(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110084007 B
(45)授权公告日 2023.11.28

(21)申请号 201811355486.5
(22)申请日 2014.10.13
(65)同一申请的已公布的文献号
申请公布号 CN 110084007 A
(43)申请公布日 2019.08.02
(62)分案原申请数据
201410539483.2 2014.10.13
(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心
(72)发明人 吕鲲
(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
专利代理师 林祥
(51)Int.Cl.
G06F 21/31(2013.01)
G06Q 20/20(2012.01)
G06Q 20/40(2012.01)
G06Q 30/0601(2023.01)
H04L 67/306(2022.01)
H04L 9/40(2022.01)
G06Q 50/00(2012.01)

(56)对比文件
CN 103024744 A,2013.04.03
CN 103123712 A,2013.05.29
TW 201104602 A,2011.02.01
CN 102045634 A,2011.05.04
CN 103944722 A,2014.07.23
CN 103530772 A,2014.01.22

审查员 冉凡坤

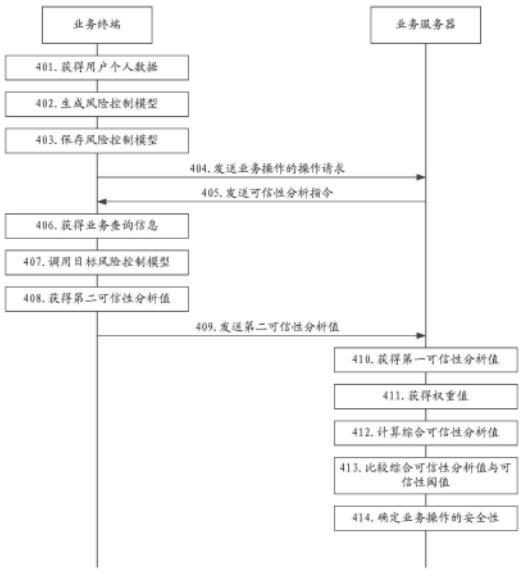
权利要求书2页 说明书10页 附图5页

(54)发明名称

风险控制模型的构建方法、装置及终端

(57)摘要

本申请公开了风险控制模型的构建方法、装置及终端，该方法包括：根据终端用户的授权权限从业务终端内获得用户个人数据；通过分析所述用户个人数据生成多个风险控制模型；将所述多个风险控制模型保存到所述业务终端的本地安全控制数据库。



CN 110084007 B

1.一种风险控制模型的构建方法,其特征在于,所述方法包括:

根据终端用户的授权权限从业务终端内获得用户个人数据;所述用户个人数据为所述终端用户的私密信息;

通过分析所述用户个人数据生成风险控制模型;

将所述风险控制模型保存到所述业务终端的本地安全控制数据库;所述业务终端基于所述风险控制模型获得待发送至业务服务器的第二可信性分析值,所述第二可信性分析值用于辅助业务服务器确定所述业务终端的业务操作的安全性。

2.根据权利要求1所述的方法,其特征在于,所述将所述风险控制模型保存到所述业务终端的本地安全控制数据库之前,还包括:

对所述风险控制模型分别进行加密;

所述将所述风险控制模型保存到所述业务终端的本地安全控制数据库具体为:

将加密后的风险控制模型保存到所述业务终端的本地安全控制数据库。

3.根据权利要求1所述的方法,其特征在于,所述用户个人数据包括至少一种下述数据:

用户社交数据、兴趣爱好数据、日常习惯数据。

4.根据权利要求3所述的方法,其特征在于,所述风险控制模型包括至少一个下述模型:

根据所述用户社交数据生成的社交关系控制模型、根据所述兴趣爱好数据生成的兴趣爱好控制模型、根据所述日常习惯数据生成的生活习惯控制模型。

5.一种风险控制模块的构建装置,其特征在于,所述装置包括:

获得单元,用于根据终端用户的授权权限从业务终端内获得用户个人数据;所述用户个人数据为所述终端用户的私密信息;

生成单元,用于通过分析所述用户个人数据生成风险控制模型;

保存单元,用于将所述风险控制模型保存到所述业务终端的本地安全控制数据库;所述业务终端基于所述风险控制模型获得待发送至业务服务器的第二可信性分析值,所述第二可信性分析值用于辅助业务服务器确定所述业务终端的业务操作的安全性。

6.根据权利要求5所述的装置,其特征在于,所述装置还包括:

加密单元,用于对所述生成单元生成的所述风险控制模型分别进行加密;

所述保存单元,具体用于将加密后的风险控制模型保存到所述业务终端的本地安全控制数据库。

7.根据权利要求5所述的装置,其特征在于,所述用户个人数据包括至少一种下述数据:

用户社交数据、兴趣爱好数据、日常习惯数据。

8.根据权利要求7所述的装置,其特征在于,所述风险控制模型包括至少一个下述模型:

根据所述用户社交数据生成的社交关系控制模型、根据所述兴趣爱好数据生成的兴趣爱好控制模型、根据所述日常习惯数据生成的生活习惯控制模型。

9.一种终端,其特征在于,包括:

处理器;用于存储所述处理器可执行指令的存储器;

其中,所述处理器被配置为:

根据终端用户的授权权限从业务终端内获得用户个人数据;所述用户个人数据为所述终端用户的私密信息;

通过分析所述用户个人数据生成风险控制模型;

将所述风险控制模型保存到所述业务终端的本地安全控制数据库;所述业务终端基于所述风险控制模型获得待发送至业务服务器的第二可信性分析值,所述第二可信性分析值用于辅助业务服务器确定所述业务终端的业务操作的安全性。

风险控制模型的构建方法、装置及终端

[0001] 本申请为2014年10月13日提交中国专利局、申请号为201410539483.2、申请名称为“验证业务操作安全性的方法、装置、终端及服务器”的中国专利申请的分案申请。

技术领域

[0002] 本申请涉及通信技术领域，尤其涉及风险控制模型的构建方法、装置及终端。

背景技术

[0003] 随着智能终端的发展和网络应用的普及，用户可以通过终端上安装的各种应用客户端实现各种业务操作，例如，社交类即时通信业务，购物支付类业务等。要实现上述业务，终端用户往往需要在服务器上注册业务账户，并基于该业务账户实现一定的业务操作。

[0004] 现有技术中，可以基于大数据挖掘技术获得终端用户的网络行为数据，在通过业务账户进行业务操作时，业务服务器可以根据终端用户的网络行为数据对业务安全性进行验证，以避免业务风险。但是，由于网络行为数据的挖掘主要局限于终端用户的历史业务数据，历史浏览数据等，数据内容比较单一，从而导致业务操作安全性验证的结果不够准确。

