(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111863168 A
(43)申请公布日 2020.10.30

(21)申请号 202010666884.X

(22)申请日 2020.07.10

(66)本国优先权数据
201910626876.X 2019.07.11 CN

(71)申请人 中国医学科学院阜外医院
地址 100037 北京市西城区北礼士路167号

(72)发明人 唐熠达 邵春丽 刘勇 苏中谦
汪京嘉 田间 程宇镳

(51)Int.Cl.
G16H 10/60(2018.01)
G16H 80/00(2018.01)
G06F 16/27(2019.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)
H04L 9/00(2006.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)

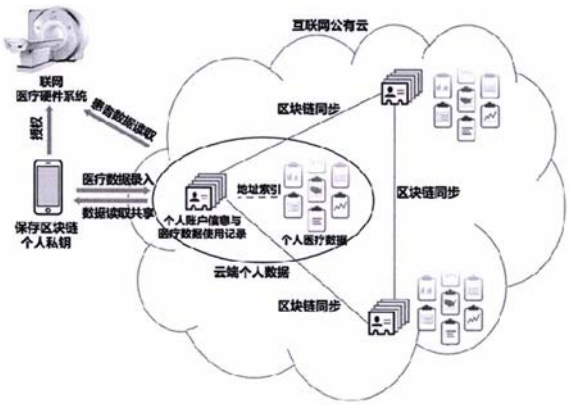
权利要求书2页 说明书11页 附图1页

(54)发明名称

一种具有交换协议的硬件系统

(57)摘要

本发明属于医疗领域，具体提供了具有交换协议的硬件系统，包含数据收集、存储和运算的硬件系统，在病人知情同意或主动提交的前提下，将病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况录入具有交换协议的硬件系统中，可以直接互相推送医患信息。通过本发明的实施，打破医疗机构间信息不互通的壁垒，为患者和医疗机构提供了一个可自行管理医疗流程的工具。



CN 111863168 A

1.一种具有交换协议的硬件系统，包含数据收集、存储和运算的硬件系统，其特征在于：在病人知情同意或主动提交的前提下，将病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况录入硬件系统中，其中病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况的录入或调用采用加密和/或解密方式。

2.根据权利要求1所述的硬件系统，其特征在于：所述硬件系统与可穿戴设备按照协议接口进行的信息录入和/或输出；所述可穿戴设备选自耳机、音箱、手环或手机中的一种或多种。

3.根据权利要求1所述的硬件系统，其特征在于：所述硬件系统可以录入病人的纸质病历、诊断报告，医生的语音诊断或医学影像中的一种或多种。

4.根据权利要求3所述的硬件系统，其特征在于：所述纸质病历、诊断报告或医学影像可以进行识别或识别后存储。

5.根据权利要求1-4任一所述的硬件系统，其特征在于：所述的病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况和/或新冠肺炎感染状况可以分级向首诊医生和/或急诊医生推送。

6.根据权利要求1-4任一所述的硬件系统，其特征在于：所述的病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况在重症急诊时直接向首诊医生和/或急诊医生推送。

7.根据权利要求1-4任一所述的硬件系统，其特征在于：所述的病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况在重症急诊时直接向首诊医生和/或急诊医生推送，上述操作可以由病人先行设置。

8.根据权利要求1-7任一所述的硬件系统，其特征在于：所述的硬件系统可以将医生的诊疗方案、给药处方或病历记录与病人的诊断报告或既往病史的临床禁忌进行比对或运算；如有错误或存疑，则不设分级地反馈给医生。

9.根据权利要求1-7任一所述的硬件系统，其特征在于：所述的硬件系统可以将病人对于诊疗重要程度向医生披露。

10.根据权利要求1-7任一所述的硬件系统，其特征在于：可以在用户确认授权前提下，向病人或监护人推送用患者教育信息、用药频次、用药处方、运动处方、就诊提醒、复查提醒或医嘱信息中的一种或多种。

11.根据权利要求10所述的硬件系统，其特征在于：所述硬件系统可以按照设定程序自行运算。

12.根据权利要求10所述的硬件系统，其特征在于：所述的自行运算的结果可以向医生推送。

13.根据权利要求10所述的硬件系统，其特征在于：所述的自行运算的结果可以向病人推送。

14.根据权利要求1-13任一所述的硬件系统，其特征在于：所述的自行运算的结果可以通过近距离通讯技术，向周边支持同样协议的其他医疗器械硬件推送，实现医疗器械之间的患者数据自动共享，以及潜在的器械使用风险提示。

15.根据权利要求1-13任一所述的硬件系统，其特征在于：所述的病人为高危病人或所

述病人年龄超过65岁。

一种具有交换协议的硬件系统

技术领域：

[0001] 本发明属于医学治疗领域，具体本发明提供了一种打破医疗机构间信息不互通的壁垒，实现大数据共享平台系统，对病患监控提供可靠的支持。

背景技术：

[0002] 基于AI的大数据管理在各行业广泛应用，但由于医疗行业的特殊性，涉及专业、精准、个人隐私的保护等限制，很难做到大数据的收集和共享，目前的现状是各医院的电子病历系统均为封闭系统，很难做到具有交换协议的硬件系统内信息互联，更不可能与医疗体系外的平台对接。因此大数据的收集几乎成为不可能。

[0003] 虽然保护了医疗信息的隐私安全性，但对整体国民疾病现状的研究只能基于有针对性的队列研究，而且每个研究需要耗费大量人力物力财力的资源和时间成本，往往研究结果存在着滞后性。

[0004] 而且很多研究的人群在不同疾病中重复信息收集，极大浪费科研资源；因为缺乏整体疾病的大数据管理，难以国家的医疗战略提供强有力的支撑依据。

[0005] 如何既能保证医疗信息的准确可靠又保护患者隐私，并且能够打破医疗机构间信息不互通的壁垒，实现大数据共享平台，对国家医疗策略提供可靠的依据。这一问题尚无没有完美的解决方案。

