(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 113766512 A
(43)申请公布日 2021.12.07

(21)申请号 202111315344.8

(22)申请日 2021.11.08

(71)申请人 广州天鹏计算机科技有限公司
地址 510000 广东省广州市天河区珠江东路11号1501室

(72)发明人 陆广林

(51)Int.Cl.
H04W 12/63(2021.01)
H04W 12/033(2021.01)
H04W 12/06(2021.01)
H04W 12/08(2021.01)
H04L 29/06(2006.01)
G16H 10/60(2018.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)

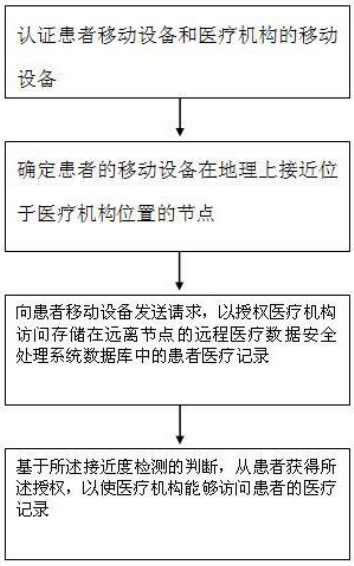
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种医疗大数据信息安全处理方法及系统

(57)摘要

本发明提供了一种医疗大数据信息安全处理方法及系统，该方法包括：认证患者移动设备和医疗机构的移动设备；确定患者的移动设备在地理上接近位于医疗机构位置的节点；向患者移动设备发送请求，以授权医疗机构访问存储在远离节点的远程医疗数据安全处理系统数据库中的患者电子病历；基于所述接近度检测的判断，从患者获得所述授权，以使医疗机构能够访问患者的电子病历。本发明提出了一种医疗大数据信息安全处理方法及系统，允许患者将医疗信息数据以安全格式存储在独立的数据库中，并使每个患者能够允许不同的医务人员访问有限范围的数据，允许患者保存和存储个人访问密钥，防止对医疗信息数据的未授权访问。



CN 113766512 A

1.一种医疗大数据信息安全处理方法,用于实现患者医疗数据的安全访问,其特征在于,包括:

在远程服务器上认证患者的移动设备;

认证医疗机构的移动设备;

通过电子设备接近度检测来确定患者的移动设备在地理上接近位于医疗机构位置的节点,用于判断医疗机构是否可以访问存储在远离所述节点的远程医疗数据安全处理系统中的患者电子病历;

向患者移动设备发送请求,以授权医疗机构访问存储在远离所述节点的远程医疗数据安全处理系统数据库中的患者电子病历;

基于所述接近度检测的判断,从患者获得所述授权,以使医疗机构能够访问患者的电子病历;

获得用于解密存储在医疗数据安全处理系统数据库中的患者电子病历的患者个人电子密钥,其中对所述患者个人电子密钥的访问由患者在指定的有限时间段内提供;

在远程服务器上利用所述患者的私密密钥来解密患者的电子病历;

利用医疗机构和远程服务器的异步PKI密钥对患者的电子病历进行二次加密并安全地传输给医疗机构以供查看和更新;

在医疗数据安全处理系统数据库中存储用患者的私密密钥加密的患者的电子病历;

在服务器接收存储在医疗数据安全处理系统数据库中的患者电子病历的定位符;

利用定位符在医疗数据安全处理系统数据库中找到患者的电子病历,以供医疗机构查看和更新;其中所述医疗数据安全处理系统数据库不以非加密格式维护或存储除定位符之外的任何患者识别信息。

2.根据权利要求1所述的方法,其特征在于,进一步包括:

从所述医疗机构接收更新的患者电子病历,所述更新的患者电子病历利用所述服务器的异步PKI密钥加密;

使用服务器的个人PKI密钥解密更新的患者电子病历;

用患者的私密密钥二次加密服务器上更新的患者电子病历;

将更新的加密记录存储在医疗数据安全处理系统数据库中。

3.根据权利要求1所述的方法,其特征在于,进一步包括:

接收医疗机构的移动设备的操作者的指纹,并验证其与医疗机构的存储的指纹匹配,所述医疗机构被患者授权访问存储在医疗数据安全处理系统数据库中的该患者的个人电子病历;