发明内容

[0005] 本申请提供风险控制模型的构建方法、装置及终端，以解决现有技术中业务操作安全性验证结果不够准确的问题。

[0006] 根据本申请实施例的第一方面，提供一种风险控制模型的构建方法，所述方法包括：

[0007] 根据终端用户的授权权限从业务终端内获得用户个人数据；

[0008] 通过分析所述用户个人数据生成风险控制模型；

[0009] 将所述风险控制模型保存到所述业务终端的本地安全控制数据库。

[0010] 根据本申请实施例的第二方面，提供另一种风险控制模型的构建方法，所述方法包括：

[0011] 获得单元，用于根据终端用户的授权权限从业务终端内获得用户个人数据；

[0012] 生成单元，用于通过分析所述用户个人数据生成风险控制模型；

[0013] 保存单元，用于将所述风险控制模型保存到所述业务终端的本地安全控制数据库。

[0014] 根据本申请实施例的第三方面，提供一种终端，包括：

[0015] 处理器；用于存储所述处理器可执行指令的存储器；

[0016] 其中，所述处理器被配置为：

[0017] 根据终端用户的授权权限从业务终端内获得用户个人数据；

[0018] 通过分析所述用户个人数据生成风险控制模型；

[0019] 将所述风险控制模型保存到所述业务终端的本地安全控制数据库。

[0020] 本申请实施例中，业务终端接收业务服务器发送的业务操作的可信性分析指令

后,根据可信性分析指令调用预存的风险控制模型,获得业务操作的可信性分析结果,并将该可信性分析结果发送至业务服务器,业务服务器根据该可信性分析结果确定业务操作的安全性。应用本申请实施例对业务操作的安全性进行验证时,可以利用业务终端内部的风险控制模型获得业务操作的可信性分析结果,由于风险控制模型可以根据业务终端内保存的用户私密数据生成,更能真实反映用户的社交关系、生活习惯等,因此在业务终端上利用上述风险控制模型对业务操作进行可信性评判,可以提高业务操作安全验证的准确性。

附图说明

[0021] 图1为本申请实施例的验证业务操作安全性的场景示意图;

[0022] 图2为本申请验证业务操作安全性的方法的一个实施例流程图;

[0023] 图3为本申请验证业务操作安全性的方法的另一个实施例流程图;

[0024] 图4为本申请验证业务操作安全性的方法的另一个实施例流程图;

[0025] 图5为本申请验证业务操作安全性的装置所在设备的一种硬件结构图;

[0026] 图6为本申请验证业务操作安全性的装置的一个实施例框图;

[0027] 图7为本申请验证业务操作安全性的装置的另一个实施例框图;

[0028] 图8为本申请验证业务操作安全性的装置的另一个实施例框图。

具体实施方式

[0029] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0030] 在本申请使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0031] 应当理解,尽管在本申请可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本申请范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0032] 参见图1,为本申请实施例的验证业务操作安全性的场景示意图:

[0033] 图1场景中包括:业务服务器,以及在业务服务器上注册过业务账户的用户的手机,结合本申请实施例中的描述,图1中示出的手机包括作为业务终端的手机A和作为第三方终端的手机B。其中,手机A本地设置了安全控制数据库,该安全控制数据库中包括根据手机A内的用户个人数据建立的多个风险控制模型,业务服务器收到业务操作请求后,通过向手机A发送业务操作的可信性分析指令,以使手机A通过调用风险控制模型获得业务操作的可信性分析结果,并返回给业务服务器,业务服务器根据该可信性分析结果确定业务操作的安全性。本申请实施例中,由于用户个人数据是保存在手机上的用户的私密数据,其更能

真实反映用户的社交关系、生活习惯等,因此利用基于上述私密数据建立的风险控制模型对用户的业务操作进行可信性评判,可以提高业务操作安全验证的准确性。

[0034] 参见图2,为本申请验证业务操作安全性的方法的一个实施例流程图,该实施例从业务终端侧进行描述:

[0035] 步骤201:接收业务服务器发送的业务操作的可信性分析指令。

[0036] 本申请实施例中,业务终端的终端用户可以预先在业务服务器上注册业务账户,以便终端用户在根据业务账户登录业务服务器后,可以基于业务服务器完成各种业务操作。其中,业务终端可以包括各种智能手机、平板电脑、PC(Personal Computer,个人计算机)等;业务服务器可以是由可信第三方设置并支持实现特定业务的服务器,例如,可以具体为支持物品选择交易的第三方支付系统服务器。

[0037] 本申请实施例中,业务终端的终端用户可以通过业务终端主动向业务服务器发送业务操作的操作请求,例如,终端用户在业务终端上进行转账操作,则业务终端向业务服务器发送该转账操作的操作请求;或者,第三方终端可以向业务服务器发送针对业务终端的终端用户的业务操作的操作请求,例如,第三方终端的终端用户在购买某件商品后,向业务服务器发送请求业务终端的终端用户进行代付操作的操作请求。在业务服务器接收到业务操作的操作请求后,向业务终端发送该业务操作的可信性分析指令。

[0038] 步骤202:根据可信性分析指令调用预存的风险控制模型,获得业务操作的可信性分析结果。

[0039] 本申请实施例中,业务终端在获得终端用户的授权权限后,可以基于该权限从业务终端内获得用户个人数据,其中,用户个人数据可以包括用户社交数据、兴趣爱好数据、日常习惯数据等;业务终端通过分析上述用户个人数据生成多个风险控制模型,每个风险控制模型中可以包含业务信息与业务可信性分析值的对应关系,其中,风险控制模型可以包括根据用户社交数据生成的社交关系控制模型,根据兴趣爱好数据生成的兴趣爱好控制模型,根据日常习惯数据生成的生活习惯控制模型等;然后业务终端可以将这些风险控制模型加密后,保存到业务终端的本地安全控制数据库内。

[0040] 本实施例中,业务终端可以根据可信性分析指令,获得业务操作的业务查询信息,其中,根据发送操作请求的终端的不同,可以有如下不同的业务查询信息获取方式:

[0041] 第一种方式,当由业务终端向业务服务器发送操作请求时,业务终端可以在接收到可信性分析指令时,根据自身发送的操作请求获得业务操作的业务查询信息,该业务查询信息可以包括业务对象信息、业务操作类型信息、业务操作内容信息等。例如,以业务操作为转账操作为例,其中业务对象信息为转账对象的姓名,业务操作类型信息为转账,业务操作内容信息为转账金额。

