(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114866351 B
(45)授权公告日 2022.10.14

(21)申请号 202210785708.7
(22)申请日 2022.07.06
(65)同一申请的已公布的文献号
申请公布号 CN 114866351 A
(43)申请公布日 2022.08.05
(73)专利权人 湖南创星科技股份有限公司
地址 410000 湖南省长沙市长沙高新开发区岳麓西大道1698号麓谷科技创新创业园B1栋7楼、8楼及B2栋7楼、8楼
(72)发明人 任强 文建全 段志强 彭炜 黄刊迪 马云露
(74)专利代理机构 长沙智德知识产权代理事务所(普通合伙) 43207
专利代理师 陈铭浩
(51)Int.Cl.
H04L 9/40(2022.01)
G06F 21/56(2013.01)
G06K 9/62(2022.01)
(56)对比文件
WO 2017013712 A1,2017.01.26
US 2019065681 A1,2019.02.28
CN 109544373 A,2019.03.29
CN 108492196 A,2018.09.04
CN 109615012 A,2019.04.12
CN 109636635 A,2019.04.16
CN 109671476 A,2019.04.23
CN 111986037 A,2020.11.24
CN 112560027 A,2021.03.26
CN 112801805 A,2021.05.14
CN 113095365 A,2021.07.09
CN 113704731 A,2021.11.26
审查员 王星

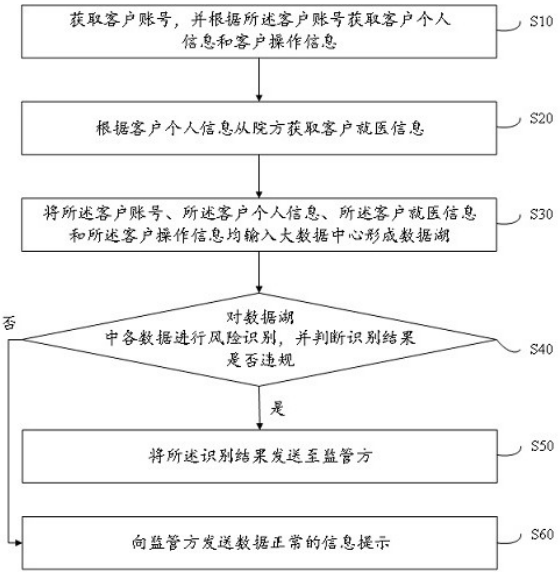
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种基于区块链的区域医疗处方监管方法及系统

(57)摘要

本发明公开了一种基于区块链的区域医疗处方监管方法及系统，该方法包括获取客户账号，并根据客户账号获取客户个人信息和客户操作信息；根据客户个人信息从院方获取客户就医信息；将客户账号、客户个人信息、客户就医信息和客户操作信息均输入大数据中心形成数据湖；对数据湖中各数据进行风险识别，并判断识别结果是否违规；当识别结果为违规时，将识别结果发送至监管方；当识别结果为不违规时，向监管方发送数据正常的信息提示。方本发明的技术方案通过大数据中心整合所有数据，并对识别出违规的数据，并将识别结果发送至监管方，以供监管方进行检测和确认，这样极大的降低了监管方的工作难度，有效的提高了监管方的工作效率。



CN 114866351 B

1.一种基于区块链的区域医疗处方监管方法,其特征在于,包括:

获取客户账号,并根据所述客户账号获取客户个人信息和客户操作信息;客户操作信息包括登录信息、页面操作信息、登录相关信息、日志信息和户端的静态基本信息,静态基本信息包括当前用户浏览器的类型、UserAgent、用户的IP地址、cookie信息、浏览器的插件信息和http请求头;

根据客户个人信息从院方获取客户就医信息;

将所述客户账号、所述客户个人信息、所述客户就医信息和所述客户操作信息均输入大数据中心形成数据湖;

对数据湖中各数据进行风险识别,并判断识别结果是否违规;

当所述识别结果为违规时,将所述识别结果发送至监管方;