接收患者移动设备的操作者的指纹,并验证其与存储的患者授权的指纹匹配,以授权访问存储在医疗数据安全处理系统数据库中的该患者的个人电子病历。

4.根据权利要求1所述的方法,其特征在于,进一步包括:

维护映射到每个注册患者的定位符的单独数据库;

接收和处理患者的身份信息,以访问医疗数据安全处理系统数据库;

在认证患者的身份和请求访问医疗数据安全处理系统数据库的患者移动设备时,将存储在医疗数据安全处理系统数据库中的患者电子病历的定位符传输到服务器,用于读取和更新对记录的访问。

5.一种医疗大数据信息安全处理系统，其特征在于，用于执行权利要求1-4所述的方法。

一种医疗大数据信息安全处理方法及系统

技术领域

[0001] 本发明涉及大数据安全技术领域，特别涉及一种医疗大数据信息安全处理方法及系统。

背景技术

[0002] 现如今，患者的医疗数据信息由患者接受治疗的不同的医院、门诊医生、药房以及相关服务提供方保存。当一个患者改变不同的地理位置接受不同医生的治疗时，由于隐私保护、以及不同医疗提供方的内部政策，系统变得更加复杂。一方面，患者的健康记录必须是安全和保密的，必须严格保护对这些记录的访问，防止未授权的用户对医疗信息的访问；另一方面，医生都必须拥有关于患者病史、病情、治疗方案的完整和准确的信息。目前现有的系统允许患者邀请医生共享其患者的医疗数据。然而，这些系统要求使用医生或其受托人的用户标识和密码授予他们授权。因此，越来越多的用户密码由患者发布以访问其医疗信息，增加了通过非法途径获取患者个人秘钥的可能性。

发明内容

[0003] 为解决上述现有技术所存在的问题，本发明提出了一种医疗大数据信息安全处理方法及系统，该方法包括：

在远程服务器上认证患者的移动设备；

认证医疗机构的移动设备；

通过电子设备接近度检测来确定患者的移动设备在地理上接近位于医疗机构位置的节点，用于判断医疗机构是否可以访问存储在远离所述节点的远程医疗数据安全处理系统中的患者电子病历；

向患者移动设备发送请求，以授权医疗机构访问存储在远离所述节点的远程医疗数据安全处理系统数据库中的患者电子病历；

基于所述接近度检测的判断，从患者获得所述授权，以使医疗机构能够访问患者的电子病历；

获得用于解密存储在医疗数据安全处理系统数据库中的患者电子病历的患者个人电子密钥，其中对所述患者个人电子密钥的访问由患者在指定的有限时间段内提供；

在远程服务器上利用所述患者的私密密钥来解密患者的电子病历；

利用医疗机构和远程服务器的异步PKI密钥对患者的电子病历进行二次加密并安全地传输给医疗机构以供查看和更新；

在医疗数据安全处理系统数据库中存储用患者的私密密钥加密的患者的电子病历；

在服务器接收存储在医疗数据安全处理系统数据库中的患者电子病历的定位符；

利用定位符在医疗数据安全处理系统数据库中找到患者的电子病历，以供医疗机构查看和更新；其中所述医疗数据安全处理系统数据库不以非加密格式维护或存储除定位

符之外的任何患者识别信息。

[0004] 优选地，进一步包括：

从所述医疗机构接收更新的患者电子病历，所述更新的患者电子病历利用所述服务器的异步PKI密钥加密；

使用服务器的个人PKI密钥解密更新的患者电子病历；

用患者的私密密钥二次加密服务器上更新的患者电子病历；

将更新的加密记录存储在医疗数据安全处理系统数据库中。

[0005] 优选地，进一步包括：

接收医疗机构的移动设备的操作者的指纹，并验证其与医疗机构的存储的指纹匹配，所述医疗机构被患者授权访问存储在医疗数据安全处理系统数据库中的该患者的个人电子病历；

接收患者移动设备的操作者的指纹，并验证其与存储的患者授权的指纹匹配，以授权访问存储在医疗数据安全处理系统数据库中的该患者的个人电子病历。

[0006] 优选地，进一步包括：

维护映射到每个注册患者的定位符的单独数据库；

接收和处理患者的身份信息，以访问医疗数据安全处理系统数据库；

在认证患者的身份和请求访问医疗数据安全处理系统数据库的患者移动设备时，将存储在医疗数据安全处理系统数据库中的患者电子病历的定位符传输到服务器，用于读取和更新对记录的访问。