[0042] 第二种方式,当由第三方终端向业务服务器发送操作请求时,业务服务器可以从该操作请求中获得业务查询信息,然后业务服务器将该业务查询信息携带在可信性分析指令中并发送至业务终端,业务终端从该可信性分析指令中获得业务查询信息,该业务查询信息可以包括业务对象信息、业务操作类型信息、业务操作内容信息等。例如,以业务操作为代付操作为例,其中业务对象信息为代付发起人的姓名,业务操作类型信息为代付,业务操作内容信息为代付金额。

[0043] 在获得业务操作的业务查询信息后,业务终端可以根据业务操作的类型从预存的

风险控制模型中调用目标风险控制模型;在调用到目标风险控制模型后,业务终端可以以业务查询信息为关键字查找目标风险控制模型,获得与查找到的业务信息对应的业务可信性分析值作为可信性分析结果。

[0044] 步骤203:将可信性分析结果发送至业务服务器,以使业务服务器根据可信性分析结果确定业务操作的安全性。

[0045] 由上述实施例可见,该实施例对业务操作的安全性进行验证时,可以利用业务终端内部的风险控制模型获得业务操作的可信性分析结果,由于风险控制模型可以根据业务终端内保存的用户私密数据生成,更能真实反映用户的社交关系、生活习惯等,因此在业务终端上利用上述风险控制模型对业务操作进行可信性评判,可以提高业务操作安全验证的准确性。

[0046] 参见图3,为本申请验证业务操作安全性的方法的另一个实施例流程图,该实施例从业务服务器侧进行描述:

[0047] 步骤301:向业务终端发送业务操作的可信性分析指令。

[0048] 步骤302:接收业务终端发送的可信性分析结果,该可信性分析结果为业务终端根据可信性分析指令调用预存的风险控制模型获得的该业务操作的可信性分析结果。

[0049] 上述步骤301和步骤302中业务服务器从发送可信性分析指令到接收到可信性分析结果的过程与前述图2所示实施例中的描述一致,在此不再赘述。

[0050] 步骤303:根据该可信性分析结果确定业务操作的安全性。

[0051] 本实施例中,业务服务器上保存有本地风险控制模型,与现有技术一致,该本地风险控制模型可以根据终端用户的网络行为数据创建,在对业务操作的安全性进行验证时,业务服务器可以先根据该本地风险控制模型获得业务操作的第一可信性分析值,并将业务终端发送的可信性分析结果作为第二可信性分析值,然后分别获取为第一可信性分析值和第二可信性分析值设置的权重值,将第一可信性分析值和第二可信性分析值分别与各自的权重值相乘求和,得到综合可信性分析值,然后比较该综合可信性分析值和预设的可信性阈值,根据比较结果,如果综合可信性分析值大于可信性阈值,则可以确定该业务操作安全,如果综合可信性分析值不大于可信性阈值,则可以确定该业务操作不安全。

[0052] 由上述实施例可见,该实施例对业务操作的安全性进行验证时,可以利用业务终端内部的风险控制模型获得业务操作的可信性分析结果,由于风险控制模型可以根据业务终端内保存的用户私密数据生成,更能真实反映用户的社交关系、生活习惯等,因此在业务终端上利用上述风险控制模型对业务操作进行可信性评判,可以提高业务操作安全验证的准确性。

[0053] 参见图4,为本申请验证业务操作安全性的方法的另一个实施例流程图,该实施例通过业务终端与业务服务器之间的交互详细描述了验证业务操作安全性的过程:

[0054] 步骤401:业务终端根据终端用户的授权权限从业务终端内获得用户个人数据。

[0055] 业务终端内的用户个人数据为终端用户的私密信息,本申请实施例在利用用户个人数据对业务操作的可信性进行分析时,可以预先获得终端用户的授权权限,并基于该授权权限获得业务终端内的用户个人数据。在实际应用中,可以设置一APP(Application,应用),以获取用户个人数据,当终端用户安装该APP后,即获得终端用户的授权权限,可以从业务终端内读取用户个人数据。

[0056] 其中,用户个人数据可以包括至少一种下述数据:

[0057] 1、用户社交数据,可以包括业务终端内的常规通信信息,例如,通信录内的分组信息、联系人信息、备注信息等,通话记录内的通话对象、通话时长、通话次数信息等,短消息记录内的短消息对象、短消息数量等;也可以包括业务终端内安装的即时通信工具内的通信信息,例如,即时通信联系人信息、每个联系人的联系时长信息等。

[0058] 2、兴趣爱好数据,可以包括通过业务终端内浏览器获得的终端用户的浏览记录信息,例如,用户搜索的商品信息、事件信息等;也可以包括通过业务终端内的定位装置获得的用户的地理位置信息,例如,用户常去的餐厅、商场等;

[0059] 3、日常习惯数据,可以包括业务终端内记事本记录的信息,例如,用户行程信息、提醒事项信息等;也可以包括业务终端内的工具设置信息,例如,闹钟设置时间、日历提醒事项等。

[0060] 需要说明的是,终端用户可以通过授权,指定业务终端获取所有的用户个人数据,也可以指定业务终端获得上述用户个人数据中的至少一种数据,对此本申请实施例不进行限制。

[0061] 步骤402:业务终端通过分析用户个人数据生成多个风险控制模型。

[0062] 在步骤401中获得用户个人数据后,可以对不同类型的用户个人数据进行分析,得到至少一个下述风险控制模型,每个风险控制模型包含了业务信息与业务可信性分析值的对应关系:

[0063] 1、根据用户社交数据生成的社交关系控制模型,该社交关系控制模型可以包括用户的联系人与该联系人的可信性分析值的对应关系。例如,对于联系人A,如果其为终端用户的亲人,则联系人A可以获得最高的可信性分析值;对于联系人B,如果其加入用户通信录的时间较长,且与用户通话频率较高,则联系人B可能为用户的同事或朋友,因此其也可以获得较高的可信性分析值;对于联系人C,如果其加入用户通信录的时间较短,且仅与用户有较少的短信交互,则联系人C可能为陌生人,会获得较低的可信性分析值。

[0064] 2、根据兴趣爱好数据生成的兴趣爱好控制模型,该兴趣爱好控制模型可以包括用户的感兴趣对象与该感兴趣对象的可信性分析值的对应关系。例如,如果用户的感兴趣对象为笔记本电脑,且用户的浏览记录表明用户在一段时间内频繁浏览关于笔记本电脑的相关信息,则可以为笔记本电脑设置较高可信性分析值;如果用户的感兴趣对象为某个商场,但地理位置信息表明该用户几乎未来过该商场,则可以为该商场设置较低的可信性分析值。

[0065] 3、根据日常习惯数据生成的生活习惯控制模型,该生活习惯控制模型包括用户的生活对象与该生活对象的可信性分析值的对应关系。例如,用户的生活对象为每晚8点到公园跑步一小时,则为每晚8点到9点在公园跑步设置较高的可信性分析值。

