的敏感数据类型或者限制访问类型被大量访问,此时可能出现了信息泄露或者信息公开的风险,因而需要对其进行加固。

[0053] 可选的,可以获取与至少一个目标访问权限等级关联的第二数量,之后响应于确定所述至少一个目标访问权限等级对应的各个用户中有所述第二数量的用户对应的所述访问频率大于第一阈值,对所述目标交管信息系统中的数据进行加固。

[0054] 其中,第二数量可以为与目标访问权限等级对应的数量的预警值。其中,目标访问权限等级最高,其对应的数量较低,第二数量小于第一数量。比如说,若目标访问权限等级为R,且R对应的第二数量为30,则说明若有30个用户对目标访问权限等级的数据进行了访问,并且这30个用户对目标访问权限等级的数据的访问频率均大于第一阈值,则说明目标交管信息系统的最敏感的数据类型或者严禁限制访问类型被大量访问,此时可能出现了信息泄露或者信息公开的风险,因而需要对其进行加固。

[0055] 可选的,可以响应于所述访问频率均大于所述第一阈值的用户数量在各个授权用户中的占比满足预设条件,对所述目标交管信息系统中的数据进行加固。

[0056] 其中,预设条件可以为占比大于或者等于75%。举例来说,若当前在指定的周期内访问目标交管信息系统的用户一共有300个,其中,288个用户的访问频率均高于第一阈值,也即访问频率均大于所述第一阈值的用户数量在各个授权用户中的占比满足预设条件,此时对所述目标交管信息系统中的数据进行加固,此时说明目标交管信息系统的敏感数据类型或者限制访问类型被大量访问,此时可能出现了信息泄露或者信息公开的风险,因而需要对其进行加固。

[0057] 可选的,对目标交管信息系统中的数据进行加固,包括:

[0058] 对所述目标交管信息系统中的关键数据进行加密和备份,并将备份好的所述关键数据的数据包发送到多个关联的交管信息系统中进行存储;

[0059] 启动更新维护程序,对所述目标交管信息系统进行更新维护。

[0060] 可选的,可以启动预设的更新维护程序,以按照现有交管信息系统的架构和规划需求,分析并确定需要进行更新和维护的区域和项项目,制定相应的更新方案。或者,可以向开发人员发送维护指令,以提示开发人员开发更新维护程序,根据具体情况可以选择编程语言和数据库技术,并编写相应的执行脚本。需要说明的是,对于生产环境中的交管信息系统,先在测试环境中进行系统更新,以避免因错误的更新操作导致系统不稳定或停机的风险。在更新前备份原有系统数据和程序,防止出现不可逆损失,运行更新维护程序,根据提示完成更新和维护相关操作。在更新和维护过程中,需要不断监控系统状态和异常反馈,及时调整更新方案,确保所有工作都得到正确的执行。更新后,进行必要的验证和测试,以确保更新后的系统正常运行,能够满足用户需求,并记录更新和维护过程中的所有操作及结果,用以追溯问题或作为后续运维工作的参考。

[0061] 需要说明的是,在对交管信息系统中的重要数据进行加固时,可以使用加密算法,保护数据安全的方法,其目的是使数据在传输和存储过程中不被未经授权的人员访问或窃取。加密算法可以保护各种类型的数据,包括文本、图像、音频和视频等。

[0062] 可选的,可以采用对称加密算法,其特点是加密和解密使用相同的密钥。对称加密算法包括DES、3DES、AES等。其中,AES算法是一种比较流行的对称加密算法,其密钥长度可以为128位、192位或256位。在AES算法中,加密和解密过程都是通过轮函数完成的。轮函数

包括四个步骤:字节代替、列混淆、行移位和轮密钥加。其中,轮密钥加是指将轮密钥与明文进行异或运算,以增加加密的强度。对称加密算法的解密方法与加密方法相同,都是使用相同的密钥进行解密。因此,在使用对称加密算法时,需要注意密钥的安全性,以避免密钥被泄露导致数据被盗取。