当所述识别结果为不违规时,向监管方发送数据正常的信息提示;

所述对数据湖中各数据进行风险识别,并判断识别结果是否违规的步骤,还包括:

构建计算模型;

根据所述数据湖内的各数据通过所述计算模型,获取账号特征;

通过模拟退火算法对所述账号特征进行处理,分别获取隐含状态变量和观测变量;

通过维特比算法分别对所述隐含状态变量和所述观测变量进行处理,获取客户账号的隐含状态;

根据所述隐含状态判断该所述客户账号是否为恶意账号。

2.根据权利要求1所述的一种基于区块链的区域医疗处方监管方法,其特征在于,所述对数据湖中各数据进行风险识别,并判断识别结果是否违规的步骤,包括:

通过先聚类再分类的方式识别所述数据湖中各数据,以识别出被盗风险账号;

当识别出为所述被盗风险账号时,判定识别结果为违规;

所述当所述识别结果为违规时,将所述识别结果发送至监管方的步骤,包括:

根据所述被盗风险账号获取关联信息;

将所述被盗风险账号和所述关联信息发送至所述监管方。

3.根据权利要求2所述的一种基于区块链的区域医疗处方监管方法,其特征在于,所述通过先聚类再分类的方式识别所述数据湖中各数据,以识别出被盗风险账号的步骤,包括:

通过Kmeans算法和粒子群算法中至少一者对所述数据湖内各数据进行聚类获得聚类中心;

通过Kmeans算法对所述聚类中心进行再次处理;

通过朴素贝叶斯算法、决策树算法和随机森林算法中至少一者对经过再次处理的所述聚类中心进行分类,以识别出为所述被盗风险账号。

4.根据权利要求1所述的一种基于区块链的区域医疗处方监管方法,其特征在于,所述当所述识别结果为违规时,将所述识别结果发送至监管方的步骤,包括:

当所述客户账号为恶意账号时,获取所述恶意账号对应的所述账号特征,分别将所述账号特征和所述恶意账号发送至监管方;

所述当所述识别结果为不违规时,向监管方发送数据正常的信息提示的步骤,包括:

当所述客户账号为不是恶意账号时,向监管方发送数据正常的信息提示。

5.根据权利要求1所述的一种基于区块链的区域医疗处方监管方法,其特征在于,所述

计算模型为隐马尔可夫模型。

6.根据权利要求1所述的一种基于区块链的区域医疗处方监管方法,其特征在于,所述对数据湖中各数据进行风险识别,并判断识别结果是否违规的步骤,还包括:

通过BoostFS算法对所述数据湖内各数据进行行为特征选择分析,以识别出为恶意程序,并对恶意程序进行动静态检测;

当发现为恶意程序时,判定识别结果为违规。

7.根据权利要求1所述的一种基于区块链的区域医疗处方监管方法,其特征在于,所述对数据湖中各数据进行风险识别,并判断识别结果是否违规的步骤,还包括:

通过降低错分类代价的代价敏感学习算法对所述数据湖内的各数据进行预设处理,对运行程序进行恶意评估,以判断运行程序是否为恶意程序。

8.根据权利要求1所述的一种基于区块链的区域医疗处方监管方法,其特征在于,所述当所述识别结果违规时,将所述识别结果发送至监管方的步骤之后,还包括:

获取监管方是否确定所述识别结果为违规行为;

当监管方确定所述识别结果为违规行为时,将所述识别结果关联的所述客户账号标注为违规账号;

当监管方对确定所述识别结果为非违规行为时,向所述识别结果关联的所述客户账号发送风险提示;

所述客户就医信息包括院方文本信息和院方非文本信息:所述客户操作信息包括登录信息、页面操作信息、登录相关信息、日志信息和户端的静态基本信息。

9.一种基于区块链的区域医疗处方监管系统系统,其特征在于,所述监管系统应用于上述权利要求1-8任一所述的一种基于区块链的区域医疗处方监管方法,所述监管系统包括:

云服务器,所述服务器用于获取客户账号,并根据所述客户账号获取客户个人信息和客户操作信息;根据客户个人信息从院方获取客户就医信息;

大数据中心,所述大数据中心用于将所述客户账号、所述客户个人信息、所述客户就医信息和所述客户操作信息均输入大数据中心形成数据湖;

处理模块,所述处理模块用于对数据湖中各数据进行风险识别,并判断识别结果是否违规;当所述识别结果违规时,将所述识别结果发送至监管方;当所述识别结果不违规时,向监管方发送数据正常的信息提示。

一种基于区块链的区域医疗处方监管方法及系统

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种基于区块链的区域医疗处方监管方法及系统。

背景技术

[0002] 随着信息技术的发展，医院的信息化建设也逐渐普及开来。目前，每一家医院基本都拥有自己的信息系统，通常包括若干的数据采集终端，用于采集用药数据、病历数据、治疗费用数据等医疗数据并存储在医院的数据库中。

[0003] 对于监管部门来讲，获取足够多的医疗数据能对医疗机构进行有效监管，是判断就诊人和院方的行为是否为合理行为，以及是否符合相关规定提供的重要依据。目前虽然也出现了一些相关服务系统，通过将各医院信息系统的业务数据按照相监管部门的要求对数据进行整合传输，供监管部门进行审查，但是，目前的系统主要是对所有医疗数据进行存储和传输，没有进一步对数据进行风险识别，不能向监管部门提供用于辅助识别违规信息的辅助意见，导致监管部门无法通过相关系统获取对应的技术支撑。

发明内容

[0004] 本发明的主要目的在于提供一种基于区块链的区域医疗处方监管方法及系统，旨在解决现有系统无法对医疗信息系统的数据进行进一步的风险识别，无法为起到辅助相关部门对医院和用户进行监督的目的。