发明内容：

[0006] 本发明的目的在于提供一种具有交换协议的硬件系统，包含数据收集、存储和运算的硬件系统，所述的硬件系统在病人知情同意或主动提交的前提下，将病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况录入硬件系统中，其中病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况的录入或调用采用加密和/或解密方式。

[0007] 上述的硬件系统，所述的病人的的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况，尤其特别强调是微生物感染状况以及新冠肺炎感染状况，其中的来源也可以是操作系统、社交媒体、打车软件、游戏软件、共享家居软件、导航软件、旅行推送软件、视频软件或支付系统，尤其包括IOS、安卓、优酷、爱奇艺、youtube、Airbnb、微博、去哪儿、携程、快手、抖音、百度地图、高德地图、谷歌地图、腾讯地图、头条、脸书、推特、微信、支付宝等。

[0008] 上述的硬件系统，硬件系统与可穿戴设备按照协议接口进行的信息录入和/或输出；所述可穿戴设备选自耳机、音箱、手环或手机中的一种或多种。

[0009] 上述的硬件系统，其特征在于所述硬件系统可以录入病人的纸质病历、诊断报告，医生的语音诊断或医学影像中的一种或多种。

[0010] 上述的硬件系统，其特征在于所述纸质病历、诊断报告或医学影像可以进行识别或识别后存储。

[0011] 上述的硬件系统，其特征在于所述的病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况可以分级向首诊医生和/或急诊医生推送。

[0012] 上述的硬件系统，其特征在于所述的病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况在重症急诊时直接向首诊医生和/或急诊医生推送。

[0013] 上述的硬件系统，其特征在于所述的病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况在重症急诊时直接向首诊医生和/或急诊医生推送，上述操作可以由病人先行设置。

[0014] 上述的硬件系统，其特征在于所述的硬件系统可以将医生的诊疗方案、给药处方或病历记录与病人的诊断报告或既往病史的临床禁忌进行比对或运算；如有错误或存疑，则不设分级地反馈给医生。

[0015] 上述的硬件系统，其特征在于所述的硬件系统可以将病人对于诊疗重要程度向医生披露。

[0016] 上述的硬件系统，其特征在于可以在用户确认授权前提下，向病人或监护人推送用患者教育信息、用药频次、用药处方、运动处方、就诊提醒、复查提醒或医嘱信息中的一种或多种。

[0017] 上述的硬件系统，其特征在于所述硬件系统可以按照设定程序自行运算。

[0018] 上述的硬件系统，其特征在于所述的自行运算的结果可以向医生推送。

[0019] 上述的硬件系统，其特征在于所述的自行运算的结果可以向病人推送。

[0020] 上述的硬件系统，其特征在于所述的病人为高危病人。

[0021] 上述的硬件系统，其特征在于所述的病人年龄超过65岁。

[0022] 上述的硬件系统，可以采用以下方法实现：

[0023] (1)将个人医疗数据，用个人密钥加密，并存储在可以在公网寻址的分布式存储空间，并以个人医疗数据的哈希值作为空间内数据的索引key值；

[0024] (2)在区块链上的加密个人账户信息中，记录个人医疗数据的公网存储地址与数据的哈希值；

[0025] (3)当联网的医疗硬件系统需要访问个人医疗数据时，可以通过区块链的智能合约向病患发出数据访问请求，病患确认授权后，会将准许访问的个人医疗数据的哈希值与公网访问地址作为智能合约的一部分，让第三方获取；

[0026] (4)联网的医疗硬件系统通过智能合约获取用户个人医疗数据的公网存储地址与哈希值，并使用哈希值在存储空间内作为索引key值获取加密的医疗数据，然后可以通过哈希值对比验证其正确性。

[0027] (5)联网的医疗硬件系统通过同态加密算法，对获取的加密个人医疗数据进行运算，获取运算结果。

[0028] 上述的医疗系统，可以采用以下方法实现：

[0029] (1)个人医疗数据通过用户存储在可穿戴设备的私用密钥进行加密，存储在互联网上；

[0030] (2)个人医疗互联网索引数据，通过用户存储在可穿戴设备或者手机上的私用密钥进行加密，存储在区块链上；

[0031] (3)个人医疗数据有联网的医疗硬件系统读取请求时，用户用自己存储在可穿戴

设备或者手机上的私用密钥对硬件系统读取请求进行确认,然后对个人医疗数据进行解密;

[0032] (4)解密的个人医疗数据用密码散列函数SHA产生摘要;

[0033] (5)用户用自己存储在可穿戴设备或者手机上的私用密钥对摘要再加密,形成数字签名;

[0034] (6)将解密的个人医疗数据和加密的摘要同时发送给读取请求硬件;

[0035] (7)读取请求硬件使用用户存储在公有区块链上的公共密钥对发送来的摘要解密,获取用户端对个人医疗数据生成的摘要,同时对收到的个人医疗数据用SHA编码加密产生又一摘要;如两者一致,则说明传送过程中信息没有被破坏或篡改过;

[0036] (8)用户将此次个人医疗数据的硬件读取请求信息,同步到区块链上。

[0037] 上述的医疗系统,可以采用以下方法实现:

[0038] (1)联网的医疗数据智能分析硬件系统发起分析请求,分成两部分信息进入智能合约,第一部分包含控制参数,另一部分描述计算分析任务;

[0039] (2)来自智能合约的分析请求信息,通过一个编译通道,结合控制参数,编译成可以直接分析加密个人医疗数据的基础计算指令集;

[0040] (3)基础计算指令集发送到用户,获得授权后,将用户的加密个人医疗数据通过基础计算指令集进行计算;