[0063] 或者,也可以采用非对称加密算法,其中,非对称加密算法是一种比对称加密算法更加安全的加密方法,其特点是加密和解密使用不同的密钥。非对称加密算法包括RSA和ECC等。在RSA算法中,加密和解密使用的密钥是一对公钥和私钥。公钥是可以公开的,用于加密数据;私钥是保密的,用于解密数据。RSA算法的加密过程是将明文进行公钥加密,解密过程是将密文进行私钥解密。在ECC算法中,加密和解密使用的密钥是一对椭圆曲线上的点。ECC算法的加密过程是将明文进行点乘运算,解密过程是将密文进行点乘逆运算。非对称加密算法的解密方法相对于对称加密算法更加复杂。因为非对称加密算法加密使用的公钥是公开的,所以其安全性较高。或者,可以将对称加密算法和非对称加密算法结合使用,以达到安全性和效率的平衡。可选的,还可以使用哈希算法,其中,哈希算法是一种将任意长度的消息压缩成固定长度的算法,其主要应用是验证数据的完整性和一致性。哈希算法包括MD5、SHA-1、SHA-2等。在哈希算法中,加密过程是将明文进行哈希计算,得到一个固定长度的哈希值。哈希值具有唯一性和不可逆性,即不同的明文得到的哈希值是不同的,相同的明文得到的哈希值也是相同的;同时,不能通过哈希值推导出原始明文。哈希算法没有解密方法,因为哈希算法是一种单向函数,即无法通过哈希值推导出原始明文。因此,在使用哈希算法时,需要注意选择合适的哈希算法和哈希值长度,以确保数据的完整性和一致性。

[0064] 可选的,可以按照预设的频率,对每个用户在目标交管信息系统中的事件日志进行分析,以获取用户的行为特征,其中,行为特征包括登录时间、访问路径、时间间隔、交互行为,之后获取与所述用户的标识信息关联的参考行为特征,然后比较所述用户的行为特征和对应的所述参考行为特征之间的相似度,在所述相似度小于预设阈值的情况下,对所述目标交管信息系统中的数据进行加固。

[0065] 本公开实施例中,该装置首先响应于接收到任一用户对目标交管信息系统的数据访问指令,确定所述任一用户的访问权限等级以及待访问数据的类型,其中,所述数据访问指令中包含有所述任一用户的标识信息和所述待访问数据的类型,之后判断所述类型是否属于预设的敏感数据类型或者限制访问类型,若所述类型属于所述预设的敏感数据类型或者限制访问类型,则将所述任一用户的标识信息,以及所述任一用户的访问时间存储在数据库中,之后按照指定的周期,根据所述数据库中各个用户对应的访问时间和标识信息,确定每个所述访问权限等级对应的各个用户在所述指定的周期的访问频率,然后基于各个所述访问权限等级对应的各个用户的访问频率,对所述目标交管信息系统中的数据进行加固。由此,能够结合每个用户的访问频率和访问时间,来判断是否对交管信息系统中的数据进行加固,从而可以自适应的对交管信息系统的数据进行安全加固,降低用户访问过程中对交管信息系统所造成的安全威胁,通过对数据加固,可以保证数据在传输、存储和处理过程中的机密性、完整性和可用性,从而有效地防止数据被非法获取、篡改或破坏等风险,提高系统的可靠性和稳定性,降低业务中断和数据损失风险。保护企业形象和声誉:对于一些敏感业务,如电子支付、公共安全等,数据的泄露或损坏可能会导致公司形象受损,给企业带来巨大的经济损失。数据加固可以帮助企业更好地保护数据和系统,避免这类安全事件

的发生，从而保护企业形象和声誉。

[0066] 为了实现上述实施例，本公开还提出一种交管信息系统的数据安全加固方法装置。

[0067] 图2为本公开第三实施例所提供的交管信息系统的数据安全加固方法装置的结构框图。

[0068] 如图2所示，该交管信息系统的数据安全加固方法装置200可以包括：

[0069] 第一确定模块210，用于响应于接收到任一用户对目标交管信息系统的数据访问指令，确定所述任一用户的访问权限等级以及待访问数据的类型，其中，所述数据访问指令中包含有所述任一用户的标识信息和所述待访问数据的类型；

[0070] 判断模块220，用于判断所述类型是否属于预设的敏感数据类型或者限制访问类型；

[0071] 存储模块230，用于若所述类型属于所述预设的敏感数据类型或者限制访问类型，则将所述任一用户的标识信息，以及所述任一用户的访问时间存储在数据库中；

[0072] 第二确定模块240，用于按照指定的周期，根据所述数据库中各个用户对应的访问时间和标识信息，确定每个所述访问权限等级对应的各个用户在所述指定的周期的访问频率；

