文章编号:1000-5862(2017)05-0484-07

安全存储医疗记录的区块链方法研究

梅 颖
(中国传媒大学计算机学院,北京 100024)

摘要:针对医疗信息系统中存在的医疗信息记录存储的安全和隐私保护问题,结合区块链和云存储技术,提出了一个医疗记录安全存储方案. 该方案利用区块链来保存医疗记录的公共信息、匿名身份和访问权限,使医疗记录的真实数据加密保存在链下存储结构中,有效实现了病人对个人医疗数据的所有权和访问权限的控制以及对敏感医疗数据的安全存储.

关键词:区块链;医疗记录;安全存储;隐私保护
中图分类号:TP 391 **文献标志码**:A **DOI**:10.16357/j.cnki.issn1000-5862.2017.05.07

0 引言

在医疗保健系统中,病人的医疗记录(包括处方、化验单、病理结果、核磁共振图像等)都是宝贵的数据资产,若能够为医生、护理人员和研究者创建一个共享的数据源,提供及时、准确和广泛的病人健康数据,并实现跨机构的数据共享,则可以帮助医护人员制定优化的治疗计划,并为研究人员提供宽泛的数据集以研究疾病、加速生物医药的研发. 然而,有许多因素制约了病人医疗记录信息的共享,如电子医疗记录的普及程度还不高,大多医疗机构还是采用纸质医疗记录,医疗记录的数据结构不统一、不兼容,无法实现安全跨机构的网络共享,最主要的还是涉及到医疗记录的安全和隐私问题[1].

个人的医疗记录属于个人数据,涉及到个人隐私和安全问题,其所有权归个人所有,只有授权的用户才可以访问相关的医疗记录. 保护个人医疗记录的隐私不仅是道德的责任,更是法律的强制要求. 数据匿名性可以用来保护个人医疗记录数据的安全. 在个人数据隐私保护方面,研究人员已提出了许多针对个人数据进行隐私保护的技术. k-匿名,通过构建匿名数据集使得每个敏感信息和其他的 $k-1$ 个记录具有不可区分性[2]. 和 k-匿名相关的扩展包括 l-多样性,通过对敏感数据采用足够多样的数据集表示来实现对敏感信息的隐私保护[3],还有 t-closeness,通过对敏感信息重新分布实现隐私保护[4]. 有研究证实了用以上方法实现的匿名数据集,只要提供少量的数据点或者高维度的数据就可以被解匿名[5-6]. 其他的隐私保护方法还包括差分隐私,通过在计算过程中添加噪音来保护隐私[7];还有同态加密,将隐私数据进行加密并允许任何计算运行在密文上[8]. 传统的电子医疗记录存储模式均采取中心化的模式,传统的数据安全模型依靠创建越来越坚固的墙,例如增加多因子认证访问控制,采用更强的加密方案等. 然而,这也意味着一旦敌手进入了系统,就可以访问到所有数据,存在有单点失败问题. 同时,用户必须依赖于可信第三方的诚实性.

近年来,随着云计算技术的发展和应用,电子医疗记录系统呈现出向以病人为中心的趋势发展,即病人对自己的医疗记录有更多的控制权. 在此模型下,病人将自己的医疗记录存储在云服务器上,通过访问权限的控制有选择地和医生或者其他 3 方医疗机构共享医疗数据. 然而云服务器并不是一个完全可信的第 3 方,Xhafa F 等[9]提出了一个基于云的医疗记录系统,该方案采用基于属性的加密方案应用病人的病症对医疗数据进行加密,而不泄漏对病情的详细描述和医生所在的部门. 方案实际采用的是对称加密方案,其对称密钥采用基于属性的加密方案进行封装. 然而该方案的实现必须依赖一个称之为全局权威(Global Authority,GA)的完全可信的第 3 方负责密钥管理. 它负责发布公共密码参数,为系统中

收稿日期:2017-03-22
基金项目:国家科技支撑计划(2015BAK05B03)资助项目.
作者简介:梅 颖(1973-),男,湖北黄梅人,副教授,博士,主要从事应用密码学、数据安全和隐私保护等方面的研究.
E-mail:178445547@qq.com

的医生生成密钥. 这也是该方案的主要缺点之一.