[0007] 本发明进一步提出了一种医疗大数据信息安全处理系统，用于执行上述的医疗大数据信息安全处理方法。

[0008] 本发明相比现有技术，具有以下优点：

本发明提出了一种医疗大数据信息安全处理方法及系统，允许患者将医疗信息数据以安全格式存储在独立的数据库中，并使每个患者能够允许不同的医务人员访问有限范围的数据，允许患者保存和存储个人访问密钥，防止对医疗信息数据的未授权访问。

附图说明

[0009] 图1是根据本发明实施例的医疗大数据信息安全处理方法的流程图。

具体实施方式

[0010] 下文与图示本发明原理的附图一起提供对本发明一个或多个实施例的详细描述。结合这样的实施例描述本发明，但是本发明不限于任何实施例。本发明的范围仅由权利要求书限定，并且本发明涵盖诸多替代、修改和等同物。在下文描述中阐述诸多具体细节以使提供对本发明的透彻理解。出于示例的目的而提供这些细节，并且无这些具体细节中的一些或所有细节也可以根据权利要求书实现本发明。

[0011] 本发明的一方面提供了一种医疗大数据信息安全处理方法及系统。图1是根据本发明实施例的医疗大数据信息安全处理方法及系统流程图。

[0012] 本发明允许不同的患者将其医疗信息数据以安全和加密的格式存储在中心化位置，并且只使用一个密钥，用于访问其以加密格式单独存储在医疗数据安全处理系统中的

医疗信息数据，如果没有患者的正确密钥，则拒绝访问或读取患者存储的医疗信息，使得患者可以快速建立、更新和上传由特定医生或医院维护的医疗数据给患者的其他医疗信息。患者能够限制对任何患者医疗服务提供者的医疗信息的子集的访问，并且能够根据特定时间和地点与医生共享查看或更新，例如在医生就诊、医院治疗期间。

[0013] 每个医生和每个电子病历可能只有特定患者的医疗信息子集，而患者可以控制和访问更完整的医疗信息，并且可以在患者离开医疗地点后移除所有访问授权，但保持医疗信息可由患者访问。本发明允许医务人员快速上传数据到医疗数据安全处理系统，但是利用每个患者的私钥来加密每个患者的医疗信息数据，使这种上传安全和防篡改。医疗机构将患者数据从电子病历转移到更安全的医疗数据安全处理系统，只能使用医疗机构持有的私有对称密钥解密。将医疗数据安全处理系统中医生的个人患者记录复制到患者的医疗数据安全处理系统，患者的医疗信息用患者的对称私钥二次加密，并存储在医疗数据安全处理系统，对患者的医疗信息数据副本的访问由患者拥有，并且该访问可以由患者授权给多个医疗机构。

[0014] 患者控制对存储在云中的医疗信息数据的访问。当患者在医疗地点的地理位置时，患者允许访问该医疗信息并与医生共享。医生在虚拟医疗目录中查看和更新患者的医疗信息。更新完成后，医疗机构的任何人都将无法再访问患者的医疗信息，降低了为每个医疗机构授予医疗信息永久访问权而导致的风险。

[0015] 本发明的患者记录包含记录定位符。患者的记录由记录定位符标识，而不需要个人身份信息。每个不同患者的记录用其自己所有者的对称加密密钥分别加密，患者拥有并控制对存储在数据记录库中的自身的加密的医疗信息数据的访问，其通过控制对称的私有加密密钥以及通过所需的授权和映射过程来实现。在该过程中，患者被认证，然后该映射被提供给患者的实际加密记录。在优选实施例中，系统使用的数据结构不包括任何个人信息，例如姓名、地址等。这些数据只能通过匿名密钥识别和访问。