[0066] 需要说明的是,对于上述风险控制模型中未包含的业务信息,则可以默认其对应的可信性分析值为0。

[0067] 步骤403:业务终端将多个风险控制模型保存到本地安全控制数据库。

[0068] 本实施例中,为了保证业务终端内风险控制模型的安全性,使得终端用户的私密信息不会泄露,可以对步骤402中得到的多个风险控制模型进行加密,并将加密后的风险控制模型保存到本地安全控制数据库中,相应的,在使用风险控制模型时,可以采用与加密算

法对应的解密算法对加密的风险控制模型进行解密即可。

[0069] 步骤404:当终端用户发起业务操作时,业务终端向业务服务器发送该业务操作的操作请求。

[0070] 本实施例中,终端用户预先在业务服务器上注册了业务账户,当终端用户根据该业务账户登录业务服务器后,可以基于业务服务器完成各种业务操作。在终端用户发起某个业务操作时,业务终端向业务服务器发送该业务操作的操作请求,该操作请求中可以包含业务对象信息、业务类型信息、业务内容信息等,例如当业务操作为终端用户向好友转账一万元,则业务对象信息可以包括好友的用户名、姓名、手机号码、邮箱等,业务类型信息为转账,业务内容信息为转账金额一万元。

[0071] 步骤405:业务服务器根据该操作请求向业务终端发送业务操作的可信性分析指令。

[0072] 本实施例中,当业务服务器接收到业务操作的操作请求后,请求回调业务终端对该业务操作的可信性进行分析,此时业务服务器向业务终端发送该业务操作的可信性分析指令。

[0073] 步骤406:业务终端根据发送的操作请求获得业务操作的业务查询信息。

[0074] 如前步骤404中所述,业务操作的操作请求中可以包含业务对象信息、业务类型信息、业务内容信息等,业务终端可以将上述信息作为业务操作的业务查询信息。

[0075] 步骤407:业务终端根据该业务操作的类型从多个风险控制模型中调用目标风险控制模型。

[0076] 由于业务终端本地安全控制数据库中保存了多个风险控制模型,每个风险控制模型可以对应不同类型的业务操作,因此本实施例中,业务终端可以根据业务操作的类型从多个风险控制模型中调用与该业务操作的类型对应的目标风险控制模型。例如,当业务操作的类型为转账或代付时,其涉及到转账的对象和发起代付的对象,这些对象与终端用户之间存在某种社交关系,因此可以从风险控制模型中调用社交关系控制模型。

[0077] 步骤408:业务终端以业务查询信息为关键字查找目标风险控制模型,获得与查找到的业务信息对应的业务可信性分析值,该业务可信性分析值为第二可信性分析值。

[0078] 业务终端以步骤406中获得的业务查询信息为关键字查找目标风险控制模型,以获得作为第二可信性分析值的业务可信性分析值。仍以业务操作为终端用户向好友转账一万元为例,则步骤406中对应获得的而业务查询信息可以包括作为业务对象信息的好友的用户名、姓名、手机号码、邮箱等,业务类型信息为转账,业务内容信息为转账金额一万元,步骤407中相应根据业务类型信息“转账”调用的目标风险控制模型为社交关系控制模型;业务终端可以以好友姓名和手机号码为关键字查找社交关系控制模型,获得对应的业务可信性分析值,由于好友与终端用户具有亲密关系,因此在生成社交关系控制模型时,该业务可信性分析值较高。

[0079] 步骤409:业务终端向业务服务器发送第二可信性分析值。

[0080] 步骤410:业务服务器根据本地风险控制模型获得该业务操作的第一可信性分析值。

[0081] 本实施例中,业务服务器上保存有本地风险控制模型,与现有技术一致,该本地风险控制模型可以根据终端用户的网络行为数据创建,在对业务操作的安全性进行验证时,

业务服务器可以先根据该本地风险控制模型获得业务操作的第一可信性分析值。

[0082] 步骤411:业务服务器分别获得第一可信性分析值和第二可信性分析值的权重值。

[0083] 本实施例中,业务服务器可以预先为自身获得的第一可信性分析值和从业务终端获得的第二可信性分析值设置权重值,并将设置的权重值保存在本地。需要说明的是,上述权重值可以根据实际应用的需要进行调整,对此本申请实施例不进行限制。

[0084] 步骤412:业务服务器根据权重值计算第一可信性分析值和第二可信性分析值的综合可信性分析值。

[0085] 本步骤中业务服务器可以将第一可信性分析值与其权重值相乘,并将第二可信性分析值与其权重值相乘,将上述两个乘积相加作为综合可信性分析值。

[0086] 步骤413:业务服务器比较综合可信性分析值与预设的可信性阈值。

[0087] 本实施例中,业务服务器可以预先设置可信性阈值,以便通过比较综合可信性分析值与该可信性阈值,确定业务操作的安全性。

[0088] 仍以转账业务为例,假设业务服务器上预先设置的可信性阈值为60,为第一可信性分析值和第二可信性分析值设置的权重值分别为80%和20%,业务服务器自身获得的第一可信性分析值为50,业务服务器从业务终端获得的第二可信性分析值为90,则按照步骤412计算得到的综合可信性分析值为:80%×55+20%×90=62。

[0089] 步骤414:根据比较结果确定该业务操作的安全性。

[0090] 根据步骤413中的比较结果,如果综合可信性分析值大于可信性阈值,则可以确定业务操作安全,如果综合可信性分析值不大于可信性阈值,则可以确定业务操作不安全。例如,终端用户要转账给好友一万元,如果按照现有技术,由于该转账金额较大,则业务服务器根据计算得到的第一可信性分析值55(小于可信性阈值60),会确定该转账业务不可信,但显然该验证结果不准确;而采用本申请实施例,由于可以结合业务终端获得的第二可信性分析值,结合步骤413中的示例,计算得到的综合可信性分析值为62,由于该综合可信性分析值62大于可信性阈值60,因此可以确定该转账业务安全,由此可见,采用本申请实施例可以提高对业务操作安全性验证的准确性。

[0091] 由上述应用实施例可见,该实施例对业务操作的安全性进行验证时,可以利用业务终端内部的风险控制模型获得业务操作的可信性分析结果,由于风险控制模型可以根据业务终端内保存的用户私密数据生成,更能真实反映用户的社交关系、生活习惯等,因此在业务终端上利用上述风险控制模型对业务操作进行可信性评判,可以提高业务操作安全验证的准确性。