随着基于比特币的区块链技术得到了广泛的研究和应用,区块链作为一个分布式可验证的公共账本,具有匿名性、分布式、去可信第 3 方等特性,可以作为构建可行计算平台的基础[10]. 本文针对个人医疗记录共享过程中存在的安全和隐私问题,结合区块链技术和云存储技术,提出了一个分布式的个人医疗记录安全存储和共享的方案. 在该方案中,医疗记录由个人所有,其使用权限也由个人控制. 个人既可以共享他们的医疗记录给科研机构,也有能力及时撤销其权限. 有效地实现了个人医疗记录的安全存储和有效使用.

1　区块链技术

1.1　区块链工作原理

区块链是一个分布式的数据结构,它可以在网络成员间复制和共享. 它是比特币底层支撑技术,有效地解决了双花问题[11]. 可以把区块链想象成一个日志,记录被成批地存放在带时间标记的数据块中,每一个数据块使用它的密码哈希进行标识,每个数据块引用其前面产生的数据块的哈希值,这样就创建了一个数据块的链条,称之为区块链(如图 1). 区块链中每个数据块都包含一列交易和一个前一区块的哈希值(有个例外,区块链的第一个区块中不包含这个哈希值,称之为创世块). 网络中的任何节点都可以访问这个有序的、向后链接的数据块列表,读取网络交易数据并计算出网络中所有交易的状态[12].

在区块链网络中,所有节点形成了一个点对点通信网络,通过复制每个节点在同一个区块链上进行操作,其工作过程如下:

1)用户通过一对公钥/私钥对和区块链进行交互[13],公钥作为他们的网络地址,每产生一笔交易,就会用其私钥对交易进行签名,并向它的下一跳节点进行广播. 采用公钥密码可以给网络带来认证、完整性、不可抵赖性等特性;

2)邻居节点收到交易消息后首先验证消息的有效性,如果有效就会继续向其下一跳节点转发,如果无效则直接丢弃. 最终,这些有效的交易将会传播到整个网络;

3)在一定的时间间隔内交易会被网络收集和验证,并排序打包成一个带有时间标记的候选块,这个过程称之为挖矿. 根据网络采用的共识机制,获胜矿工节点会将其候选块广播到网络;

4)网络节点验证矿工提交的候选块,检测块中是否包含有效的交易以及是否通过哈希引用到其链中早先产生的块,如果验证通过则将该块加入到其区块链中,否则丢弃之. 这标志着这轮循环结束.

以上是一个不断重复的过程,每一个规定的时间间隔都会重复一次. 当网络中的每个节点都遵从上述步骤,则他们所操作共享的区块链就会成为一个已验证的具有时间标记的网络活动记录[14].

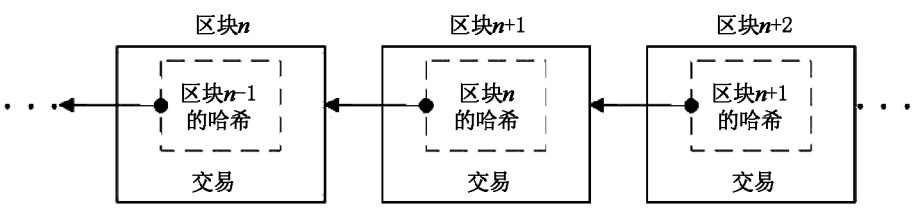

图 1　区块链数据结构

1.2　分布式共识机制

网络节点需要就新挖出的区块里所包含交易的正确性以及它们的顺序达成一致,否则节点的区块链副本可能不一致,最终导致区块链出现分叉. 从而无法保证全网络的节点对网络交易维持一个权威的唯一的时序表. 为了解决这个问题,就需要一个分布式的共识机制.

在理想的场景下,所有的验证节点就下一个区块中所包含交易的顺序进行投票,将遵从大多数的决定. 然而在一个任何人都可以加入的开放的网络环境下,这将是一个灾难,因为极容易遭受女巫攻击[15]:一个单个的实体可以以多个身份加入网络,从而获得多个投票权,导致少数的实体可能获得网络控制权.