[0073] 加固模块250，用于基于各个所述访问权限等级对应的各个用户的访问频率，对所述目标交管信息系统中的数据进行加固。

[0074] 可选的，所述第一确定模块，具体用于：

[0075] 对所述任一用户进行生物识别，以判断所述任一用户是否为预先授权的用户，所述生物识别包含有人脸识别、指纹识别和活体检测；

[0076] 在所述任一用户为预先授权的用户的情况下，对所述任一用户进行密码验证，并在验证通过的情况下，根据所述任一用户对所述目标交管信息系统的操作，生成数据访问指令。

[0077] 可选的，所述加固模块，具体用于：

[0078] 获取与每个所述访问权限等级关联的第一数量；

[0079] 响应与确定任一访问权限等级对应的各个用户中有所述第一数量的用户对应的所述访问频率大于第一阈值，对所述目标交管信息系统中的数据进行加固。

[0080] 可选的，所述加固模块，具体用于：

[0081] 获取与至少一个目标访问权限等级关联的第二数量；

[0082] 响应于确定所述至少一个目标访问权限等级对应的各个用户中有所述第二数量的用户对应的所述访问频率大于第一阈值，对所述目标交管信息系统中的数据进行加固。

[0083] 可选的，所述加固模块，具体用于：

[0084] 响应于所述访问频率均大于所述第一阈值的用户数量在各个授权用户中的占比满足预设条件，对所述目标交管信息系统中的数据进行加固。

[0085] 可选的，所述加固模块，具体用于：

[0086] 对所述目标交管信息系统中的关键数据进行加密和备份，并将备份好的所述关键数据的数据包发送到多个关联的交管信息系统中进行存储；

[0087] 启动更新维护程序，对所述目标交管信息系统进行更新维护。

[0088] 可选的，该装置，还包括：

[0089] 分析模块，用于按照预设的频率，对每个所述用户在所述目标交管信息系统中的事件日志进行分析，以获取所述用户的行为特征，其中，所述行为特征包括登录时间、访问路径、时间间隔、交互行为；

[0090] 获取模块，用于获取与所述用户的标识信息关联的参考行为特征；

[0091] 比较模块，用于比较所述用户的行为特征和对应的所述参考行为特征之间的相似度；

[0092] 处理模块，用于在所述相似度小于预设阈值的情况下，对所述目标交管信息系统中的数据进行加固。

[0093] 本公开实施例中，该装置首先响应于接收到任一用户对目标交管信息系统的数据访问指令，确定所述任一用户的访问权限等级以及待访问数据的类型，其中，所述数据访问指令中包含有所述任一用户的标识信息和所述待访问数据的类型，之后判断所述类型是否属于预设的敏感数据类型或者限制访问类型，若所述类型属于所述预设的敏感数据类型或者限制访问类型，则将所述任一用户的标识信息，以及所述任一用户的访问时间存储在数据库中，之后按照指定的周期，根据所述数据库中各个用户对应的访问时间和标识信息，确定每个所述访问权限等级对应的各个用户在所述指定的周期的访问频率，然后基于各个所述访问权限等级对应的各个用户的访问频率，对所述目标交管信息系统中的数据进行加固。由此，能够结合每个用户的访问频率和访问时间，来判断是否对交管信息系统中的数据进行加固，从而可以自适应的对交管信息系统的数据进行安全加固，降低用户访问过程中对交管信息系统所造成的安全威胁。

[0094] 为了实现上述实施例，本公开还提出一种计算机设备，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行程序时，实现如本公开前述实施例提出的交管信息系统的数据安全加固方法。

[0095] 为了实现上述实施例，本公开还提出一种非临时性计算机可读存储介质，存储有计算机程序，计算机程序被处理器执行时实现如本公开前述实施例提出的交管信息系统的数据安全加固方法。

[0096] 为了实现上述实施例，本公开还提出一种计算机程序产品，当计算机程序产品中的指令处理器执行时，执行如本公开前述实施例提出的交管信息系统的数据安全加固方法。

[0097] 图3示出了适于用来实现本公开实施方式的示例性计算机设备的框图。图3显示的计算机设备12仅仅是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

[0098] 如图3所示，计算机设备12以通用计算设备的形式表现。计算机设备12的组件可以包括但不限于：一个或者多个处理器或者处理单元16，系统存储器28，连接不同系统组件(包括系统存储器28和处理单元16)的总线18。