[0092] 与本申请验证业务操作安全性的方法的实施例相对应,本申请还提供了验证业务操作安全性的装置的实施例。

[0093] 本发明验证业务操作安全性的装置的实施例可以分别应用在终端或业务服务器上。装置实施例可以通过软件实现,也可以通过硬件或者软硬件结合的方式实现。以软件实现为例,作为一个逻辑意义上的装置,是通过其所在设备的CPU将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言,如图5所示,为本发明验证业务操作安全性的装置所在设备的一种硬件结构图,除了图5所示的CPU、内存、网络接口、以及非易失性存储器之外,实施例中装置所在的设备通常还可以包括其他硬件,对此图5不再分别示出。

[0094] 参见图6,为本申请验证业务操作安全性的装置的一个实施例框图,该装置可以应用在业务终端内,该装置包括:接收单元610、分析单元620和发送单元630。

[0095] 其中,接收单元610,用于接收业务服务器发送的业务操作的可信性分析指令;

[0096] 分析单元620,用于根据所述可信性分析指令调用预存的风险控制模型,获得所述业务操作的可信性分析结果;

[0097] 发送单元630,用于将所述可信性分析结果发送至所述业务服务器,以使所述业务服务器根据所述可信性分析结果确定所述业务操作的安全性。

[0098] 参见图7,为本申请验证业务操作安全性的装置的另一个实施例框图,该装置在图6所示装置基础上,进一步包括:获得单元640、生成单元650、加密单元660和保存单元670。

[0099] 其中,获得单元640,用于根据终端用户的授权权限从业务终端内获得用户个人数据;

[0100] 生成单元650,用于通过分析所述用户个人数据生成所述风险控制模型;

[0101] 加密单元660,用于对所述生成单元生成的所述风险控制模型进行加密;

[0102] 保存单元670,用于将加密后的风险控制模型保存到所述业务终端的本地安全控制数据库。

[0103] 结合上述图6或图7所示的装置实施例,在一个可选的实现方式中:

[0104] 所述分析单元620可以包括:

[0105] 业务查询信息获得子单元,用于根据所述可信性分析指令,获得所述业务操作的业务查询信息;

[0106] 目标风险控制模型调用子单元,用于根据所述业务操作的类型从所述预存的风险控制模型中调用目标风险控制模型,所述风险控制模型中包含业务信息与业务可信性分析值的对应关系;

[0107] 业务可信性分析值获得子单元,用于以所述业务查询信息为关键字查找所述目标风险控制模型,获得与查找到的业务信息对应的业务可信性分析值。

[0108] 在另一个可选的实现方式中:

[0109] 上述业务查询信息获得子单元,可以具体用于从所述可信性分析指令中获得由所述可信性分析指令携带的所述业务操作的业务查询信息,所述业务查询信息为所述业务服务器根据第三方终端发送的所述业务操作的操作请求获得的信息。

[0110] 在另一个可选的实现方式中:

[0111] 所述发送单元630,还可以用于当终端用户发起所述业务操作时,向业务服务器发送所述业务操作的操作请求;

[0112] 所述业务查询信息获得子单元,可以具体用于在接收到所述可信性分析指令时,根据发送的所述操作请求获得所述业务操作的业务查询信息。

[0113] 参见图8,为本申请验证业务操作安全性的装置的另一个实施例框图,该装置可以应用在业务服务器内,该装置包括:

[0114] 该装置包括:发送单元810、接收单元820和验证单元830。

[0115] 其中,发送单元810,用于向业务终端发送业务操作的可信性分析指令;

[0116] 接收单元820,用于接收所述业务终端发送的可信性分析结果,所述可信性分析结果为所述业务终端根据所述可信性分析指令调用预存的风险控制模型获得的所述业务操

作的可信性分析结果；

[0117] 验证单元830，用于根据所述可信性分析结果确定所述业务操作的安全性。

[0118] 在一个可选的实现方式中：

[0119] 所述接收单元820，还可以用于接收第三方终端发送的所述业务操作的操作请求；

[0120] 所述装置还可以包括(图8中未示出)：获得单元，用于根据所述操作请求获得所述业务操作的业务查询信息；

[0121] 所述发送单元810，可以具体用于向业务终端发送携带了所述业务操作的业务查询信息的操作请求，以使所述业务终端以所述业务查询信息为关键字查找目标风险控制模型，获得与查找到的业务信息对应的业务可信性分析值，所述目标风险控制模型为所述业务终端根据所述业务操作的操作类型从所述预存的风险控制模型中调用的风险控制模型。

[0122] 在另一个可选的实现方式中：

[0123] 所述接收单元820，还可以用于当所述业务终端的终端用户发起所述业务操作时，接收所述业务终端发送的所述业务操作的操作请求；

[0124] 所述发送单元810，可以具体用于将所述操作请求作为触发指令，向所述业务终端发送所述业务操作的可信性分析指令。

[0125] 在另一个可选的实现方式中：

[0126] 所述验证单元830可以包括(图8中未示出)：

[0127] 可信性分析值获得子单元，用于根据本地风险控制模型获得所述业务操作的第一可信性分析值；

[0128] 权重值获得子单元，用于将所述业务终端发送的可信性分析结果作为第二可信性分析值，分别获得所述第一可信性分析值和所述第二可信性分析值的权重值；

[0129] 综合可信性分析值计算子单元，用于根据所述权重值计算所述第一可信性分析值和第二可信性分析值的综合可信性分析值；

[0130] 可信性分析值比较子单元，用于比较所述综合可信性分析值与预设的可信性阈值；

[0131] 业务安全性确定子单元，如果所述综合可信性分析值大于所述可信性阈值，则确定所述业务操作安全，如果所述综合可信性分析值不大于所述可信性阈值，则确定所述业务操作不安全。

[0132] 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0133] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置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申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0134] 由上述实施例可见，在对业务操作的安全性进行验证时，可以利用业务终端内部的风险控制模型获得业务操作的可信性分析结果，由于风险控制模型可以根据业务终端内保存的用户私密数据生成，更能真实反映用户的社交关系、生活习惯等，因此在业务终端上

利用上述风险控制模型对业务操作进行可信性评判,可以提高业务操作安全验证的准确性。

[0135] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的,本申请的真正范围和精神由下面的权利要求指出。