比特币通过挖矿计算的昂贵代价来解决这个问题,单个的实体伪装成多个身份无法使其获得更多的投票权,因为每个单个实体的计算资源都是有限的. 而且每个节点都有其自己的候选块,如果它能找到一个正确的随机数(nonce),将它置于候选区块的头部就可以使得该头部的 SHA-256 哈希值是以约定数量的 0 开头[16],任何节点都可以参与解决这个难题的竞赛,生成所谓的工作量证明(proof-of-work,POW),第 1 个解决难题的节点就可以向网络提交候选块. 因为采用的是单向密码哈希函数,网络节点

能够很容易验证给出的答案是否满足要求,如果答案正确就将该区块加入其区块链中.

当 2 个节点几乎同时挖出候选块并传播到网络中时,网络就会出现分叉. 但是这种分叉通常可以在下一块中自动地解决,因为工作量证明机制要求节点应该采用最长的分叉,而且 2 个竞争的分叉同时又生成下一块是不可能的,无论哪个分叉最先变长都将会被网络节点作为正确的分叉而采用. 这样又使得网络达成正确事件顺序的共识.

2 医疗记录安全存储方案

该方案利用区块链技术和链下云存储技术实现医疗记录的安全存储和共享,称之为健康链,其体系结构如图 2 所示. 在健康链中主要有医生、病人和第 3 方机构(如科研机构等)3 类交易主体,医生可以来自不同的医疗机构,负责给病人进行诊断治疗并为病人提供医疗记录,病人可以在不同的医疗机构看病,对个人的医疗记录拥有所有权和支配权,医院及第 3 方机构可以以有偿的方式使用病人的医疗记录. 在健康链中,病人以匿名的方式参加交易,健康链接受 2 种新类型的交易,分别是访问控制和数据存储. 区块链中的信息都是公开的,敏感的个人数据都不会出现在健康链的公共账本中,除了实现一些如价值流通等区块链的基本功能,还可以存储一些个人医疗记录的概要信息. 由于区块链的存储容量受限制,所以个人医疗记录都存放在链下的云存储中,区块链中只保留对该数据在云存储中的引用.

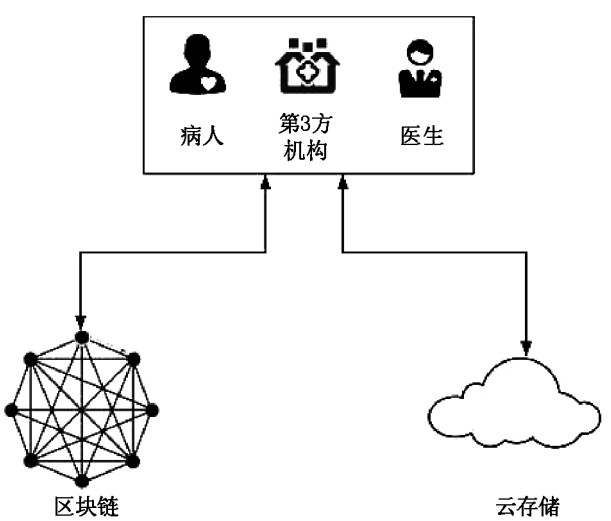

图 2 健康链体系结构

下面按照区块链的基础架构模型(如图 3)给出健康链各层的详细设计.

图 3 区块链的基础架构模型

2.1 数据层

健康链的数据层存储着病人医疗记录的信息摘要和具体数据在云存储中的位置,结构相同的区块通过链式结构形成数据的链条. 系统负责创建创世块,网络节点新产生的区块经过验证后被加入到主链上,形成对交易数据的永久保存. 在健康链中通过时间戳来保证各区块按照时序链接,通过哈希函数来保证数据不被篡改,通过公钥加密实现身份认证,这些技术一起使用保证了健康链的安全.

健康链中的交易通过 Merkle 树进行组织,主要包含访问控制和数据存储 2 种类型的交易. 健康链的交易结构如图 4 所示.

