doi:10.11959/j.issn.1000-436x.2015329

基于 PBAC 模型和 IBE 的医疗数据访问控制方案

张怡婷[1,2]，傅煜川[1]，杨明[1]，罗军舟[1]
(1. 东南大学 计算机科学与工程学院，江苏 南京 210096；2. 南京邮电大学 计算机学院，江苏 南京 210023)

摘 要：医疗卫生领域形成的医疗大数据中包含了大量的个人隐私信息，面临着外部攻击和内部泄密的潜在安全隐患。传统的访问控制模型没有考虑用户访问目的在侧重数据隐私的访问控制中的重要作用，现有的对称、非对称加密技术又都存在密钥管理、证书管理复杂的问题。针对这些问题，提出了综合应用 PBAC 模型和 IBE 加密技术的访问控制方案，支持针对医疗数据密文的灵活访问控制。通过加入条件目的概念对 PBAC 模型进行扩展，实现了对目的树的全覆盖；以病患 ID、条件访问位和预期目的作为 IBE 身份公钥进行病患数据加密，只有通过认证并且访问目的符合预期的用户才能获得相应的私钥和加密数据，从而实现对病患信息的访问。实验结果证明，该方案达到了细粒度访问控制和隐私保护的目的，并具有较好的性能。

关键词：隐私保护；访问控制；基于目的；基于身份加密
中图分类号：TP309 **文献标识码**：A

Access control scheme for medical data based on PBAC and IBE

ZHANG Yi-ting[1,2], FU Yu-chuan[1], YANG Ming[1], LUO Jun-zhou[1]
(1. School of Computer Science and Engineering, Southeast University, Nanjing 210096, China;
2. School of Computer Science & Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: Due to the large amount of personal privacy information contained, the medical big data formed in the health care industry was faced with potential threats of both external attacks and internal data leakages. However, traditional access control technology didn't take into account the important role of user access purpose in the access control schemes that emphasized data privacy, and existing symmetric and asymmetric encryption technologies both face problems such as the complexity of key and certificate management. To address these problems, a novel access control scheme based on PBAC model and IBE encryption technology was proposed, which could provide flexible access control of encrypted medical data. By introducing the concept of conditioned purpose, the PBAC model was extended to achieve full coverage of purpose trees. Furthermore, the scheme used patient ID, conditioned bit and intended purpose as the IBE public key, with which patients' data were encrypted. Only users who pass the authentication and whose access purposes conform to the intended purposes can obtain the corresponding private keys and the encrypted data, thereby achieving access to patients' information. Experimental results prove that the scheme can achieve the goals of fine-grained access control and privacy protection with high performance.

Key words: privacy preserving; access control; purpose based; identity-based encryption

1 引言

随着互联网、云计算和物联网技术的快速发展和普及应用，各个行业和领域都产生了大量的数据，人类社会和科学研究已进入大数据时代。大数据在推动社会发展和文明进步的同时，也带来了突出的安全和隐私问题，面临着数据公开与隐私保护的矛盾[1,2]。尤其是在医疗卫生行业，建立基于云计算技术的区域卫生信息平台已经成为我国各地医疗信息化建设的一个重要组成部分，其基本思路是

收稿日期：2015-03-30；**修回日期**：2015-10-06
基金项目：国家自然科学基金资助项目（61272054, 61320106007）；国家科技支撑计划课题基金资助项目（2010BAI88B03）
Foundation Items: The National Natural Science Foundation of China (61272054, 61320106007); The National Key Technology R&D Program of China (2010BAI88B03)

将区域内各个医疗机构的医疗数据上传并存储到卫生信息平台云端，通过信息数据的集中存储和资源共享，支撑居民电子健康档案、双向转诊、同城互认等医疗业务系统，从而为居民提供更便捷的医疗服务。然而，由于这些医疗数据中包含了大量的个人隐私信息，不可避免会面临巨大的安全隐患。无论是平台外部攻击者的恶意攻击，还是内部管理人员有意或无意的操作，都有可能导致隐私信息的泄露。

为了保护医疗数据的隐私性，一方面需要加强系统的访问控制，另一方面需要对医疗数据进行加密处理。然而传统的访问控制技术没有考虑用户访问目的在侧重数据隐私的访问控制中的重要作用，现有的对称、非对称加密技术又都存在密钥管理或证书管理的难题。因此，如何针对医疗数据隐私保护的实际需求，设计适用的加密和访问控制机制，是亟待解决并且具有重要意义的问题。