[0016] 系统不仅为患者保留匿名加密的医疗信息数据，还提供独立的密钥库服务器和安全目录映射服务器，作为访问医疗数据安全处理系统数据中的医疗信息的附加安全保护层。密钥库服务器为保存其个人对称密钥的副本的患者提供了安全的电子存储。密钥库服务器将密钥直接提供给医疗数据安全处理系统服务器，或患者的授权设备。医疗数据安全处理系统账户目录映射服务器在用私密密钥和正确验证的患者凭证执行请求的认证之后，为给定患者提供医疗数据安全处理系统账户，并将基于来自特定患者的密钥库服务器的私密密钥，为给定患者提供医疗数据安全处理系统账户。最后，在获得了患者的私密密钥和特定患者的账户后，医疗数据安全处理系统服务器处理和验证该数据，并使用患者的私密密钥来检索或更新医疗数据安全处理系统数据。私有密钥与医疗数据安全处理系统数据存储在不同的服务器位置。从患者存储在医疗数据安全处理系统的数据中去除可识别信息，并且简化为仅账户或定位符和加密的患者记录。即使没有被授权的人截获了该数据记录，如果不将其与正确的患者账户相关联，该信息实际上将是无用的。因此，为医疗数据安全处理系统数据访问和更新能力增加了安全级别。

[0017] 根据本发明，医疗数据安全处理系统服务器不存储用于访问医疗数据安全处理系统中患者的医疗信息数据的患者私密密钥的副本。系统服务器仅在有限的时间段内接收患者的密钥，用于在有限的指定时间段内，例如在患者访问医疗机构期间，由患者授权读取和

更新医疗信息数据。一旦授权访问或更新过程完成，系统服务器将擦除患者的密钥。患者的永久密钥由该患者保存在个人电子设备或放置在密钥库中。

[0018] 在可选的实施例中，也可以通过请求移动设备的操作者的指纹、在授权服务器接收该指纹并将其与每个患者的注册记录进行比较来确认操作患者移动设备的身份，以确保正确的人操作患者的移动设备。允许患者使用不同的移动设备，并通过传输由移动设备上的硬件和应用软件提取的指纹，向授权服务器确认其身份。在移动设备上执行的应用程序预先请求用户录入指纹，并将其发送给服务器进行认证。

[0019] 关于每个患者移动设备的邻近信息被发送到邻近检测服务器并在该服务器判断，并且医疗机构的移动设备信息在医疗机构移动设备服务器接收和处理。患者认证服务器与医疗机构移动设备服务器通信，基于患者在医疗机构的出现和密钥授权，患者使用安全密钥授权对特定医疗机构进行访问。它还可以依赖于设备操作者的指纹认证，以确保患者已经授权访问，并且授权的医疗机构操作已经请求访问患者的医疗信息的移动设备。

[0020] 传输对称密钥以使用患者的对称密钥加密或解密医疗信息患者的数据。患者在预设的时间内向系统服务器和医疗数据安全处理系统提供并传输其对称密钥，以允许特定授权的医疗机构访问患者在医疗数据安全处理系统的加密医疗信息。该患者的私密密钥不是由医疗机构发送或维护的，患者只需要一个密钥就可以让多个医务人员读取和更新患者的医疗信息，该医疗信息以加密格式存储在医疗数据安全处理系统。

[0021] 传输协议利用PKI非对称密钥加密传输进行安全传输，使用患者的私有对称密钥对患者的医疗信息数据进行加密和解密，包括对存储记录的更新。患者移动设备与服务器建立安全通信。患者移动设备接收服务器公钥，并使用服务器公钥加密患者的私有对称密钥，该服务器公钥由系统服务器发送给患者移动设备。系统服务器从患者移动设备接收患者的对称私钥，并使用服务器的私钥来解密传输。当患者给予特定医疗机构独立的授权时，允许其使用患者的对称私钥在系统服务器上解密和读取或更新该患者的医疗信息。这允许系统服务器在特定医疗机构的授权访问期间加密和解密医疗数据安全处理系统的数据。一旦授权到期，系统服务器将擦除患者的私有对称密钥，并且不保存在其任何内部存储器或医疗数据安全处理系统数据库中。

[0022] 服务器还与医疗机构的移动设备以及存储加密患者病历的医疗数据安全处理系统服务器和数据通信。当确认特定授权医生被允许使用移动设备读取或更新患者的医疗信息时，它使用患者的私有对称密钥解密患者的医疗信息，该密钥在授权访问期间被接收并保存在系统服务器。然后，其使用医生的PKI非对称密钥来二次加密医疗信息数据，以安全传输到医疗机构的移动设备。