[0099] 总线18表示几类总线结构中的一种或多种，包括存储器总线或者存储器控制器，外围总线，图形加速端口，处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说，这些体系结构包括但不限于工业标准体系结构(Industry Standard Architecture；以下简称：ISA)总线，微通道体系结构(Micro Channel Architecture；以下简称：MAC)总线，增强型ISA总线、视频电子标准协会(Video Electronics Standards

Association;以下简称:VESA)局域总线以及外围组件互连(Peripheral Component Interconnection;以下简称:PCI)总线。

[0100] 计算机设备12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被计算机设备12访问的可用介质,包括易失性和非易失性介质,可移动的和不可移动的介质。

[0101] 存储器28可以包括易失性存储器形式的计算机系统可读介质,例如随机存取存储器(Random Access Memory;以下简称:RAM)30和/或高速缓存存储器32。计算机设备12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例,存储系统34可以用于读写不可移动的、非易失性磁介质(图3未显示,通常称为“硬盘驱动器”)。尽管图3中未示出,可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器,以及对可移动非易失性光盘(例如:光盘只读存储器(Compact Disc Read Only Memory;以下简称:CD-ROM)、数字多功能只读光盘(Digital Video Disc Read Only Memory;以下简称:DVD-ROM)或者其它光介质)读写的光盘驱动器。在这些情况下,每个驱动器可以通过一个或者多个数据介质接口与总线18相连。存储器28可以包括至少一个程序产品,该程序产品具有一组(例如至少一个)程序模块,这些程序模块被配置以执行本公开各实施例的功能。

[0102] 具有一组(至少一个)程序模块42的程序/实用工具40,可以存储在例如存储器28中,这样的程序模块42包括但不限于操作系统、一个或者多个应用程序、其它程序模块以及程序数据,这些示例中的每一个或某种组合中可能包括网络环境的实现。程序模块42通常执行本公开所描述的实施例中的功能和/或方法。

[0103] 计算机设备12也可以与一个或多个外部设备14(例如键盘、指向设备、显示器24等)通信,还可与一个或者多个使得用户能与该计算机设备12交互的设备通信,和/或与使得该计算机设备12能与一个或多个其它计算设备进行通信的任何设备(例如网卡,调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口22进行。并且,计算机设备12还可以通过网络适配器20与一个或者多个网络(例如局域网(Local Area Network;以下简称:LAN),广域网(Wide Area Network;以下简称:WAN)和/或公共网络,例如因特网)通信。如图所示,网络适配器20通过总线18与计算机设备12的其它模块通信。应当明白,尽管图中未示出,可以结合计算机设备12使用其它硬件和/或软件模块,包括但不限于:微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0104] 处理单元16通过运行存储在系统存储器28中的程序,从而执行各种功能应用以及数据处理,例如实现前述实施例中提及的方法。

[0105] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本公开的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外,在不相互矛盾的情况下,本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0106] 此外,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者

隐含地包括至少一个该特征。在本公开的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

[0107] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现定制逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本公开的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本公开的实施例所属技术领域的技术人员所理解。

[0108] 在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，"计算机可读介质"可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。计算机可读介质的更具体的示例(非穷尽性列表)包括以下:具有一个或多个布线的电连接部(电子装置)，便携式计算机盘盒(磁装置)，随机存取存储器(RAM)，只读存储器(ROM)，可擦除可编辑只读存储器(EPROM或闪速存储器)，光纤装置，以及便携式光盘只读存储器(CDROM)。另外，计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质，因为可以例如通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序，然后将其存储在计算机存储器中。

[0109] 应当理解，本公开的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。如，如果用硬件来实现和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现:具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0110] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0111] 此外，在本公开各个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时，也可以存储在一个计算机可读取存储介质中。

[0112] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。尽管上面已经示出和描述了本公开的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本公开的限制，本领域的普通技术人员在本公开的范围内可以对上述实施例进行变化、修改、替换和变型。