针对这个需求，本文提出了综合应用 PBAC 模型和身份加密技术（IBE, identity-based encryption）的访问控制方案，以支持医疗数据密文的灵活访问控制。本文的主要工作包括：1）对 PBAC 模型进行了扩展，加入了条件目的的概念，实现了对目的树的全覆盖。2）以围绕数据的预期目的构造 IBE 身份公钥为核心思路，设计了包括数据的预期目的绑定和加密、用户的角色分配和角色的访问目的权限分配、访问目的匹配和数据解密等核心步骤的综合应用 PBAC、RBAC 模型和 IBE 加密技术的数据访问控制方案。3）从功能和性能 2 个方面进行了访问控制方案的验证，实验结果表明该方案既能对外提供较细粒度的访问控制，又能避免内部人员的信息泄密，并且具有较好的性能。

2　相关工作

2.1　身份加密技术

身份加密技术是由 Adi Shamir[3]最先提出的，其设计目标是使通信双方能够在不交换公钥、不需要保存密钥目录以及不需要第三方认证服务的情况下实现信息的安全交换。在基于身份的密码机制中，依旧需要一个可信第三方，但是与 PKI 中的 CA 用于公钥查询和管理不同，这个可信第三方用于私钥的生成，称为私钥生成中心（PKG, private key generator）。每个合法用户必须持有自己身份的有效证明，才能够向 PKG 申请获取特定身份所对应的私钥。PKG 在系统建立的时候需要确定整个系统的公共参数和主密钥：公共参数由整个系统中所有参与的用户所共有，而主密钥由 PKG 掌握。PKG 利用主密钥，结合用户身份和公共参数，计算出用户的私钥。用户仅需要与 PKG 交互一次就可以获取自己身份所对应的私钥，然后可以离线完成所有的加解密和签名工作，该私钥由用户自己负责保密。

在 Shamir 提出基于身份的密码机制设想后，直到 2001 年才由 Boneh 和 Franklin [4]设计出第一个实用的 IBE 方案（BF-IBE），该方案利用了椭圆曲线上的双线性 Weil 配对，在随机预言模型下具有选择密文安全性。与此同时，Cocks 等[5]提出了基于二次剩余的 IBE 方案，不过该方案的效率明显低于前者。Sakai 和 Kasahara[6]设计了同样利用双线性配对的 IBE 方案（SK-IBE），通过采用基于指数逆（exponent-inversion）的新密钥提取方法提高了算法的性能。Canetti 等[7]在 2003 年提出了一种称为选择身份（selective-ID）的弱安全模型，并在该模型下设计了一个不借助随机预言机的 IBE 方案[8]。该方案虽然在标准模型下是可证明安全的，但是效率较低。因此，Boneh 和 Boyen[9, 10]随后又提出了在选择身份模型下更加实用有效的 IBE 系统，构造了 2 个效率较高的 IBE 方案（BB-IBE），并且进一步提出了一个不依赖随机预言机的完全安全的 IBE 方案[11]。2005 年，Waters[12]简化了文献[11]中的设计，提出了一个更加高效的版本。2006 年，Gentry[13]针对 Boneh 等和 Waters 的 IBE 方案系统参数较长的问题，提出了一个可证明安全的新 IBE 方案，并且该方案具有接收者匿名性。2009 年，Waters[14]提出了双重系统加密（dual system encryption）技术，可用于在简单假设下构造完全安全并具有较短参数的 IBE、分层身份加密[15]（HIBE, hierarchical IBE）方案，并且该技术在后续研究中被用于新构造方案的完全安全性证明。在文献[14]的基础上，2010 年，Lewko 等[16]设计了一种不使用标签的双重系统加密实现技术，并进一步构造了完全安全且具有较短密文长度的 HIBE 方案。此外，针对 IBE 方案中的安全约简和安全损失问题，Chen 等[17]在 2013 年构造了首个标准假设下完全安全的 IBE 方案，其安全损失仅取决于安全参数的设置，而与密钥查询数量无关。