[0041] (4)计算过程中个人医疗数据一致保持加密状态,确保个人数据的保密性;

[0042] (5)计算结果通过用户的私钥进行解密,并发送回联网的医疗数据智能分析硬件系统;用户将此次个人医疗数据的分析请求信息,同步到区块链上作为不可篡改的历史记录。

[0043] 上述的硬件系统,所述的同态加密算法,满足以下条件:

[0044] (1)Enc(PK,m)加密函数以区块链上的用户加密数据公钥PK和消息m作为输入,输出加密个人医疗数据c;

[0045] (2)Dec(SK,c)解密函数以用户私钥和加密个人医疗数据c作为输入,输出消息m;

[0046] (3)Eval(PK,f,c1,…,cl)评估函数以区块链上的用户加密数据公钥、分析算法f以及加密个人医疗数据c1到cl,输出加密的数据cf;

[0047] (4)当c1＝Enc(PK,m1),…,cl＝Enc(PK,ml)Mf＝f(m1,…,ml);

[0048] (5)Cf＝Eval(PK,f,c1,…,cl);

[0049] (6)满足对于任何分析算法f,mf＝Dec(SK,cf)。

[0050] 上述的硬件系统,所述大量病人数据,在病人授权情况下,建立大样本的疾病队列,通过定向分析或人工智能算法,完成相关科研领域的研究。

[0051] 通过本发明的实施,可以实现以下优势:

[0052] 1、纳入65岁以上以及高危人群人群,建立患者的基本健康档案。

[0053] 2、上传历次就诊的医疗记录,系统协助归类整理,使患者有一套时间轴完整,分类清晰,内容丰富的电子病历。首次通过目前新兴的区块链技术运用于个人医疗管理数据和隐私保护。

[0054] 3、可外挂可穿戴设备,实时上传患者日常监测的医疗数据记录,实现异常监测报警。

[0055] 4、完整医疗数据整合，为患者就诊提供便利。患者可自行决定向接诊医生出示自己的健康档案记录，便于医生迅速了解患者病情，给予及时准确的救治。

[0056] 5、根据患者病情，提供个体化提醒功能，包括服药提醒，就诊提醒，复查提醒等。

[0057] 6、建立专病社区，定期推送相关权威的医疗相关的患者教育信息，利于疾病防控。

[0058] 7、基于大量患者数据，在患者授权情况下，建立大样本的疾病队列，通过定向分析或人工智能算法，完成相关科研领域的研究，为国家医疗战略提供科学依据。

[0059] 本发明系统主要需要解决的技术问题包括：解决医患之间的信息不对称；还要解决当前医护人员与既往医护人员的信息、判断和记录的信息不对称。把诊疗的准确性依据大数据的判断，而不是单个医生的能力上，是医疗模式的重大革新。

[0060] 本发明基于区块链技术的去中心化分布式数据加密存储方法，利用了区块链技术分布式账本的技术优势，记录个人账户信息与医疗数据的使用记录，确保这些记录不可篡改，同时链上保存分布存储的加密的个人医疗数据的索引地址，满足了存储大数据量加密个人医疗数据的实际需求，实现了个人可控权限下的个人医疗数据共享，以及为基于同态加密技术的数据统计分析提供了基础平台。

[0061] 但是电子货币的区块链只保存账户与交易信息，数据量很小，很容易实现分布式存储与同步，但不适合保存数据量很大的个人医疗数据，所以还没有完全类似的基于区块链技术的分布式存储大数据量数据的方案，以及基于这些数据进行整体统计分析的方案。

[0062] 目前，单系统甚至云端数据库都是高度中心化的，这使它们很容易沦为黑客的攻击目标，也有可能人为地发生泄密，而且及易受到影响(比如断电)，不是保证用户个人医疗数据存储隐私性和自我可控性的合理技术方案。相比之下，基于区块链的分布式加密存储不会遇到这些问题，因为它利用了异地分布的区域性或全球性节点。

[0063] 假若单点受到攻击或是出现断电，不会造成灾难性影响，因为其他地方的节点会继续发挥作用。同时，区块链的分布式账本，也确保了所有个人医疗数据的使用记录，相比与中心化的存储方案，是不容易被篡改的。

[0064] 通过本发明的实施，加快了医患之间信息交换速度，为病情的准确诊断，快速施治，减少医患纠纷和摩擦，提供了有效途径；是医疗模式在生理和心理两面的整合改善。

附图说明

[0065] 图1本发明系统运行示意图

[0066] 图2本发明系统同态加密运行示意图

具体实施方式

[0067] 本发明的实验例证是为了说明本发明而不是限制本发明。

[0068] 本发明具体提供了具有交换协议的硬件系统，包含数据收集、存储和运算的硬件系统，在病人知情同意或主动提交的前提下，将病人的账户信息和/或个人医疗数据和/或微生物感染状况和/或新冠肺炎感染状况录入具有交换协议的硬件系统中，可以直接互相推送医患信息。通过本发明的实施，打破医疗机构间信息不互通的壁垒，为患者和医疗机构提供了一个可自行管理医疗流程的工具。

[0069] 引入同态加密技术，分析加密分布式存储的用户个人医疗数据，解决了第三方进

行大数据科研分析过程中的个人数据隐私问题。

[0070] 实施例1

[0071] 将区块链技术与数据分布式存储技术结合，满足普通人群疫情调研数据的去中心化加密存储、可控共享、使用记录不可篡改的需求。

[0072] 普通人群的医疗数据的数据存储量非常大，不适合放在区块链上进行全链同步，因此需要进行分布式加密存储，并在区块链上的个人账户信息中记录存储的地址索引，实现链上链下同步的加密个人医疗数据存储。主要实现步骤为：