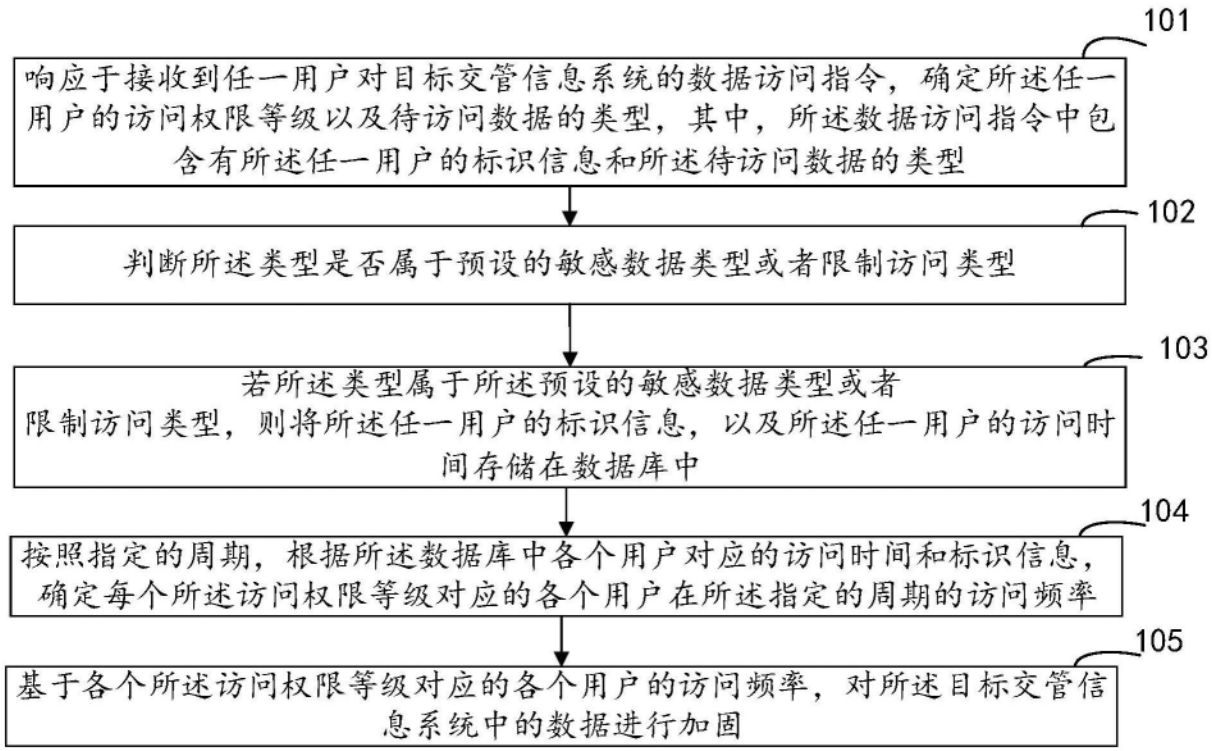

101
响应于接收到任一用户对目标交管信息系统的数据访问指令，确定所述任一用户的访问权限等级以及待访问数据的类型，其中，所述数据访问指令中包含有所述任一用户的标识信息和所述待访问数据的类型
102
判断所述类型是否属于预设的敏感数据类型或者限制访问类型
103
若所述类型属于所述预设的敏感数据类型或者限制访问类型，则将所述任一用户的标识信息，以及所述任一用户的访问时间存储在数据库中
104
按照指定的周期，根据所述数据库中各个用户对应的访问时间和标识信息，确定每个所述访问权限等级对应的各个用户在所述指定的周期的访问频率
105
基于各个所述访问权限等级对应的各个用户的访问频率，对所述目标交管信息系统中的数据进行加固