[0005] 为实现上述目的，本发明提供的一种基于区块链的区域医疗处方监管方法，包括：

[0006] 获取客户账号，并根据所述客户账号获取客户个人信息和客户操作信息；

[0007] 根据客户个人信息从院方获取客户就医信息；

[0008] 将所述客户账号、所述客户个人信息、所述客户就医信息和所述客户操作信息均输入大数据中心形成数据湖；

[0009] 对数据湖中各数据进行风险识别，并判断识别结果是否违规；

[0010] 当所述识别结果为违规时，将所述识别结果发送至监管方；

[0011] 当所述识别结果为不违规时，向监管方发送数据正常的信息提示。

[0012] 优选的，所述对数据湖中各数据进行风险识别，并判断识别结果是否违规的步骤，包括：

[0013] 通过先聚类再分类的方式识别所述数据湖中各数据，以识别出被盗风险账号；

[0014] 当识别出为所述被盗风险账号时，判定识别结果为违规；

[0015] 所述当所述识别结果为违规时，将所述识别结果发送至监管方的步骤，包括：

[0016] 根据所述被盗风险账号获取关联信息；

[0017] 将所述被盗风险账号和所述关联信息发送至所述监管方。

[0018] 优选的，所述通过先聚类再分类的方式识别所述数据湖中各数据，以识别出被盗风险账号的步骤，包括：

[0019] 通过Kmeans算法和粒子群算法中至少一者对所述数据湖内各数据进行聚类获得聚类中心；

[0020] 通过Kmeans算法对所述聚类中心进行再次处理；

[0021] 通过朴素贝叶斯算法、决策树算法和随机森林算法中至少一者对经过再次处理的所述聚类中心进行分类，以识别出为所述被盗风险账号。

[0022] 优选的，所述对数据湖中各数据进行风险识别，并判断识别结果是否违规的步骤，还包括：

[0023] 构建计算模型；

[0024] 根据所述数据湖内的各数据通过所述计算模型，获取账号特征；

[0025] 通过模拟退火算法对所述账号特征进行处理，分别获取隐含状态变量和观测变量；

[0026] 通过维特比算法分别对所述隐含状态变量和所述观测变量进行处理，获取客户账号的隐含状态；

[0027] 根据所述隐含状态判断该所述客户账号是否为恶意账号。

[0028] 优选的，所述当所述识别为结果违规时，将所述识别结果发送至监管方的步骤，包括：

[0029] 当所述客户账号为恶意账号时，获取所述恶意账号对应的所述账号特征，分别将所述账号特征和所述恶意账号发送至监管方；

[0030] 所述当所述识别结果为不违规时，向监管方发送数据正常的信息提示的步骤，包括：

[0031] 当所述客户账号为不是恶意账号时，向监管方发送数据正常的信息提示。

[0032] 优选的，所述计算模型为隐马尔可夫模型。

[0033] 优选的，所述对数据湖中各数据进行风险识别，并判断识别结果是否违规的步骤，还包括：

[0034] 通过BoostFS算法对所述数据湖内各数据进行行为特征选择分析，以识别出为恶意程序，并对恶意程序进行动静态检测；

[0035] 当发现为恶意程序时，判定识别结果为违规。

[0036] 优选的，所述对数据湖中各数据进行风险识别，并判断识别结果是否违规的步骤，还包括：

[0037] 通过降低错分类代价的代价敏感学习算法对所述数据湖内的各数据进行预设处理，对运行程序进行恶意评估，以判断运行程序是否为恶意程序。

[0038] 优选的，所述当所述识别结果违规时，将所述识别结果发送至监管方的步骤之后，还包括：

[0039] 获取监管方是否确定所述识别结果为违规行为；

[0040] 当监管方确定所述识别结果为违规行为时，将所述识别结果关联的所述客户账号标注为违规账号；

[0041] 当监管方对确定所述识别结果为非违规行为时，向所述识别结果关联的所述客户账号发送风险提示；

[0042] 所述客户就医信息包括院方文本信息和院方非文本信息:所述客户操作信息包括

登录信息、页面操作信息、登录相关信息、日志信息和户端的静态基本信息。

[0043] 此外，为实现上述目的，本发明还提供一种基于区块链的区域医疗处方监管系统，所述监管系统应用于上述任一所述的一种基于区块链的区域医疗处方监管方法，所述监管系统包括：

[0044] 云服务器，所述服务器用于获取客户账号，并根据所述客户账号获取客户个人信息和客户操作信息；根据客户个人信息从院方获取客户就医信息；

[0045] 大数据中心，所述大数据中心用于将所述客户账号、所述客户个人信息、所述客户就医信息和所述客户操作信息均输入大数据中心形成数据湖；

[0046] 处理模块，所述处理模块用于对数据湖中各数据进行风险识别，并判断识别结果是否违规；当所述识别结果违规时，将所述识别结果发送至监管方；当所述识别结果不违规时，向监管方发送数据正常的信息提示。

[0047] 通过大数据中心整合所有数据，并对所有数据进行识别，以识别出违规的数据，并将识别结果发送至监管方，以供监管方进行检测和确认，这样极大的降低了监管方的工作难度，有效的提高了监管方的工作效率。

附图说明

[0048] 图1为本发明一种基于区块链的区域医疗处方监管方法的流程示意图；

[0049] 图2为本发明一种基于区块链的区域医疗处方监管系统的功能模块示意图。

[0050] 本发明目的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0051] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0052] 在后续的描述中，使用用于表示元件的诸如“模块”、“部件”或“单元”的后缀仅为了有利于本发明的说明，其本身没有特定的意义。因此，“模块”、“部件”或“单元”可以混合地使用。

[0053] 请参阅图1，为实现上述目的，本发明的第一实施例中提供一种基于区块链的区域医疗处方监管方法，包括：

[0054] 步骤S10，获取客户账号，并根据客户账号获取客户个人信息和客户操作信息；

[0055] 步骤S20，根据客户个人信息从院方获取客户就医信息；

[0056] 步骤S30，将客户账号、客户个人信息、客户就医信息和客户操作信息均输入大数据中心形成数据湖；

[0057] 步骤S40，对数据湖中各数据进行风险识别，并判断识别结果是否违规；

[0058] 步骤S50，当识别结果为违规时，将识别结果发送至监管方；

[0059] 步骤S60，当识别结果为不违规时，向监管方发送数据正常的信息提示。

[0060] 通过大数据中心整合所有数据，并对所有数据进行识别，以识别出违规的数据，并将识别结果发送至监管方，以供监管方进行检测和确认，这样极大的降低了监管方的工作难度，有效的提高了监管方的工作效率。