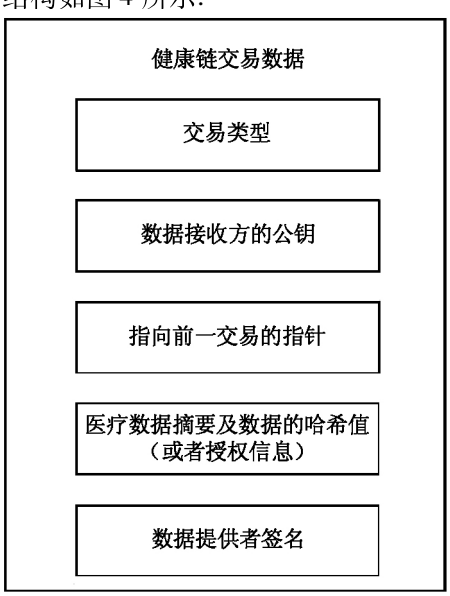

图 4 健康链交易数据结构

在健康链交易中,交易类型由交易类型字段进行识别,用于指示矿工节点使用不同的规则验证交易的有效性. 在数据存储交易中只保存对资源的简要描述等公共数据,而重要的敏感个人医疗记录数据都保存在链下的云存储中,并将其相关记录的引用以及原始数据的哈希值保存在区块链中. 数据在链下云存储中都是以密文保存. 在数据存储的交易中,记录生产者会将病人的医疗记录 M、描述记录的元数据 metadata 以及签名写入到区块链中,如{ M; metadata; Sig(M; metadata)}. 对个人医疗记录的使用权限完全由病人自己控制,病人可以授予某个主体访问相关数据的权限,也可以及时撤销其权限. 在访问控制交易中,数据所有者会将主体对资源的权限写入到区块链中,资源用 URI 表示,主体用数据使用者的公钥 pko 表示,医疗数据解密密钥 k 用访问对象公钥 pko 加密. 然后加上有效期和签名,如:{URI; permission; pko; expiration; Sig(URI; permission; pko); $E_{pko}(k)$}. 当被授予的权限 permission 为空集时,表明撤销其所有权限. 链下云存储会以区块链作为权限管理者,来控制不同用户对数据的访问.

2.2　网络层

健康链网络层的目的是实现网络中各个节点之间的通信,是一个 P2P 网络. 在网络中每个节点都是平等的,每个节点既可以产生信息,也可以接收信息,节点之间通过维护一个共同的账本来保持通信的一致性. 在健康链的网络中每个节点都可以创造新的区块,节点创造新的区块后通过广播的形式向全网传播,收到信息的节点会对接收到的区块信息进行验证,通过验证后继续向网络转发. 网络中的矿工节点根据共识机制进行验证,当这个新区块得到大部分节点认可后,矿工节点就会将此区块加到健康链的主链上.

2.3　共识层

共识层负责提供一种机制让分散的节点在去中心化的环境下就区块的有效性达成共识. 健康链采用工作量证明(POW)机制来保证分布式账本的一致性,其思想是将一个时间间隔内(通常设为 10 min)的交易聚集形成一个新的区块,矿工通过求解复杂的 SHA256 数学难题来竞争记账权,第 1 个求出解的矿工将其创建的区块广播给其他节点,如果大多数用户通过验证,该矿工就获得该区块的挖矿奖励,并将新区块链接到健康链的主链. POW 机制依靠其强大的计算量保证了区块链的安全性.

2.4　激励层

激励层的目的是提供一定的激励机制鼓励节点参与区块链的交易验证工作. 区块链的安全性依赖于众多节点的参与. 由于健康链不是加密货币,所以不能通过挖矿来产生货币,以激励矿工共同维护公共账本的有效性. 在健康链中法币将以代币的形式在链中流通,用于支付交易费. 在健康链中,每笔交易都会产生一定量的交易费,交易费由交易的输入和输出的差值产生,由在挖矿竞赛中获胜的矿工收集,作为挖矿奖励. 在健康链中,采用了比特币的工作量证明机制,每一个固定的时间周期内会产生一个新的区块,每个挖矿周期矿工节点的具体过程如算法 1.