[0073] (1)将普通人群疫情调研数据，用个人密钥加密，并存储在可以在公网寻址的分布式存储空间，并以个人医疗数据的哈希值作为空间内数据的索引key值；

[0074] (2)在区块链上的加密个人账户信息中，记录普通人群疫情调研数据的公网存储地址与数据的哈希值；

[0075] (3)当其他第三方需要访问普通人群疫情调研数据时，可以通过区块链的智能合约向病患发出数据访问请求，病患确认授权后，会将准许访问的个人医疗数据的哈希值与公网访问地址作为智能合约的一部分，让第三方获取；

[0076] (4)第三方通过智能合约获取用户普通人群疫情调研数据的公网存储地址与哈希值，并使用哈希值在存储空间内作为索引key值获取加密的医疗数据，然后可以通过哈希值对比验证其正确性。

[0077] (5)第三方通过同态加密算法，对获取的加密个人医疗数据进行运算，获取运算结果。

[0078] 引入同态加密技术，分析加密分布式存储的用户普通人群疫情调研数据，解决了新冠肺炎的烈性传染和流调监控问题。

[0079] 实施例2

[0080] 上述的硬件系统，所述硬件系统的个人账户信息与加密的个人医疗数据互联网地址索引，必须通过用户手机内的私有密钥认证，才能进行读取、管理与分享，每次读取与分享记录，都会记录到个人医疗数据使用记录里面，并在全网的所有区块链上不同用户节点上进行同步；以下为个人医疗数据读取的加密与解密步骤：

[0081] (1)普通人群疫情调研数据通过用户存储在可穿戴设备的私用密钥进行加密，存储在互联网上；

[0082] (2)个人医疗互联网索引数据，通过用户存储在可穿戴设备或者手机上的私用密钥进行加密，存储在区块链上；

[0083] (3)普通人群疫情调研数据有读取请求时，用户用自己存储在可穿戴设备或者手机上的私用密钥对个人医疗数据进行解密；

[0084] (4)解密的普通人群疫情调研数据用密码散列函数SHA产生摘要；

[0085] (5)用户用自己存储在可穿戴设备或者手机上的私用密钥对摘要再加密，形成数字签名；

[0086] (6)将解密的普通人群疫情调研数据和加密的摘要同时发送给读取请求方；

[0087] (7)读取请求方使用用户存储在公有区块链上的公共密钥对发送来的摘要解密，获取用户端对个人医疗数据生成的摘要，同时对收到的个人医疗数据用SHA编码加密产生又一摘要；如两者一致，则说明传送过程中信息没有被破坏或篡改过；

[0088] (8)用户将此次普通人群疫情调研数据的读取请求信息,同步到区块链上。

[0089] 实施例3

[0090] 上述的硬件系统,医疗机构可以通过区块链,向普通人群发送个人疫情征信的请求,个人确认授权后,用同态加密的分析算法发送到用户的个人医疗数据上,对加密的个人医疗数据进行加密状态下的运算,整个运算过程个人医疗数据仍旧保持加密状态;以下为基于同态加密算法的分析步骤:

[0091] (1)医疗机构方发起分析请求,分成两部分信息进入智能合约,第一部分包含控制参数,另一部分描述计算分析任务;

[0092] (2)来自智能合约的分析请求信息,通过一个编译通道,结合控制参数,编译成可以直接分析加密个人医疗数据的基础计算指令集;

[0093] (3)基础计算指令集发送到用户,获得授权后,将用户的加密个人医疗数据通过基础计算指令集进行计算;

[0094] (4)计算过程中个人医疗数据一致保持加密状态,确保个人数据的保密性;

[0095] (5)计算结果通过用户的私钥进行解密,并发送回医疗机构;用户将此次个人医疗数据的分析请求信息,同步到区块链上作为不可篡改的历史记录。

[0096] 上述的硬件系统,所述的同态加密算法,满足以下条件:

[0097] (1)Enc(PK,m)加密函数以区块链上的用户加密数据公钥PK和消息m作为输入,输出加密个人医疗数据c;

[0098] (2)Dec(SK,c)解密函数以用户私钥和加密个人医疗数据c作为输入,输出消息m;

[0099] (3)Eval(PK,f,c1,…,cl)评估函数以区块链上的用户加密数据公钥、分析算法f以及加密个人医疗数据c1到cl,输出加密的数据cf;

[0100] (4)当c1＝Enc(PK,m1),…,cl＝Enc(PK,ml)Mf＝f(m1,…,ml);

[0101] (5)Cf＝Eval(PK,f,c1,…,cl);

[0102] (6)满足对于任何分析算法f,mf＝Dec(SK,cf)。

[0103] 上述的硬件系统,所述硬件系统的信息按照病人或其监护人的授权进行分级披露。

[0104] 实施例4

[0105] 将区块链技术与数据分布式存储技术结合,满足个人医疗数据的去中心化加密存储、可控共享、使用记录不可篡改的需求。

[0106] 病患个人医疗数据的数据存储量非常大,不适合放在区块链上进行全链同步,因此需要进行分布式加密存储,并在区块链上的个人账户信息中记录存储的地址索引,实现链上链下同步的加密个人医疗数据存储。主要实现步骤为:

[0107] (1)将个人医疗数据,用个人密钥加密,并存储在可以在公网寻址的分布式存储空间,并以个人医疗数据的哈希值作为空间内数据的索引key值;

[0108] (2)在区块链上的加密个人账户信息中,记录个人医疗数据的公网存储地址与数据的哈希值;

[0109] (3)当联网的医疗硬件系统需要访问个人医疗数据时,可以通过区块链的智能合约向病患发出数据访问请求,病患确认授权后,会将准许访问的个人医疗数据的哈希值与公网访问地址作为智能合约的一部分,让联网的医疗硬件系统获取;