图1

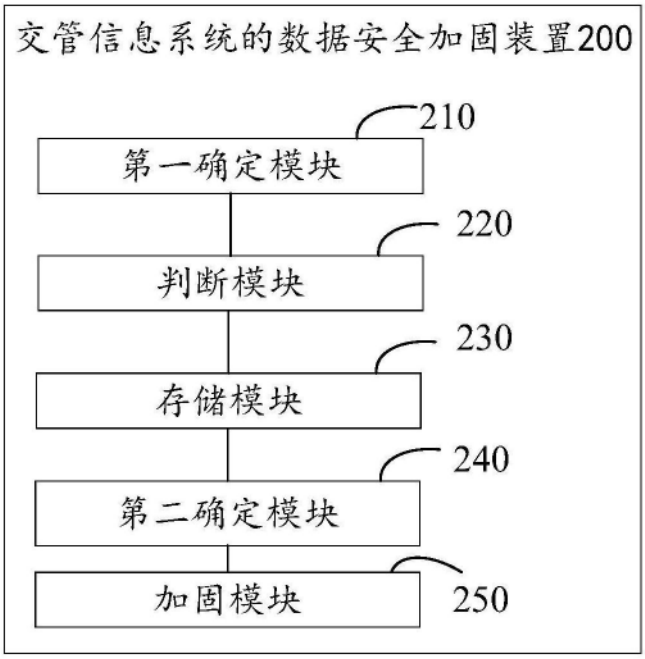

交管信息系统的数据安全加固装置200
210
第一确定模块
220
判断模块
230
存储模块
240
第二确定模块
加固模块
250

图2

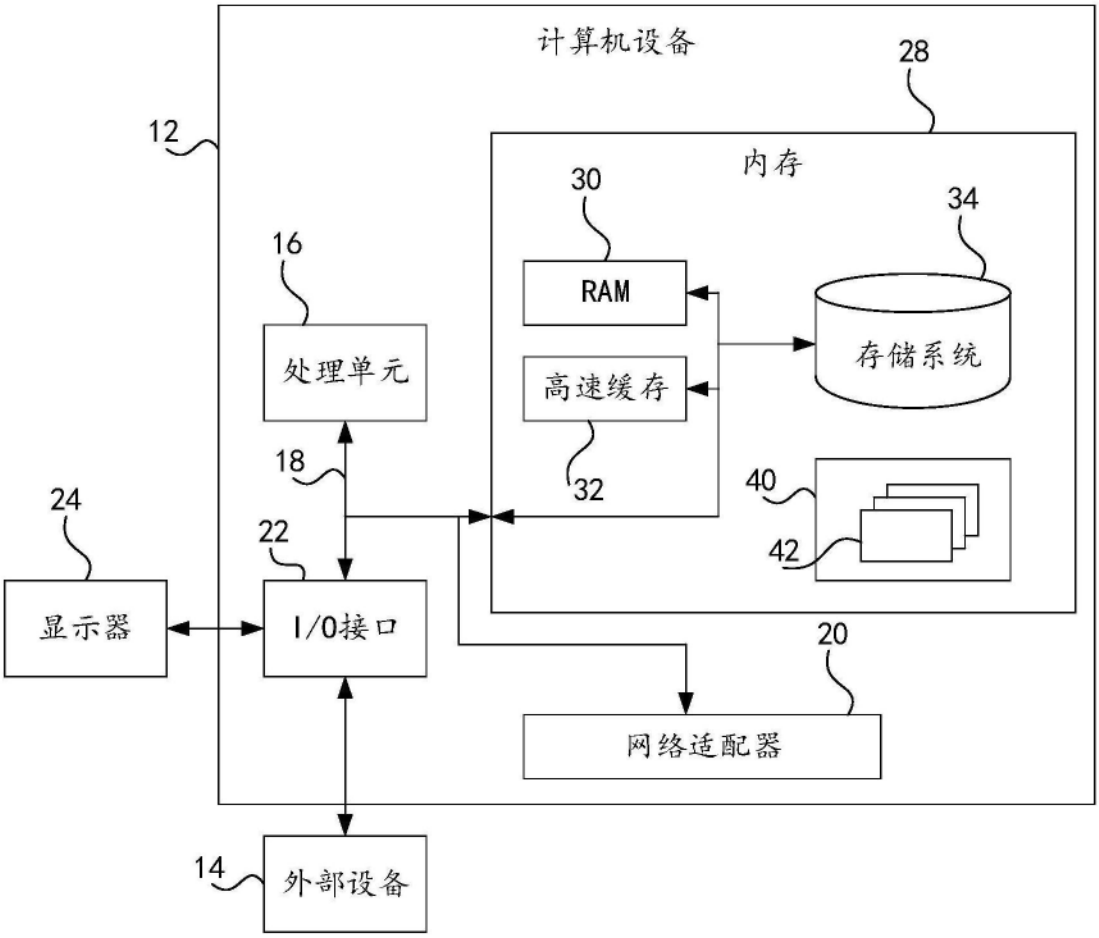

计算机设备
12
28
内存
30
34
16
RAM
处理单元
存储系统
高速缓存
18
32
40
24
22
42
显示器
I/O接口
20
网络适配器
14
外部设备

图3