[0061] 大数据中心会对数据进行采集和预处理，通过大数据中心聚合化、标准化、结构化、归一化数据，为智能监管业务等中台提供数据支持。

[0062] 大数据中心的分析加工功能基于数据湖中数据进行处理，基本处理功能包括：数据整合，将从各个业务系统获取的医疗数以患者主索引EMPI为中心进行整合，实现数据综合利用；数据自动化处理，处理过程可以实现自动处理，避免人工实时干预；数据安全性，数据处理过程要保证数据安全性，做到数据保密性、数据完整性、数据可利用等。

[0063] 具体的，客户就医信息包括院方文本信息和院方非文本信息，文本信息即为诊断结果、处方信息、审核结果、拿药结果和支付信息，非文本信息为患者诊断过程中产生的医疗图像、音频和视频；客户操作信息包括登录信息、页面操作信息、登录相关信息、日志信息和户端的静态基本信息，静态基本信息包括当前用户浏览器的类型、UserAgent、用户的IP地址、cookie信息、浏览器的插件信息和http请求头等内容。

[0064] 具体的，客户就医信息通过医院信息系统、实验室信息管理系统、电子病历和护理系统中分别获取，文本数据进行上链输入至星际文件系统中；而非文本数据存入星际文件系统之后进行hash运算把运算结果上链输入至区块链中；获取客户就医信息时，通过客户个人信息获取监管方和院方的确认，再对区块链中非文本数据和星际文件系统中文本数据经过同态加密和联邦学习算法输入大数据中心形成数据湖。

[0065] 在本发明提出的一种基于区块链的区域医疗处方监管方法的第二实施例中，基于第一实施例，步骤S40，包括：

[0066] 步骤S41，通过先聚类再分类的方式识别数据湖中各数据，以识别出被盗风险账号；

[0067] 步骤S42，当识别出为被盗风险账号时，判定识别结果为违规；

[0068] 步骤S50，包括：

[0069] 步骤S51，根据被盗风险账号获取关联信息；

[0070] 步骤S52，将被盗风险账号和关联信息发送至监管方。

[0071] 通过聚类分类的方式，将符合被盗风险账号特征的客户账号整理并识别出，打包成完整的数据包供监管方进行侦查，这样可以避免骗保，并追责至相应的院方、医师和售药处，辅助监管方对整个系统中的违规方做出线上预警、监管稽核和违规判罚。

[0072] 在本发明提出的一种基于区块链的区域医疗处方监管方法的第三实施例中，基于第二实施例，步骤S41，包括：

[0073] 步骤S43，通过Kmeans算法和粒子群算法中至少一者对数据湖内各数据进行聚类获得聚类中心；

[0074] 步骤S44，通过Kmeans算法对聚类中心进行再次处理；

[0075] 步骤S45，通过朴素贝叶斯算法、决策树算法和随机森林算法中至少一者对经过再次处理的聚类中心进行分类，以识别出为被盗风险账号。

[0076] 具体的，Kmeans算法和粒子群算法结合对数据湖内各数据进行聚类获得聚类中心，这样再结合Kmeans算法对聚类中心再处理，可以有效的提高数据的准确性。

[0077] 具体的，朴素贝叶斯算法、决策树算法和随机森林算法分别对经过再次处理的聚类中心进行分类，通过分别对各分类结果比对，可以更加准确的识别出被盗风险账号

[0078] 在本发明提出的一种基于区块链的区域医疗处方监管方法的第四实施例中，基于第一实施例，步骤S40，还包括：

[0079] 步骤S46，构建计算模型；

[0080] 步骤S47,根据数据湖内的各数据通过计算模型,获取账号特征;