[0110] (4)联网的医疗硬件系统通过智能合约获取用户个人医疗数据的公网存储地址与哈希值,并使用哈希值在存储空间内作为索引key值获取加密的医疗数据,然后可以通过哈希值对比验证其正确性。

[0111] (5)联网的医疗硬件系统通过同态加密算法,对获取的加密个人医疗数据进行智能分析运算,获取运算结果。

[0112] 引入同态加密技术,分析加密分布式存储的用户个人医疗数据,解决了联网的医疗硬件系统进行大数据智能分析过程中的个人数据隐私问题。

[0113] 实施例5

[0114] 上述的硬件系统,所述硬件系统的个人账户信息与加密的个人医疗数据互联网地址索引,必须通过用户手机内的私有密钥认证,才能进行读取、管理与分享,每次读取与分享记录,都会记录到个人医疗数据使用记录里面,并在全网的所有区块链上不同用户节点上进行同步;以下为联网的医疗硬件系统对个人医疗数据读取的加密与解密步骤:

[0115] (1)个人医疗数据通过用户存储在可穿戴设备的私用密钥进行加密,存储在互联网上;

[0116] (2)个人医疗互联网索引数据,通过用户存储在可穿戴设备或者手机上的私用密钥进行加密,存储在区块链上;

[0117] (3)联网的医疗硬件系统对个人医疗数据有读取请求时,用户用自己存储在可穿戴设备或者手机上的私用密钥对个人医疗数据进行解密;

[0118] (4)解密的个人医疗数据用密码散列函数SHA产生摘要;

[0119] (5)用户用自己存储在可穿戴设备或者手机上的私用密钥对摘要再加密,形成数字签名;

[0120] (6)将解密的个人医疗数据和加密的摘要同时发送给联网的医疗硬件系统;

[0121] (7)联网的医疗硬件系统使用用户存储在公有区块链上的公共密钥对发送来的摘要解密,获取用户端对个人医疗数据生成的摘要,同时对收到的个人医疗数据用SHA编码加密产生又一摘要;如两者一致,则说明传送过程中信息没有被破坏或篡改过;

[0122] (8)用户将此次个人医疗数据的硬件系统读取请求信息,同步到区块链上。

[0123] 实施例6

[0124] 上述的硬件系统,联网的医疗数据智能分析硬件系统可以通过区块链,向病人或监护人发送个人医疗数据分析的请求,病人或监护人确认授权后,用同态加密的分析算法发送到用户的个人医疗数据上,对加密的个人医疗数据进行加密状态下的运算,整个运算过程个人医疗数据仍旧保持加密状态;以下为基于同态加密算法的分析步骤:

[0125] (1)联网的医疗数据智能分析硬件系统发起分析请求,分成两部分信息进入智能合约,第一部分包含控制参数,另一部分描述计算分析任务;

[0126] (2)来自智能合约的分析请求信息,通过一个编译通道,结合控制参数,编译成可以直接分析加密个人医疗数据的基础计算指令集;

[0127] (3)基础计算指令集发送到用户,获得授权后,将用户的加密个人医疗数据通过基础计算指令集进行计算;

[0128] (4)计算过程中个人医疗数据一致保持加密状态,确保个人数据的保密性;

[0129] (5)计算结果通过用户的私钥进行解密,并发送回联网的医疗数据智能分析硬件

系统;用户将此次个人医疗数据的分析请求信息,同步到区块链上作为不可篡改的历史记录。

[0130] 上述的硬件系统,所述的同态加密算法,满足以下条件:

[0131] (1)Enc(PK,m)加密函数以区块链上的用户加密数据公钥PK和消息m作为输入,输出加密个人医疗数据c;

[0132] (2)Dec(SK,c)解密函数以用户私钥和加密个人医疗数据c作为输入,输出消息m;

[0133] (3)Eval(PK,f,c1,…,c1)评估函数以区块链上的用户加密数据公钥、分析算法f以及加密个人医疗数据c1到c1,输出加密的数据cf;

[0134] (4)当c1=Enc(PK,m1),…,c1=Enc(PK,m1)Mf=f(m1,…,m1);

[0135] (5)Cf=Eval(PK,f,c1,…,c1);

[0136] (6)满足对于任何分析算法f,mf=Dec(SK,cf)。

[0137] 上述的硬件系统,所述硬件系统的信息按照病人或其监护人的授权进行分级披露。

[0138] 实施例7

[0139] 血色素极低病患,性别:男,出院日期:2019年5月,年龄:73岁,住院天数;18天。

[0140] 入院及治疗情况:主要症状体征:纳差3月,发现贫血2个月以上。神志清晰,精神弱,贫血貌,血压90/50mmHg,结膜苍白,巩膜无黄染,浅表淋巴结未及肿大,双肺呼吸音清,未闻及干湿罗音,心率80bpm,律齐,腹软,无压痛及反跳痛,肝脾肋下未及,肠鸣音正常,双下肢不肿。

[0141] 主要化验X线检查结果及其他:外院Hb45g/L,医院末梢血形态未见明显异常,医院腹部CT:肝脏内异常钙化灶,胆囊内结石。

[0142] 入院诊断:重度贫血慢性萎缩性胃炎?消化道肿瘤?骨髓增生异常综合征?胆囊结石腰椎术后。

[0143] 诊疗经过:入院后完善化验检查,查血红蛋白50g/L,血小板59*109/L,予一级护理、输红细胞、补充造血原料、补液、静脉营养、消化酶等对症支持治疗。

[0144] 晨起出现发热、炎性指标升高,Tmax39.4℃,对症退热治疗效果不佳。出现巩膜黄染、腹痛、轻度咳嗽咳白痰,腹部彩超提示肝右叶囊实性区,脓肿?胆囊旁积液?胸片提示肺纹理增粗、肺不张。

[0145] 考虑腹腔脏器感染、肺部感染。化验血胆红素及尿胆原升高,网织红细胞明显升高,末梢血涂片可见“泪滴”红细胞,考虑急性溶血可能性大,予美平抗感染、碳酸氢钠碱化、洗涤红细胞纠正贫血及等治疗。完善腹部CT提示急性胆囊炎、肝脓肿?