2.2　IBE 扩展及应用

上述研究工作主要是围绕获得更高的安全性

或更高的运行效率展开，而随着对基于身份密码机制研究和应用的不断深入，一些新型 IBE 方案相继被提出。这些方案大多是在 BF-IBE、BB-IBE、SK-IBE 等方案的基础上扩展而来，具体包括 HIBE 分层身份加密机制[15]、抗泄露身份加密技术[18,19] LR-IBE（leakage-resilient IBE）、模糊身份加密技术[20] FIBE（fuzzy IBE）可撤销身份加密技术[21~23] RIBE（revocable IBE）以及 WIBE 支持通配符的身份加密技术[24]（wildcarded IBE）。在 IBE 技术的应用方面，Beato 等[25]针对在线社交网络设计了基于 IBE 技术的用户信息加密方案，并采用分布式密钥生成（DKG）协议来跨 OSN 网络建立和保存主密钥，以避免对单个可信 PKG/OSN 的依赖。Wu 等[26]针对公有云推广应用所面临的用户对数据安全性的顾虑，提出了一种基于 IBE 的代理重签名方案。

无论是 2.1 节分析的 BF-IBE、BB-IBE、SK-IBE 等标准身份加密方案，还是 2.2 节的 HIBE、LR-IBE、FIBE、RIBE、WIBE 等扩展方案，它们的核心思想都是相同的，即数据加密者利用“身份”—通常是用户的邮箱、IP 地址等，作为公钥直接对数据进行加密处理；而在解密阶段，合法用户凭借能够证明自己身份的有效凭证从可信第三方获取私钥从而解密数据。在这过程中，数据的加密和解密操作可以独立进行。从密码学角度，基于身份加密方案中的“身份”可以是任意的字符串，因此采用何种方式组成用户“身份”是 IBE 扩展或应用方案的核心要素。例如，为了适应组织机构层次化的特点，HIBE 方案[15]采用 ID 元组表示用户的身份，ID 元组之间的前缀关系用于反映用户在层次结构上的节点关系，即身份为$(ID_1,\cdots,ID_t)$的用户的祖先节点身份为$(ID_1,\cdots,ID_i)$（$i<t$），并由后者负责私钥的生成；为了使加密数据能够被具有类似属性的一组用户而不是单个用户解密，FIBE 方案[20]选择以用户属性的集合 u 作为身份，该用户可以解密使用身份 u'加密的信息，当且仅当 2 个集合 u 和 u'之间的交集大于一定的阈值；针对在线社交网络面临的用户信息泄露威胁，文献[25]以 OSNName/Username 为身份公钥，对用户在 OSN 网络中存储或者与其他用户分享的隐私信息进行加密等。

上述工作的核心是用户身份的构造，这些身份一方面将作为公钥对数据进行加密，另一方面可以反映用户之间一定的联系。借鉴这些工作，本文将目的作为用户身份，数据的使用者之间可能具有类似的目的，由其角色确定；而数据使用者（解密者）和数据提供者（加密者）之间的关系，则由目的匹配结果确定。

2.3 基于目的的访问控制

基于目的的访问控制（PBAC，purpose based access control）由 Byun 等[27, 28]最先提出，它利用一个全新的概念“目的”作为访问控制的基础，通过定义详细的隐私保护策略实现访问控制。PBAC 一经提出即引起了很大的关注，各国学者针对基于目的的访问控制进行了深入的研究。

Yang 等[29]在 2007 年提出了一个基于目的的访问控制模型，该模型的核心是 2 种类型的目的：预期目的（IP, intended purpose）和访问目的（AP, access purpose）。数据提供者给出数据的预期目的 IP，即希望数据如何被访问的要求，隐私数据只能依据其设置的预期目的进行使用；数据使用者根据自己对数据使用的意愿提出访问目的 AP，只有在 AP 匹配 IP 的前提下，数据才能够被访问。其中 IP 又由 2 个部分组成，即允许目的（AIP, allowed intended purpose）和禁止目的（PIP, prohibited intended purpose），分别表示数据在某个特定访问目的下能够被访问和禁止被访问。