算法 1 挖矿

```
Procedure Mining(健康链)
Input:健康链
Output:更新的健康链
begin
while(时间小于挖矿周期)
收集网络中广播的交易;
    if 交易类型为数据存储
    验证医疗记录发布方的签名的正确性;
    else
    验证资源的有效性和授权方签名的正确性;
    end
    if 交易验证通过
    将交易加入到候选块中;
    else
    丢弃该交易;
    end
end
根据候选块的计算满足哈希要求的随机数;
if 未收到其他节点广播的候选块
    广播自己的候选块,竞争记账权;
else
    验证收到的候选块,并加入到将健康链的主链中;
end
进入下一轮挖矿竞赛;
end.
```

2.5　合约层

健康链合约层继承了比特币区块链的设计,封装了区块链系统的各类脚本代码、算法. 可以利用脚本代码规定交易的方式和各项细节,通过合约层的脚本技术,可以实现延时支付、担保交易以及根据外部信息源触发交易事件等类型的应用.

2.6　应用层

在健康链中,主要是实现病人医疗记录的发布、保存和共享,实现如下 3 个主要功能.

2.6.1　*医疗记录发布*　病人在医院看病或者在医

院等医疗机构做检查时,医生会为该病人产生病历、检查报告等医疗数据(M). 医疗数据产生后,医生会为医疗数据生成哈希,并将医疗记录的摘要(Digest)、哈希用发行方的私钥(sk isser)签名后发布到健康链上. 同时将医疗记录用对称密钥(k)加密,并将加密密钥用病人的公钥(pk patient)加密后一起发送给病人,具体过程如算法 2 描述.

算法 2 医疗记录发布

Procedure Issuing(M)

Input:M

Output:医疗记录交易

begin

医疗数据发行方产生一个医疗记录 M;

生成需要保存在健康链上的数据{Digest; $H(M)$; Sig(Digest| $H(M)$)}并创建数据存储交易广播到网络;

将原始记录和其哈希值签名后用对称密钥加密,将加密密钥用病人的公钥加密,形成消息{ Enc_k(Digest|M|$H(M)$|Sig(Digest|M| $H(M)$)); Enc(k)}后一起发送给病人;

end

2.6.2 医疗记录存储 病人从医疗机构收到了自己的医疗数据后,首先验证机构的签名,然后用自己的私钥解密出医疗数据的加密密钥,并解密出原始医疗数据及其签名,然后生成新的加密密钥将医疗数据及其签名加密存放到云存储中保存,具体过程如算法 3 描述.

算法 3 医疗记录存储

Procedure Storing(M)

Input:加密的医疗记录{ Enc_k(Digest|M|$H(M)$|Sig(Digest|M| H(M))); Enc(k)}

Output:数据存储位置

begin

病人用自己的私钥从 Enc(k)中解密出对称密钥 k;

用对称密钥 k 解密出 Digest、M、$H(M)$、Sig(Digest|M| $H(M)$);

根据发行方的公钥验证签名的正确性;

if 签名正确

根据 M 计算其哈希值并和 $H(M)$ 比较;

if 哈希一致

医疗记录数据真实;

else

简单丢弃处理;

end

else

简单丢弃处理;

end

if 验证数据真实

将是医疗记录及其签名重新加密存储在云存储中,并记录下加密密钥和存储位置;

end

end.

2.6.3 医疗记录共享 病人的医疗数据的使用权限完全由用户自己控制,病人可以通过访问控制交易授权第 3 方访问其部分医疗记录,并可以随时收回权限. 授权时会将共享记录在云存储中的位置、使用权限、使用期限、用第 3 方使用者公钥机密的解密密钥一起写入到区块链中,云存储管理端会以此设置访问控制策略,具体过程如算法 4 描述.

算法 4 医疗记录共享

Procedure Sharing(M)

Input:请求数据方的公钥和所需的医疗记录

Output:生成一个访问控制交易

begin

接收数据请求方请求,提取出请求方公钥和数据需求;

根据请求方的数据需求,查找相关医疗记录在云存储中的位置 URI 和响应的加密密钥 k;

创建一个访问控制交易,并将响应的信息写入到交易中{URI; permission; pko; expiration; Sig(URI; permission; pko); Epko(k)}

向健康链网络广播该交易;

end.