[0136] 应当理解的是,本申请并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

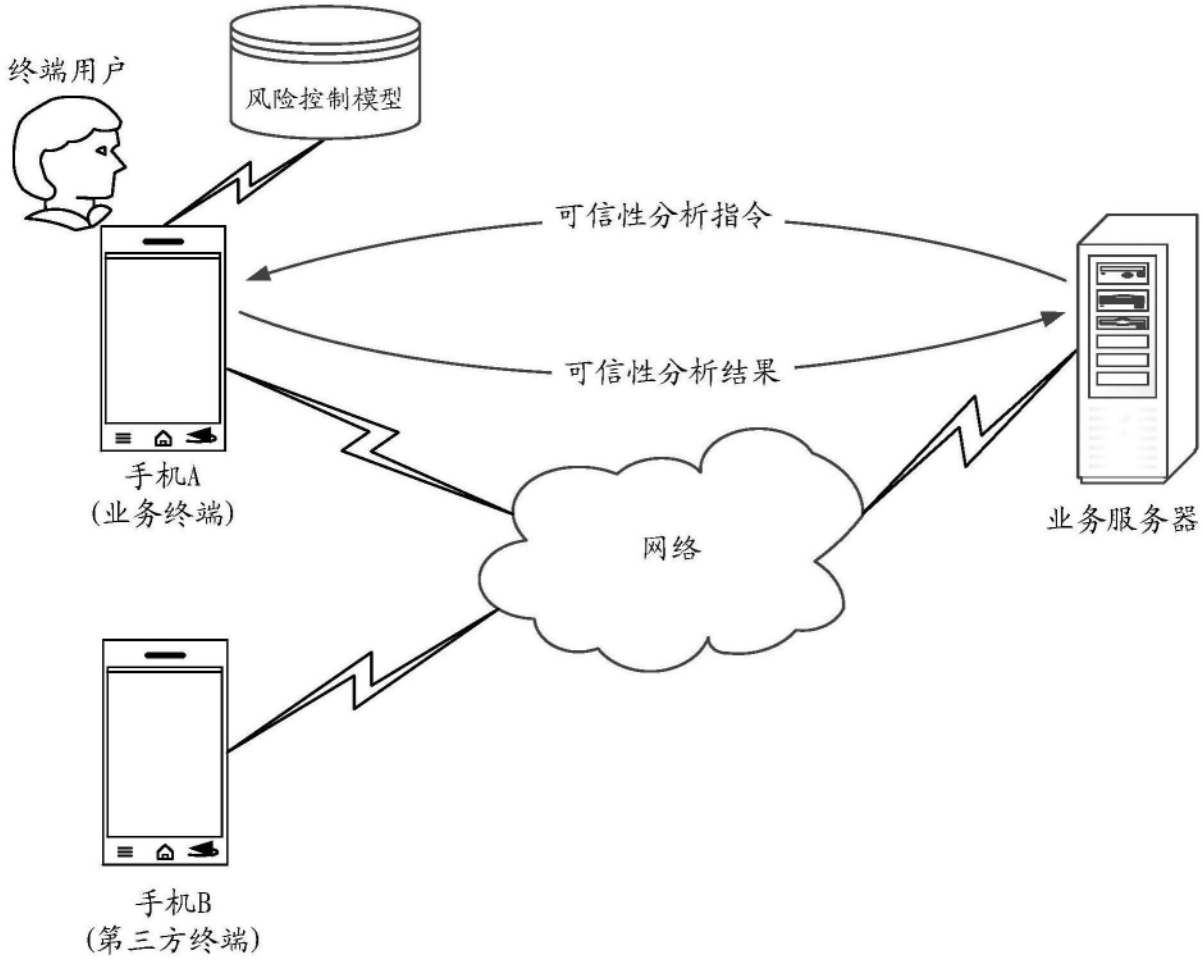

终端用户
风险控制模型
可信性分析指令
可信性分析结果
手机A
(业务终端)
网络
业务服务器
手机B
(第三方终端)

图1

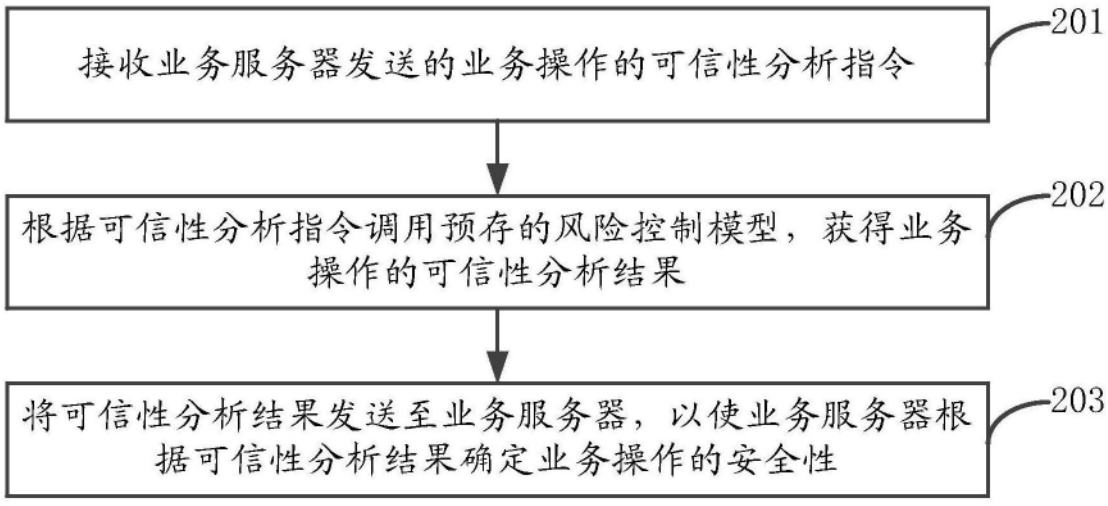

接收业务服务器发送的业务操作的可信性分析指令
201
根据可信性分析指令调用预存的风险控制模型，获得业务操作的可信性分析结果
202
将可信性分析结果发送至业务服务器，以使业务服务器根据可信性分析结果确定业务操作的安全性
203