为了同时保证数据的高质量和私密性，在隐私保护的前提下提取出更多有用的信息，Kabir 等[30]提出了一种称为有条件的基于目的的访问控制模型（CPBAC, conditional purpose-based access control）。该模型与 PBAC 模型的最大区别在于其在预期目的 AIP 和 PIP 之外增添了一个新的部分，即 CIP（conditional intended purpose），表示数据访问者在特定的访问目的下只能够有条件地获取数据。同样在模型扩展方面，Wang 等[31]从标准 RBAC 模型出发，引入目的概念，并定义了目的之间的关系以及 RBAC 模型中的 User、Session 等组件与目的的关系，设计了一种涉及目的的基于角色访问控制模型。

此外，如何实现基于 PBAC 模型的访问控制同样也是重要的研究课题，文献[28]针对关系型数据库设计了查询修改技术以实现基于目的的数据过滤；Colombo 等[32]设计了一种采用预过滤和查询重写机制的基于目的的隐私策略实施系统。然而，这些工作都需要对现有的 DBMS 系统进行扩展和改造。针对该问题，本文将基于身份的加密技术和访问控制技术结合起来，设计一种轻量级的医疗数据

密文访问控制系统。Sun 等[33]针对纯 XML 数据库，通过数据标记技术将预期目的与 XML 文档元素关联起来，并进一步结合使用控制模型（usage access control）设计了一种侧重隐私保护的综合访问控制方法。Jafari 等[34]在给出目的的形式化语义描述的基础上，设计了一种用于表述和实施基于目的隐私策略的框架。

3　访问控制模型

3.1　目的符号和定义

本文的研究工作基于 Byun 等提出的基于目的的访问控制模型展开，相关概念和定义可查阅文献[28]，此处仅给出部分符号的说明。

记目的的集合为 P，目的树为 PT。参考文献[35]，可建立如图 1 所示的医疗目的树：目的树中每一个节点表示 P 集合中的一个目的；目的树中的每一条边表示了 2 个目的之间的泛化/特化关系。

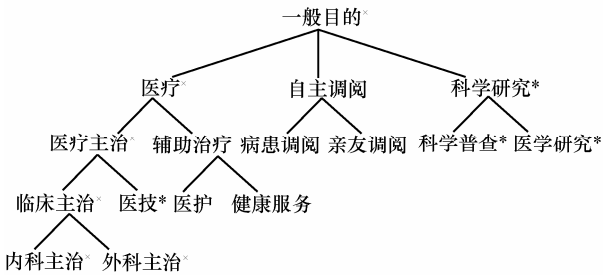


图 1　医疗目的树

假设 R 表示某个目的集合，R 中的节点均在目的树 PT 上。记 $R^{\downarrow}$ 为由 R 中节点本身以及 R 中节点在目的树中所有后代节点所组成的集合；记 $R^{\uparrow}$ 为由 R 中节点本身以及 R 中节点在目的树中所有祖先节点所组成的集合；记 $R^{\updownarrow}$ 是由 R 中节点本身以及 R 中的节点在目的树中所有祖先节点和后代节点组成的集合，即 $R^{\updownarrow} = R^{\uparrow} \cup R^{\downarrow}$。

记 AP 为访问目的，IP 为预期目的，预期目的中的允许目的为 AIP，禁止目的为 PIP。因此，一个预期目的 IP 也可以表示成<AIP, PIP>。

根据上述符号，给出 IP^*和 IP^x 这 2 个集合的定义如下

$$IP^* = AIP^{\downarrow} - PIP^{\updownarrow}$$

$$IP^x = PIP^{\updownarrow}$$

IP^*的意义在于，当数据提供者给出的允许目的 AIP 和禁止目的 PIP 存在冲突时，采用“禁止优先”原则确定实际可访问数据的目的集合，即：当且仅当 $AP \in IP^*$，数据访问者能够获取数据。IP^x 则指出了不能访问数据的目的集合。

综上，给出访问目的匹配的定义如下。

定义 1　访问目的匹配

假设 PT 是一棵目的树，在 PT 上分别有预期目的 IP=<AIP, PIP>和访问目的 AP。如果 $AP \in IP^*$，那么称 AP 与 IP 匹配，记为 $AP \Leftarrow_{PT} IP$，表明在该 AP 下数据访问者能够获取数据。