3 安全性分析

该部分对健康链从防篡改、隐私保护和安全存储 3 个方面进行了安全分析,并和方案[9](以下简称 ABE 方案)的安全性进行了一个综合比较.

3.1 防篡改

健康链上的所有信息都是公开不可篡改的,按照一定的时序排列. 健康链的分布式共识机制使信任建立在密码算法的基础之上,无需依赖可信第 3 方. 数据一旦被写入到健康链中就无法被篡改,因为每个区块都保存了其前一个区块的哈希,如果要修改某个区块的数据至少需要全网 51% 以上的算力,这几乎是不可能的事. 健康链中保存了医疗记录的原始数据的哈希,对原始数据的任何改变都会引起其哈希值的改变,所以这也直接保证了医疗记录的不可篡改性.

3.2 隐私保护

病人都是以匿名的方式在区块链上参加交易,用户每次交易都可以产生不同的公私钥对. 公共账本上不包含用户的身份信息,只包含医疗记录的元数据,医疗记录都加密存放在链下的云存储中. 而且对记录的控制权限和控制粒度都掌握在病人手里,病人可以将某个数据对象授权给某个实体,并且可

以随时撤销其访问权限.

医疗机构作为医疗记录的提供方,其身份信息必须是公开的,以保证其权威性和真实性.

其作为医疗记录的生产者可能保留了本机构生产记录的原始数据,这对于病人来说只是其医疗记录的部分信息,是零碎的,不完整的. 而且还需要相关的法律和机制防止医疗机构泄露用户的医疗记录,以保护用户的隐私.

健康链上只保存医疗记录的元数据,记录本身加密保存在链下的云存储结构中,健康链中只保存有密文的位置信息,没有病人的加密密钥是无法解密出医疗记录的明文信息,所以无法从健康链的公开信息中获取任何有关医疗记录的真实数据.

3.3　安全存储

数据的存储安全是健康链的重要特性,在本文的方案中,用户对自己的医疗记录具有所有权,并完全控制它的使用. 从数据的生产到数据的使用过程都是安全的.

1)医疗记录的公共信息(包括医疗记录元数据、加密记录的存储位置、哈希值、存取权限等)都存储在区块链上,公共可见无法篡改.

2)医疗机构作为医疗记录生产方,生成记录后即对记录进行哈希,并对哈希值进行签名,然后用病人的记录和签名用病人的公钥进行加密,并存储在链下的云存储中,并把记录的哈希和位置写入区块链,确保了数据来源的机密性、真实性;云存储的分布式存储特点保证数据存储的安全性;

3)病人收到医疗记录后,用自己的私钥解密密文,获得原始记录的哈希和签名,验证记录的完整性和真实性,并将原始记录采用对称密钥进行加密,并将其归集到自己的医疗记录存储空间. 只有授权用户才可以获得解密密钥,查看真实记录. 敌手即使从存储中获得记录,由于存储的是记录的密文,也无法获得医疗记录的任何真实信息,确保了医疗记录数据的安全.

3.4　健康链和 ABE 方案的安全性比较

ABE 方案是一个新近提出的基于云的电子医疗记录系统,该系统中医疗记录有病人存储在云上,通过采用基于属性的加密方案来实现数据的加密和共享,通过比较本文提出的方案(简称健康链)不依赖可信第 3 方,并对医疗记录具有完全的控制能力. 表 1 是两方案在安全性上的综合比较.

表 1　ABE 方案和健康链的安全性比较

	依赖可信第 3 方	安全存储	隐私保护	防篡改	对医疗记录的控制能力
ABE 方案	√	√	√	√	不完全
健康链	×	√	√	√	完全

4　总结

健康链为病人的医疗记录提供了安全的分布式存储机制,使得病人的医疗记录的所有权归病人所有,并由其控制其使用权限,建立起一个共享的、及时的、准确的和广泛的个人健康数据源. 允许个人、医疗机构和研究机构之间分享医疗信息,例如共享大量的遗传、饮食、生活方式和环境的健康数据,帮助识别和开发新的治疗方式和疾病防治.