[0023] 医疗机构的移动设备接收系统服务器的公共密钥，并使用公共密钥来加密医生的公共密钥并将其传输到系统服务器。然后，系统服务器使用医生的公钥来二次加密并将患者数据记录从系统服务器传输到医生的移动设备，移动设备接收患者记录并将其显示在医生的移动设备的屏幕上。医生的设备不具有患者的私有密钥，因为该密钥被发送到系统服务器，并且当被授权时，在授权会话期间被用于解密患者的医疗信息数据。然后，服务器用医生的非对称密钥二次加密解密的患者的医疗信息，以使从服务器安全传输到医生的移动设备。这允许医生移动设备利用其公钥和私钥来解密二次加密的患者数据，并在医生的移动设备上查看或更新该数据。对于更新，系统服务器将向医生的移动设备发送其公钥，该公

钥可用于对所传输的更新数据进行加密。然后，在系统服务器上，更新的记录将使用患者私有对称加密密钥二次加密，然后以加密形式存储在医疗数据安全处理系统。

[0024] 在完成认证并且向系统服务器和提供了用于患者数据记录的新记录位置密钥之后，创建数据记录，并用记录编号和患者的私有对称密钥对其进行加密。来自患者的请求以及用户标识和密码由系统服务器上处理，然后自动生成对认证记录数据库的请求，并接收用于患者数据记录位置的记录位置标识。位置密钥然后被发送到数据记录库，其使用该密钥来找到并返回给系统服务器该患者的加密的医疗信息数据记录。加密的医疗信息记录被传输到系统服务器，然后传输到患者的移动设备。因为没有患者的私密密钥，这些加密的数据记录无法解密和读取。医疗机构并不维护和控制对患者医疗信息数据的原始电子版本的访问。

[0025] 可选地，在私密密钥的安全数据存储方面，本发明的进一步实施例中从多个密钥因子构造加密密钥，其中构造过程包括：将多个密钥因子分配给多个密钥维护模块，每个密钥维护模块中对多个密钥因子中各自的密钥因子采用多个独立的安全防护策略；请求访问多个密钥因子以构建加密密钥。在移动设备加密数据时，加密过程包括：通过二次加密的通信信道接收多个密钥因子的子集；在移动设备生成加密密钥；并且在加密数据之后，删除通过两次加密的通信信道接收的多个密钥因子的子集，保留先前存储在移动设备的多个密钥因子中的任何一个；将加密数据存储在耦合到移动设备的多个服务器中。而在移动设备解密数据时，通过两次加密的通信信道接收多个密钥因子的子集；在移动设备生成加密密钥；并且在解密数据之后，删除通过两次加密的通信信道接收的多个密钥因子的子集，保留先前存储在移动设备的多个密钥因子。

[0026] 此外，将多个关键元素中的存储在耦合到移动设备的多个服务器中；在客户端可信计算设备内执行加密和解密；监视客户端可信存储设备内的多个密钥因子，客户端可信存储设备本地连接到客户端可信计算设备，以在加密和解密期间实现临时传输。

[0027] 在移动设备恢复多个密码，其中多个密钥因子包括用于由移动设备恢复的多个密码，多个密码与存储在多个服务器中的密码变换和存储在客户端可信存储设备中的密码恢复短语相关联，恢复多个密码还包括：通过两次加密的通信信道向客户端可信计算设备传输密码变换；以及在客户端可信计算设备处从客户端可信存储设备接收密码恢复短语。

[0028] 其中，与每个密码相关联的密码恢复短语是从对在注册过程中确定的多个问题的多个答案构建的，其中，多个问题分布在多个服务器中，并且多个答案存储在客户端可信存储设备中。

[0029] 优选地，在存储加密数据之前，在多个服务器使用第二层加密来加密数据。其中使用第二加密层加密数据包括：通过逐位添加第二多个密钥因子来生成以服务器为中心的加密密钥，第二多个密钥因子存储在多个服务器中的不同服务器上，并且其中需要第二多个密钥因子来重建以服务器为中心的加密密钥。

[0030] 其中通过二次加密通信信道接收多个密钥因子的子集还包括：提供二次加密通信信道作为补充现有通信协议的加密层，加密层通过以下步骤形成：从第一和第二因变量构造加密密钥，第一因变量由服务器的第一测量确定，第二因变量由移动设备的第二测量确定，第一和第二测量都是随机过程的函数，以使能够测量一组传输的概率结果。其中能够测量一组传输的概率结果的随机过程包括：在服务器和移动设备之间发送多个UDP报文，以及