图2

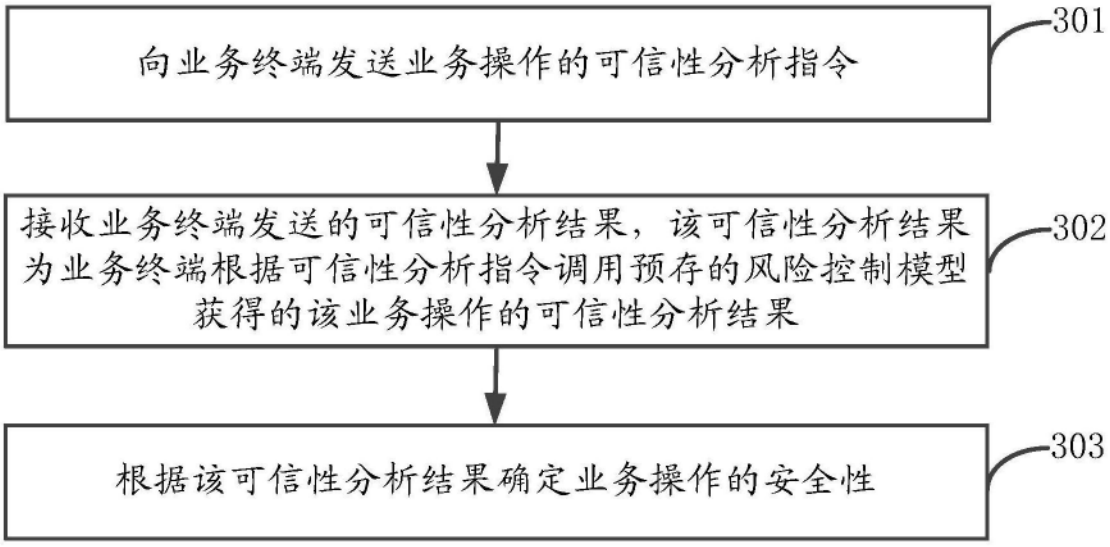

向业务终端发送业务操作的可信性分析指令
301
接收业务终端发送的可信性分析结果，该可信性分析结果为业务终端根据可信性分析指令调用预存的风险控制模型获得的该业务操作的可信性分析结果
302
根据该可信性分析结果确定业务操作的安全性
303

图3

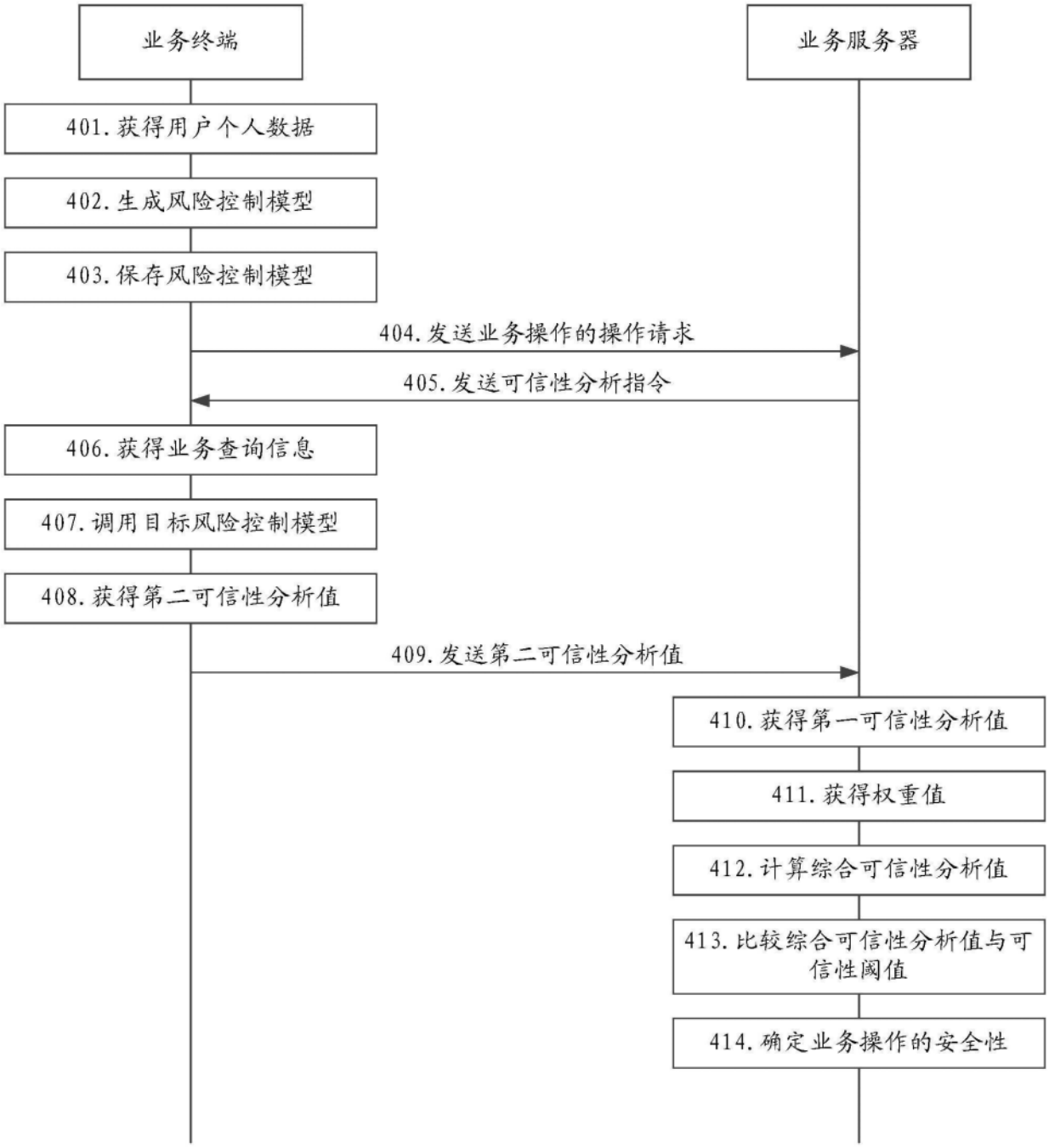

业务终端
业务服务器
401. 获得用户个人数据
402. 生成风险控制模型
403. 保存风险控制模型
404. 发送业务操作的操作请求
405. 发送可信性分析指令
406. 获得业务查询信息
407. 调用目标风险控制模型
408. 获得第二可信性分析值
409. 发送第二可信性分析值
410. 获得第一可信性分析值
411. 获得权重值
412. 计算综合可信性分析值
413. 比较综合可信性分析值与可信性阈值
414. 确定业务操作的安全性