[0146] 请普外科会诊考虑:急性胆囊炎、肝脓肿?无肝脓肿穿刺引流指征,建议继续内科保守治疗。经治疗感染逐渐控制,无新发溶血。

[0147] 行骨穿及骨髓活检,结果回报MDS/骨髓增殖性肿瘤?,请血液科会诊后建议感染控制后复查骨穿,可继续给予补充造血原料治疗。体温正常48小时后抗生素降级为来立信联合奥硝唑治疗,感染无加重,腹痛缓解,巩膜黄染消退,无咳嗽咳痰,复查腹部CT胆囊周围渗出较前好转,监测血红蛋白稳定,血胆红素降至正常,尿胆原正常,精神、饮食好转。

[0148] 住院期间出现大便次数增多,查难辨梭毒素阴性,便培养提示菌群失调,予肠道益生菌治疗后好转。

[0149] 完善胃镜提示慢性萎缩性胃炎。目前一般状况尚可，但是对病患血色素的极低状况，不能排除消化道或血液系统的肿瘤，虽然进行了骨髓穿刺，但是不能完全排除肿瘤。

[0150] 经过家属知情同意，系统录入纸质病例信息并识别，系统加密并清洗病人个人信息后，调阅某医院神经内科病程和诊断资料(2019年4月26日-29日)。

[0151] 入院诊断:1.头晕待查后循环缺血?2.缺铁性贫血3.厌食原因待查4.焦虑抑郁状态5.维生素缺乏6.叶酸缺乏7.周围神经病8.微循环障碍。

[0152] 出院诊断1.后循环缺血2.缺铁性贫血3.厌食原因待查4.焦虑抑郁状态5.维生素缺乏6.叶酸缺乏7.周围神经病8.微循环障碍。

[0153] 住院情况患者主因″间断头晕伴进食差40余天″入院。入院查体:T36.5℃,P70次/分,R20次/分,BP120/80mHig(左侧＝右侧)。

[0154] 神清，查体配合，步入病区，全身皮肤粘膜及巩膜无黄染及出血点，面色苍白，全身浅表淋巴结未扪及肿大。胸廓对称无畸形，双肺叩清，呼吸音清，未闻及干，湿性啰音，心界不大，HR:70次/分，律齐，各瓣膜听诊区未闻及病理性杂音，腹平软，无压痛，无反跳痛及肌紧张。

[0155] 肝脾肋下未及，肝区及双肾区无叩击痛，脊柱四肢无畸形，双下肢不肿。神经系统查体:神清，语利，记忆力、计算力、定向力正常，双眼睑无下垂，双侧瞳孔等大等圆，直径3mm，对光反射灵敏，眼球位置正常，眼动充分，未见眼震。双侧面纹对称，闭目有力;双侧咬肌对称有力，鼓腮无漏气，双侧鼻唇沟对称，口角无歪斜，伸舌居中，软腭上抬可，咽反射存在，无舌肌萎缩及纤颤，听力正常，双侧转颈、耸肩有力。四肢肌力5级，四肢肌容积饱满，肌张力对称适中，腱反射对称减退，双侧病理征阳性。深浅感觉系统检查正常。共济运动正常。颈软无抵抗，Kerning征、Brudzinski征阴性。双侧颈动脉及锁骨下动脉听诊区未闻及明显杂音。辅助检查:血常规:红细胞1.45*1012/L，血红蛋白57g/L。

[0156] 诊疗经过:患者入科后给予低盐低脂饮食，监测患者血压;入科后给予完善相关辅助检查。入院后给予改善心、脑供血(银杏叶)、改善微循环(前列地尔)、营养神经(腺苷钴胺)，予脂肪乳、氨基酸静脉营养、同时对症改善情绪等对症治疗。

[0157] 临检检验报告:,*红细胞1.29*10^{12}/L↓,*血红蛋白51g/L,*红细胞压积14.7%↓,*红细胞平均体积114.2flt,*平均血红蛋白含量39.4pgt,*血小板11*10～9/L↓。

[0158] CT检测右侧外侧裂区域可见点高密度钙化灶，边清锐利，双侧脑室体旁灰白质交界处白质密度略有减低，呈对称性改，脑室略有扩张，脑沟裂略有增宽，加深，中线结构无移位，颅骨骨质未见异常，头皮:组织无肿胀二所扫副鼻窦及双侧乳突蜂房显示尚可，余(-)。

[0159] CT:轮廓对称，肋骨走行未见异常，纵隔气管居中，纵隔内血管影显示清，主动脉管壁及冠走行区可见高密度钙化影像，血管间隙内可见小的淋巴结影，气管开口通畅，双肺下叶纹理略有增粗，左肺内可见索条。

[0160] 脑部扫描:直隙性脑梗塞，建议结合临床病史，对照原片，必要时随诊助诊，外侧裂区域异常钙化灶，扣髓鞘性改变，老年年性脑改变。议结合临床及相关化验室检查主动脉及冠脉粥样硬化，必要时结合相关CTA检查助诊。