[0081] 步骤S48,通过模拟退火算法对账号特征进行处理,分别获取隐含状态变量和观测变量;

[0082] 步骤S49,通过维特比算法分别对隐含状态变量和观测变量进行处理,获取客户账号的隐含状态;

[0083] 步骤S410,根据隐含状态判断该客户账号是否为恶意账号。

[0084] 具体的,账号特征为客户账号多个非违规操作组合成的可以操作,例如客户账号提交了医保保险,正在等待保险款的汇入,这时客户账号提交销毁账号,这样明显不合理的多个操作可分别认定为账号特征,判断为恶意账号。

[0085] 在本发明提出的一种基于区块链的区域医疗处方监管方法的第五实施例中,基于第四实施例,步骤S50,包括:

[0086] 步骤S53,当客户账号为恶意账号时,获取恶意账号对应的账号特征,分别将账号特征和恶意账号发送至监管方;

[0087] 步骤60,包括

[0088] 步骤S61,当客户账号不是为恶意账号时,向监管方发送数据正常的信息提示。

[0089] 在本发明提出的一种基于区块链的区域医疗处方监管方法的第六实施例中,基于第四实施例,计算模型为隐马尔可夫模型。

[0090] 在本发明提出的一种基于区块链的区域医疗处方监管方法的第七实施例中,基于第一实施例,步骤S40,还包括:

[0091] 步骤S411,通过BoostFS算法对数据湖内各数据进行行为特征选择分析,以识别出恶意程序,并对恶意程序进行动静态检测;

[0092] 步骤S412,当发现恶意程序时,判定识别结果为违规。

[0093] 具体的,行为特征为直接认定违规的操作,一般为利用漏斗攻击系统,或者恶意的在短时间内多些电击和刷新等一些损害系统的操作。

[0094] 在本发明提出的一种基于区块链的区域医疗处方监管方法的第八实施例中,基于第一实施例,步骤S40,包括:

[0095] 通过降低错分类代价的代价敏感学习算法对数据湖内的各数据进行预设处理,对运行程序进行恶意评估,以判断运行程序是否为恶意程序。

[0096] 通过代价敏感学习算法识别基于数据湖对整个系统进行监控,对未知程序进行预测性监控,对预测有恶意形成的未知程序的进行监管和重点监控。

[0097] 在本发明提出的一种基于区块链的区域医疗处方监管方法的第八实施例中步骤S60之后,还包括:

[0098] 步骤S70,获取监管方是否确定识别结果为违规行为;

[0099] 步骤S80,当监管方确定识别结果为违规行为时,将识别结果关联的客户账号标注为违规账号;

[0100] 步骤S90,当监管方对确定识别结果为非违规行为时,向识别结果关联的客户账号发送风险提示。

[0101] 客户账号标注为违规账号后,会限制其一些操作权限,这样可以避免违规账号继续进行非法操作;风险提示是提示客户要注意一些操作,避免正常的客户账号在不知情的

继续进行有风险的操作。

[0102] 具体的，步骤S80之后，还包括：

[0103] 将各违规账号汇总为账号表，并在预设时间点将账号表包发送至监管方进行更新；

[0104] 获取更新后的账号表对现有的各违规账号从新标注。

[0105] 请参阅图2，一种基于区块链的区域医疗处方监管系统，监管系统应用于上述任一的一种基于区块链的区域医疗处方监管方法，监管系统包括：

[0106] 云服务器，服务器用于获取客户账号，并根据客户账号获取客户个人信息和客户操作信息；根据客户个人信息从院方获取客户就医信息；

[0107] 大数据中心，大数据中心用于将客户账号、客户个人信息、客户就医信息和客户操作信息均输入大数据中心形成数据湖；

[0108] 处理模块，处理模块用于对数据湖中各数据进行风险识别，并判断识别结果是否违规；当识别结果违规时，将识别结果发送至监管方；当识别结果不违规时，向监管方发送数据正常的信息提示。