测量服务器和移动设备之间的多个行进时间。多个行进时间包括从服务器到移动设备和到服务器的第一阶段以及从移动设备到服务器和到移动设备的第二阶段的行进时间，多个行进时间包括第一阶段和第二阶段的延迟测量。

[0031] 其中在服务器和移动设备之间发送多个UDP报文，以及测量服务器和移动设备之间的多个行进时间，包括测量从服务器到客户端可信计算设备、到第二客户端可信计算设备以及回到服务器的多个行进时间。在服务器和移动设备之间发送多个UDP报文包括：在容易发生信道错误的通信信道上发送UDP报文，每个报文包含伪随机比特；以及在服务器接收UDP报文的多个索引，多个索引由移动设备选择，并且识别在第一次传输尝试中成功接收的UDP报文的子集；以及通过使用所识别的UDP报文子集来生成加密密钥。通过使用所识别的UDP报文的子集来生成密钥包括通过逐位加法过程来添加UDP报文的子集。

[0032] 综上所述，本发明提出了一种医疗大数据信息安全处理方法及系统，允许患者将医疗信息数据以安全格式存储在独立的数据库中，并使每个患者能够允许不同的医务人员访问有限范围的数据，允许患者保存和存储私人访问密钥，防止对医疗信息数据的未授权访问。

[0033] 显然，本领域的技术人员应该理解，上述的本发明的各模块或各步骤可以用通用的计算系统来实现，它们可以集中在单个的计算系统上，或分布在多个计算系统所组成的网络上，可选地，它们可以用计算系统可执行的程序代码来实现，从而，可以将它们存储在存储系统中由计算系统来执行。这样，本发明不限制于任何特定的硬件和软件结合。

[0034] 应当理解的是，本发明的上述具体实施方式仅仅用于示例性说明或解释本发明的原理，而不构成对本发明的限制。因此，在不偏离本发明的精神和范围的情况下所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。此外，本发明所附权利要求旨在涵盖落入所附权利要求范围和边界、或这种范围和边界的等同形式内的全部变化和修改例。

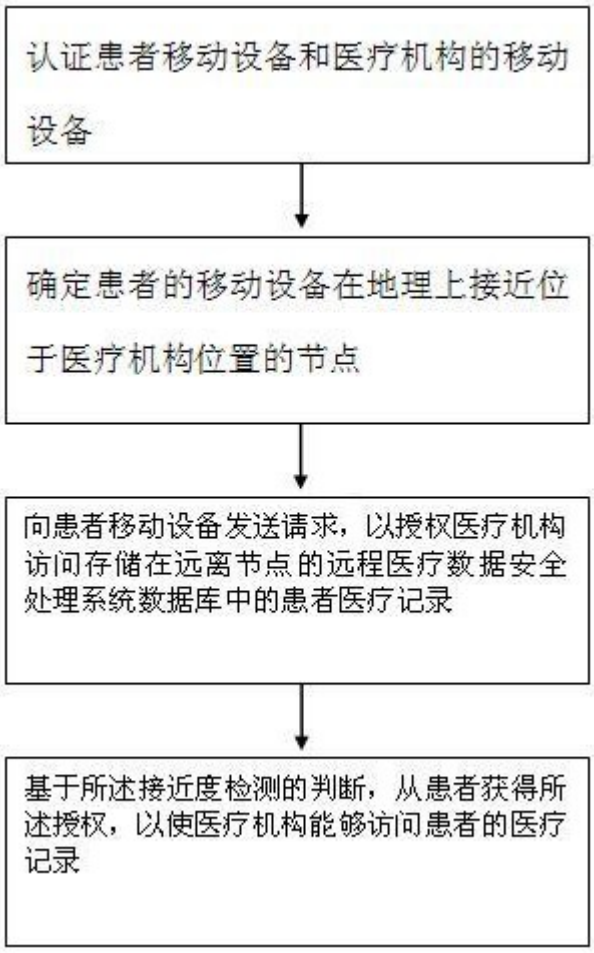

认证患者移动设备和医疗机构的移动设备
确定患者的移动设备在地理上接近位于医疗机构位置的节点
向患者移动设备发送请求，以授权医疗机构访问存储在远离节点的远程医疗数据安全处理系统数据库中的患者医疗记录
基于所述接近度检测的判断，从患者获得所述授权，以使医疗机构能够访问患者的医疗记录

图1