[0161] 但是病例调阅没有能够排除肿瘤的可能性。

[0162] 经过家属知情同意，系统录入纸质病例信息并识别，系统加密并清洗病人个人信息后，调阅某医院消化内科病程和诊断资料(2011年10月)。

[0163] 记录:性别:男性,年龄:65(当时)。

[0164] 患者本人及家属陈述:主诉恶心、呕吐伴贫血1月余。现病史患者缘于1月前无明显诱因开始出现恶心、呕吐,呕吐为非喷射性,以进食后多见,呕吐物为胃内容物,无特殊气味,不伴听力障碍,无明显头晕、头痛及视物眩晕感,无发热、寒战、腹痛、腹泻、腹胀,遂至我院门诊就诊,诊查碳13呼气实验示Hp(+),血红蛋白75g/L,红细胞计数1.84×10″/L,红细胞压积0.217,行药物治疗,效果欠佳,原有恶心、呕吐症状无明显好转。

[0165] 为求进一步治疗,患者于今日再次至我院门诊就诊,门诊以″恶心、呕吐伴贫血原因待查″收治入院,此次病程中,患者无明显畏寒、发热、头晕、头痛,无心悸、胸闷、胸痛,无咳嗽、咳痰、咯血,无腹痛、腹泻,无便血、黑便、黄疸。自起病以来,患者精神及食欲一般,睡眠可,大、小便正常,自诉体重下降约5Kg。

[0166] 既往史1997年曾因″腰椎间盘突出症″于外院行手术治疗;对″海鲜″过敏;否认″高血压、糖尿病、冠心病″等慢性病史;否认″肝炎、结核″等传染病病史;否认外伤、输血史;否认药物过敏史;预防接种随当地。个人史生于原籍,久居当地,否认疫水、疫区接触史,否认工业毒物、粉尘及放射性物质接触史,无烟酒不良嗜好;婚育史:已婚30余年,育有2子,爱人及儿子均体健。

[0167] 头颅无畸形,五官端正,双侧结膜无充水肿,巩膜无黄染,双侧瞳孔等大等圆,直径约3毫米,对光反射受敏,精神正常。耳鼻无异常分泌物。口唇红润,无发绀,鼻唇沟两侧对称、示齿口有歪斜,伸舌居中,咽部无充血。颈软无抵抗,颈静脉无怒张,气管居中,甲状腺不大。双侧胸廓对称,呼吸运动正常,胸壁无静脉曲张及压痛。双侧呼吸运动一致,呼吸动度正常,两侧语颤对称一致,无皮肤握雪感及胸膜摩擦感。叩诊呈清音,双肺呼吸音稍粗,未闻及明显干、湿罗音及胸膜摩擦音。心尖搏动位于左侧第五肋间锁骨中线内侧0.5cm,心前区无隆起,无心包摩擦感,心浊音界无扩大,心率78次/分,律齐,心音有力,各瓣膜听诊区未闻及病理性杂音。腹软,腹壁静脉无曲张,未见肠型、蠕动波及异常搏动,全腹无明显压痛、反跳痛及肌紧张,肝脾肋下未触及,腹部触诊未扪及包块,肝颈静脉回流征阴性,莫菲氏征阴性,移动性浊音阴性,叩诊呈鼓音,肠鸣音2-4次/分,未闻及气过水声及高调金属音。

[0168] 肛门及外生殖器未查。脊柱呈生理弯曲。四肢无畸形,双下肢无水肿,无静脉曲张及溃疡。四肢无畸形,无杵状指(趾),足背动脉搏动正常存在。四肢肌力V级、肌张力正常,肱二头肌反射、肱三头肌反射正常,双侧膝反射正常,双侧Hoffmann征(-),双侧Babinski征(-)。

[0169] 住院经过:患者主因恶心、呕吐伴贫血1月余入院。对″海鲜″过敏。

[0170] 入院查体:心、肺查体未及明显异常,腹平软,全腹无明显压痛、反跳痛及肌紧张,肠鸣音2-4次/分。辅助检查:碳13呼气实验示Hp(+);胃镜示胃粘膜贫血象,慢性浅表性胃炎;单一过敏原检测:IgG抗体食物组未见异常。IgE抗体混合组示狗皮毛(3+),屋尘(2+),螨虫(+),螃蟹(+)。诊断为1)巨幼细胞性贫血2)慢性浅表性胃炎3)恶心、呕吐原因待查。

[0171] 由于患者签字拒绝行头颅CT、胸部CT以及骨髓穿刺等一切进一步检查以明确贫血原因,入院后仅予补充维生素B12、营养支持等对症治疗。目前患者一般情况可,复查血常规示血红蛋白81.0g/L,维生素B12正常,未再恶心、呕吐,患者及家属要求出院,请示上级医生同意后予安排出院。

[0172] 2011.10.12出院诊断:1、巨幼细胞性贫血2、慢性浅表性胃炎。1)巨幼细胞性贫血

2)慢性浅表性胃炎3)恶心、呕吐原因待查。出院注意事项1)出院后注意休息,加强营养,定期复查血常规;2)巨幼细胞性贫血至血液科进一步治疗;3)避免接触狗皮毛、屋尘、螨虫、螃蟹等物,以免过敏;3)如有不适,门诊随诊。

[0173] 继续对病人的个人信息加密并清洗,发现病人同父同母姐姐,在2017年,同样出现“巨幼细胞性贫血”,其病程的过程与时间上接近且预后良好。

[0174] 结合2011年10月和2019年4月的个人信息清洗后病情数据调阅和家族病史调研,排除了疑似肿瘤,结合营养强化后缓慢恢复。

[0175] 因此,在2019年6月,对该病人的诊断为巨幼细胞性贫血,估计有相当可能性具有家族遗传特质。现病人回访调查表明状况良好,日常规范补充叶酸和B族维生素(2020.4.10)。

[0176] 如果没有个人病例的既往病史的调研,医生极难排除病患的恶性肿瘤的可能性。但在大数据的个人信息的加密清洗后的回溯调研,可以精准排除恶性肿瘤,并作出准确的治疗,还可以进行流行病和遗传状况调研,出院后继续追踪病患健康状况,提示用药,达成全程病情控制。