区块链的分布式结构另一个优势是内建的错误容忍和灾难恢复机制,数据分布在网络的不同节点上,不存在单点失败,一个灾难不可能同时影响到网络所有的位置. 区块链工作于标准的密码算法和协议,这些技术被大量地分析和接受认为是安全的. 这些都为病人医疗记录的安全存储和共享使用提供了安全保证.

然而健康链中还有许多需要解决的问题,如建立开放的医疗记录标准,保证医疗记录在各机构间的数据兼容性和互操作性,以及设计出合适的多方计算协议,使得数据共享过程不泄露原始数据. 开发基于健康链上的分析工具用于各种分析,包括挖掘影响结果的因子,决定优化的治疗方案,识别影响预防医药的元素,数据和支持交互查询,文本挖掘,文本分析和机器学习这些都是值得研究的方向.

5　参考文献

[1] 庞辉,梁伟,杜剑亮,等. 美国医院电子医疗记录低应用率给中国医院电子医疗记录发展的启示 [J]. 中国病案,2013,(10):11-13.

[2] Sweeney L. K-anonymity: a model for protecting privacy [J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,2002,10(5):557-570.

[3] Machanavajjhala A, Kifer D, Gehrke J, et al. *l*-diversity: privacy beyond *k*-anonymity [J]. ACM Transactions on Knowledge Discovery from Data(TKDD),2007,1(1):3.

[4] Li Nihui, Li Tiangcheng, Venkatasubramanian S. *t*-closeness: Privacy beyond k-anonymity and l-diversity [C].

IEEE 23rd International Conference on IEEE,2007:106-115.

[5] De Montjoye Y A,Hidalgo C A,Verleysen M,et al. Unique in the crowd:the privacy bounds of human mobility [J]. Scientific Reports,2013,3:1376.

[6] Narayanan A,Shmatikov V. How to break anonymity of the netflix prize dataset [EB/OL]. [2017-01-13]. http://smanticscholar. org/5611/6e8ce3f57bec578ac60f6d68333aea5af59e. pdf

[7] Dwork C. Differential privacy [M]us:Springer,2011:338-340.

[8] Gentry C. Fully homomorphic encryption using ideal lattices [J]Acm sysmpoium on computing,2009,9(4):169-178.

[9] Xhafa F,Li Jingwei,Zhao Gansen,et al. Designing cloud-based electronic health record system with attribute-based encryption [J]. Multimedia Tools and Applications,2015,74(10):3441.

[10] Zyskind G,Nathan O. Decentralizing privacy:using blockchain to protect personal data [C]. Security and Privacy Workshops(SPW),IEEE,2015:180-184.

[11] Karame G O,Androulaki E,Capkun S. Double-spending fast payments in bitcoin [C]. Proceedings of the 2012 ACM conference on Computer and communications security,2012:906-917.

[12] Antonopoulos A M. Mastering Bitcoin:unlocking digital cryptocurrencies [M]. Sebastopol O′Reilly Media,Inc,2014.

[13] Christidis K,Devetsikiotis M. Blockchains and smart contracts for the Internet of Things [J]. IEEE Access,2016,4:2292-2303.

[14] Greenspan G. Ending the bitcoin vs blockchain debate [J]. MultiChain blog URL:http://www. multichain. com/blog/2015/07/bitcoin-vs-blockchain-debate,2015.

[15] Douceur J R. The sybil attack [C]. Berlin:Springer Berlin Heidelberg,2002:251-260.

[16] Roe M. Performance of block ciphers and hash functions-one year later [C]. Berlin:Springer Berlin Heidelberg,1994:359-362.

The Utilizing Blockchain-Based Method of the Secure Storage of Medical Records

MEI Ying

(School of Computer,Communication University of China,Beijing 100024,China)

Abstract:The security and privacy preserving of medical information records in medical information system has been addressed. A scheme for secure storage of medical records based on block chain and cloud storage technology has been proposed. It uses block chain to store public information,anonymous identities and access rights of the medical records,and the encrypted real data of the medical records is stored in the off-chain cloud storage structure. It realizes the control of the patient′s ownership and access permission to the personal medical data,and secure storage of sensitive medical data.

Key words:block chain;medical records;secure storage;privacy preserving

(责任编辑:冉小晓)