[0109] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件系统的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个计算机可读存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备进入本发明各个实施例所述的方法。

[0110] 在本说明书的描述中，参考术语“一实施例”、“另一实施例”、“其他实施例”、或“第一实施例~第X实施例”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发明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一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料、方法步骤或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0111] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0112] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0113] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

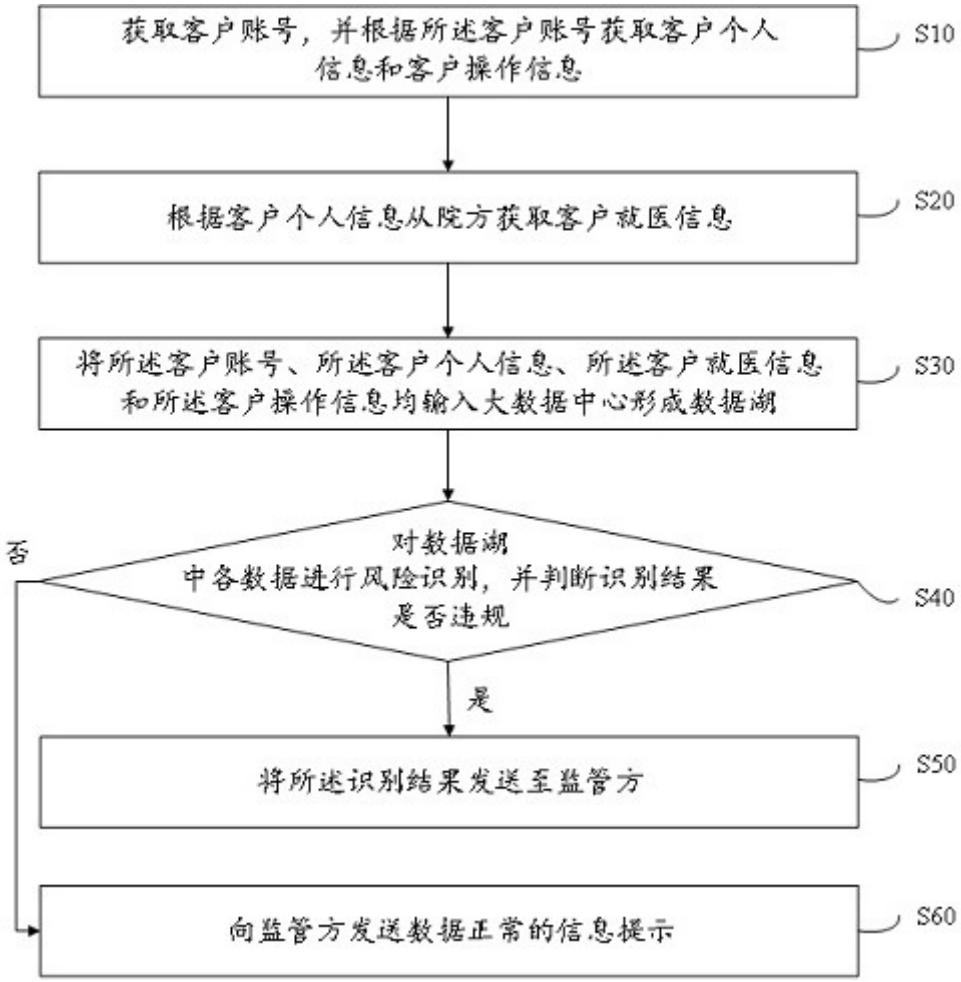

获取客户账号，并根据所述客户账号获取客户个人信息和客户操作信息
S10
根据客户个人信息从院方获取客户就医信息
S20
将所述客户账号、所述客户个人信息、所述客户就医信息和所述客户操作信息均输入大数据中心形成数据湖
S30
对数据湖中各数据进行风险识别，并判断识别结果是否违规
S40
否
是
将所述识别结果发送至监管方
S50
向监管方发送数据正常的信息提示
S60

图1


云服务器
大数据中心
处理模块

图2