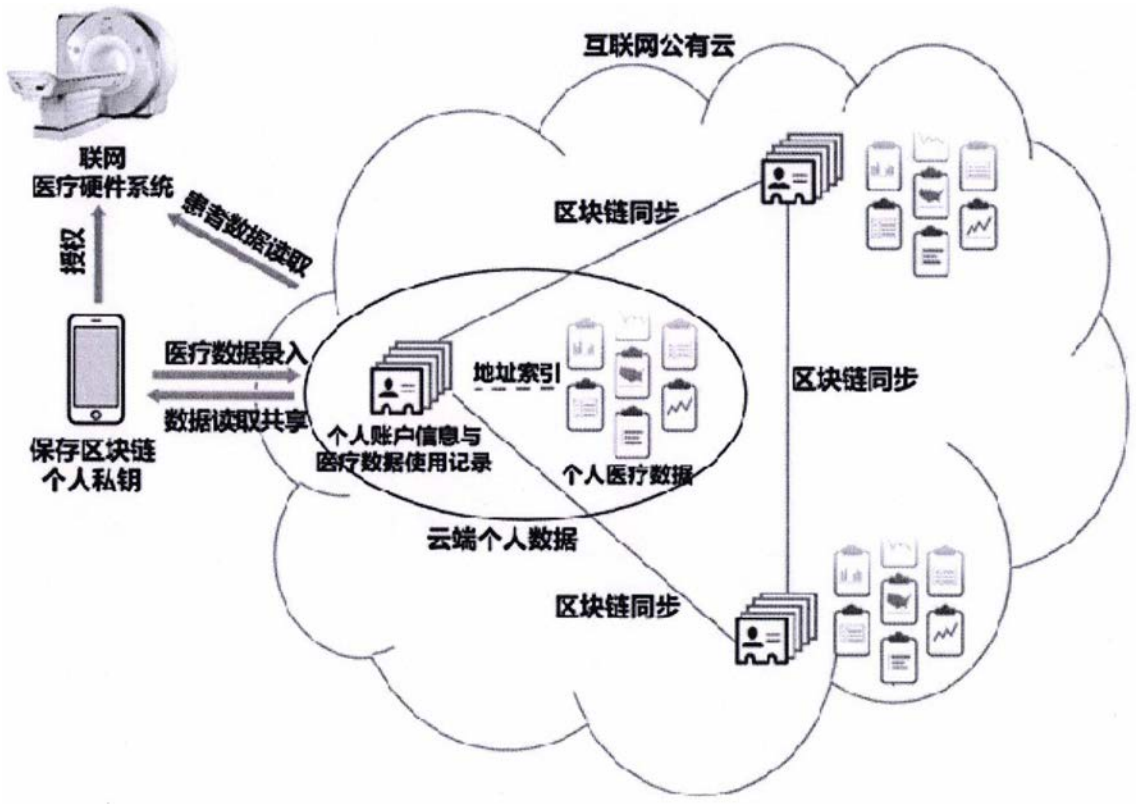

互联网公有云
联网
医疗硬件系统
授权
患者数据读取
区块链同步
医疗数据录入
数据读取共享
地址索引
个人账户信息与
医疗数据使用记录
个人医疗数据
区块链同步
保存区块链
个人私钥
云端个人数据
区块链同步

图1

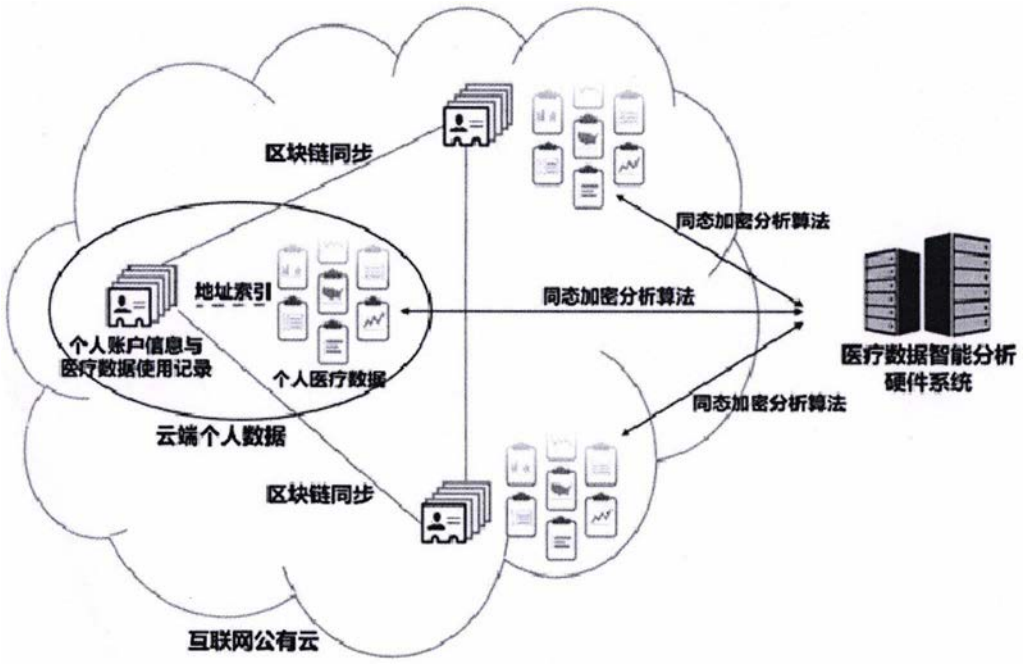

区块链同步
同态加密分析算法
地址索引
同态加密分析算法
个人账户信息与
医疗数据使用记录
个人医疗数据
医疗数据智能分析
硬件系统
同态加密分析算法
云端个人数据
区块链同步
互联网公有云

图2