图4

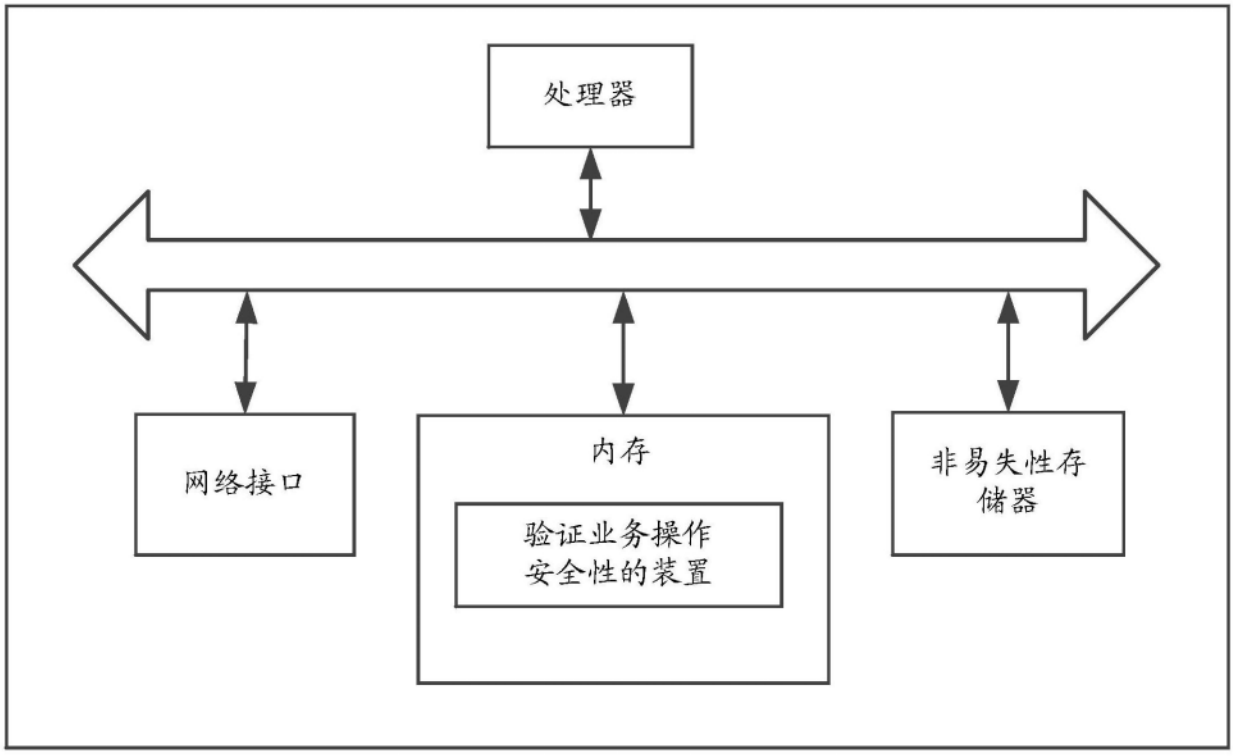

处理器
网络接口
内存
验证业务操作
安全性的装置
非易失性存
储器

图5

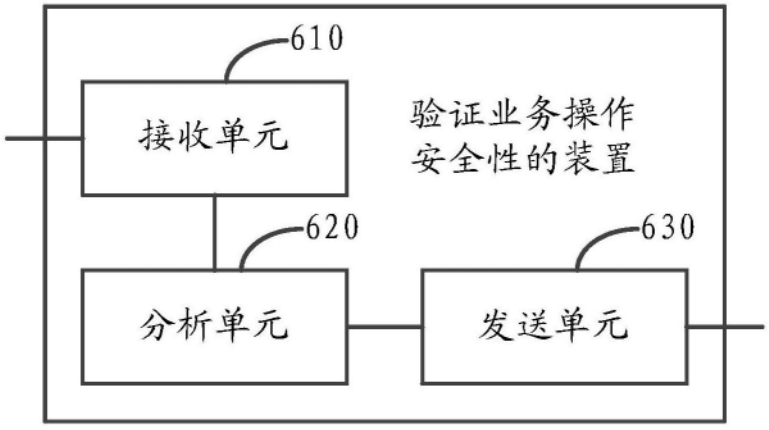

610
接收单元
验证业务操作
安全性的装置
620
630
分析单元
发送单元

图6

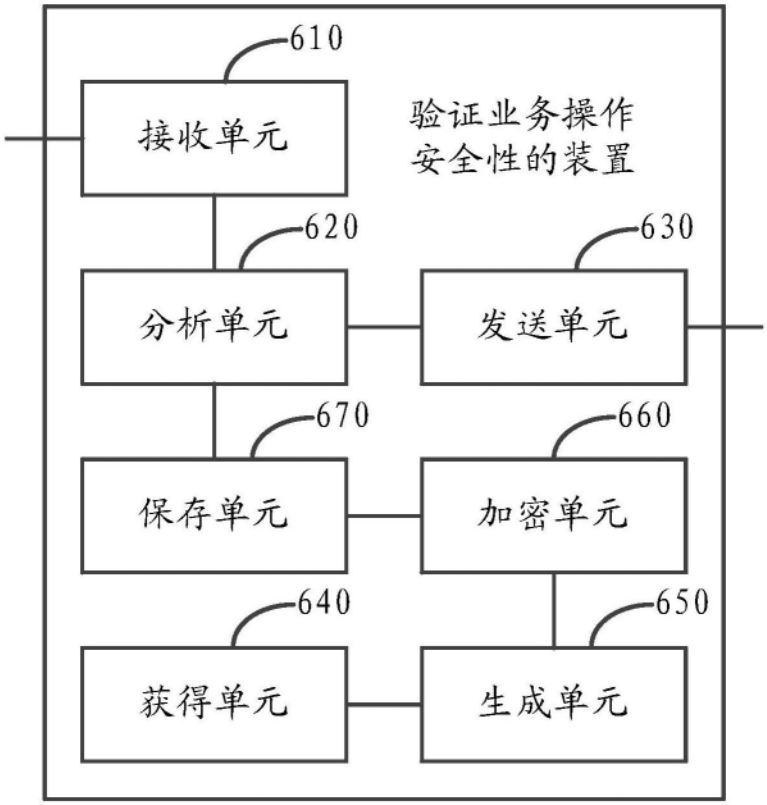

610
接收单元
验证业务操作
安全性的装置
620
630
分析单元
发送单元
670
660
保存单元
加密单元
640
650
获得单元
生成单元

图7

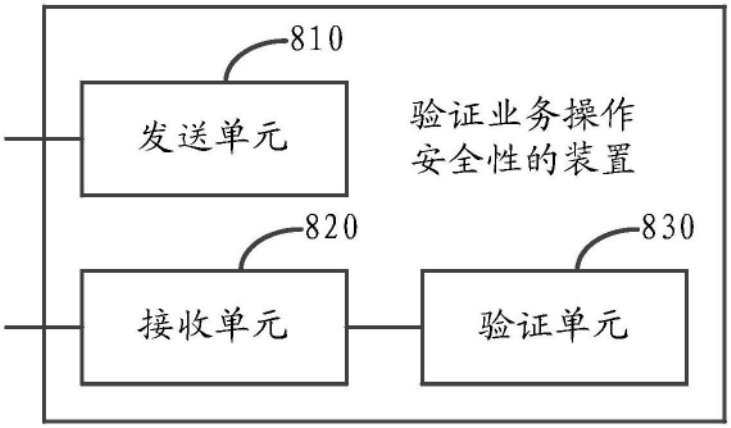

810
发送单元
验证业务操作
安全性的装置
820
830
接收单元
验证单元

图8