以图 1 为例，假设数据提供者设定的预期目的 IP=<{医疗主治, 科学研究}, {临床主治}>，则有

$AIP^{\downarrow}$ ={医疗主治, 临床主治, 内科主治, 外科主治, 医技, 科学研究, 科学普查, 医学研究}

$IP^x = PIP^{\updownarrow}$ ={临床主治, 内科主治, 外科主治, 医疗主治, 医疗, 一般目的}

$IP^* = AIP^{\downarrow} - PIP^{\updownarrow}$ ={医技, 科学研究, 科学普查, 医学研究}

那么当且仅当 $AP \in$ {医技, 科学研究, 科学普查, 医学研究}，数据访问者能够获取到数据。

3.2　条件目的的集合

由上节的例子可以看到，PBAC 模型目的树中的目的被分割成了 3 部分——IP^*、IP^x 和未分类目的。IP^*是数据提供者指定可以访问数据的目的集合，IP^x 是禁止访问数据的目的集合，未分类目的则表示数据提供者未做指定。然而，设计一个完整的访问控制方案，需要明确给出对这些未分类目的的处理方法，而同样的问题亦存在于 CPBAC 模型。为此，结合医疗数据访问控制的具体需求，本文定义了如下的新的目的集合。

定义 2　条件目的的集合 IP^+

假设 PT 是一棵目的树，目的树上的目的集合用 P 表示，那么 $IP^+ = P - IP^* - IP^x$。

此处的“条件”与文献[30]中的定义类似，即在数据发布前需要对原始数据进行匿名化处理，使数据访问者在访问数据时能够保证用户隐私。表 1 的例子展现了访问目的在属于不同目的的集合时，数据访问者能够访问到的数据。

表 1　　**不同 AP 访问得到的数据**

访问目的	姓名	年龄	常用住址	电话号码
$AP \in IP^*$	李刚	28	南京市江宁区东南大学路 2 号	138 12345678
$AP \in IP^+$	李	20~30	南京市江宁区	138
$AP \in IP^x$	—	—	—	—

假设数据提供者已经提供了某数据记录的预期目的，并且 IP^*、IP^+、IP^x 都已计算出来。当数据访问者给出访问目的 *AP*，根据 *AP* 所属的集合，从表 1 可以看到：当 $AP \in IP^*$ 时，数据访问者获取了完整的记录信息；当 $AP \in IP^+$ 时，数据访问者有条件地获取了数据；而当 $AP \in IP^x$ 时，数据访问者不能够获取该条记录的任何信息。

3.3 基于角色和目的的访问控制

PBAC 模型通常会和 RBAC 模型结合应用[36]，如图 2 所示，简记为 RPBAC（role and purpose based access control）模型，其核心内容简要描述如下。

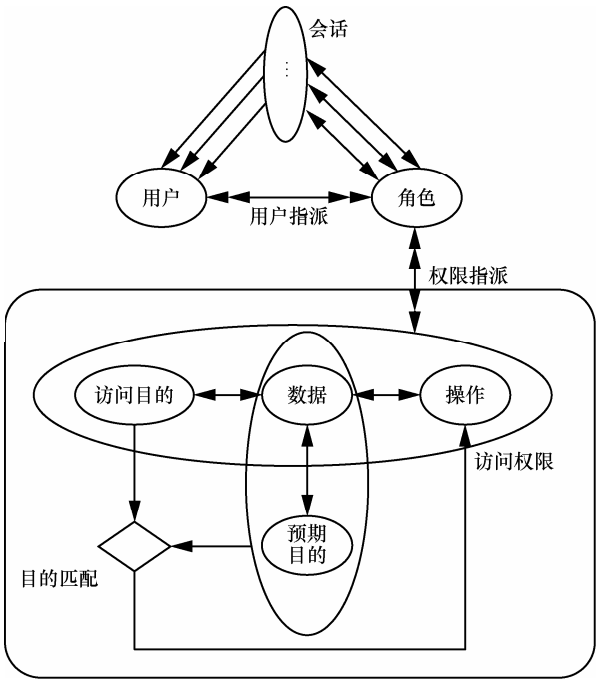


图 2 RPBAC 访问控制模型

1) 从数据提供者的角度而言，主要涉及预期目的绑定（purpose binding）*DIP*: $Data \rightarrow IP$，即建立数据和预期目的 $IP = <AIP, PIP>$ 之间的关联。

2) 从数据访问者的角度而言，涉及如下概念。

① 用户角色分配（user role assignment）

$UA \subseteq User \times Role$，表示用户和角色之间的多对多映射关系。

② 访问目的权限分配（access purpose permission assignment）

$APPA \subseteq Role \times APP$，表示角色和访问目的权限 *APP*（access purpose permission）之间的多对多映射关系。

其中，*APP* 表示所有访问目的权限的集合，可描述为三元组 $\{<ap, d, op> | ap \in AP, d \in Data, op \in Operation\}$，*AP*、*Data*、*Operation* 分别代表了访问目的、数据和操作的集合。

3) 对于访问控制系统而言，主要涉及目的匹配（purpose compliance）

$PC \subseteq APP \bowtie DIP$，表示访问目的权限与数据及其预期目的之间的一对一关系。

针对数据 *d*，访问目的权限 *APP* 中的访问目的 *ap* 和预期目的绑定 *DIP* 中的预期目的 *ip* 进行匹配运算，从而确定访问目的权限中的操作 *op*。

4 基于 IBE 的访问控制方案

本文基于 PBAC 模型和 IBE 加密技术，并借鉴 FIBE[20]以用户属性为身份公钥等工作的思路，设计了一种针对医疗数据密文的访问控制方案，其核心思想是围绕数据的预期目的构造身份公钥。方案的具体流程如下。

1) 采集病患数据，由病患本人自主设定预期目的 *IP*，系统基于病患身份号 *PID*、条件获取位 *CondBit*（0 表示完全获取信息，1 表示条件获取信息）和 *IP* 构造公钥，并使用 IBE 算法加密数据及数据的泛化版本，存储 2 个版本的加密数据至数据平台。

2) 用户（如医生）成功登录系统（亦充当私钥生成中心 PKG）后，系统自动根据用户选择的身份确定其角色，从而判断访问目的 *AP*。

3) 系统（PKG）根据 *AP* 和 *IP*，判断用户能否访问该病患的数据以及访问哪个版本的数据，返回相应数据及其对应私钥。

4) 用户使用私钥解密数据，从而调阅到病患信息或其泛化版本。

根据第 2 节相关工作分析可以看到，目前大部分 IBE 研究工作都是针对 BF-IBE[4]、SK-IBE[6]、BB-IBE[9,11]等在密码学安全性、方案性能或者适用性等方面的变形和扩展。这三者相比较，BF-IBE 方案是首个实用的身份加密方案，在随机预言模型下具有选择密文安全性；SK-IBE 同样利用双线性对工具，但在私钥提取算法方面有所区别，通过将身份映射为 Z_q^* 中的一个元素而非椭圆曲线上的一个点，在一定程度上提高了性能，并且保持了随机预言模型下的选择密文安全性；BB-IBE[9]选择采用了一个较弱的攻击模型，即选择安全攻击模型，但其安全性不依赖于随机预言机；BB-IBE[11]虽然是完全安全的 IBE 方案，但是其效率低，并不适于实际

使用。由于 BF-IBE 是安全性可以接受的首个实用的 IBE 方案，在学术界得到了普遍的关注，并且其实现流程被纳入了 IETF 标准[注1]中，本文采用 BF-IBE 方案实现基于身份的加密工作。

下面结合 IBE 形式化定义所涉及的系统建立 *Setup*、私钥提取 *Extract*、加密 *Encryption*、解密 *Decryption* 4 个算法[4]，对医疗数据访问控制方案进行具体设计，该方案由系统准备、数据提供、目的匹配以及数据获取等阶段构成。

1) 系统准备阶段

系统准备阶段是为实现医疗数据的访问控制所进行的准备工作，主要包括 3 个方面：基于身份的加密准备、目的树表的建立以及角色集合的建立。

① 基于身份的加密准备：生成 IBE 方案的公共参数和主密钥。本文采用 BF-IBE 方案实现基于身份的加密工作，在 BF-IBE 方案的系统建立阶段，给定一个安全参数 p 进行如下工作。

步骤 1　输入安全参数 $p\in Z^+$，生成大素数 q 和 2 个 q 阶群 G_1 和 G_2，G_1 和 G_2 之间存在一个双线性映射关系 e：$G_1\times G_1\to G_2$。挑选一个随机生成元 $g\in G_1$。

步骤 2　随机挑选主密钥 $s\in Z_q^*$，计算 $P_{\text{pub}}=sg$。

步骤 3　选择散列函数 H_1: $\{0,1\}^*\to G_1$，H_2: $G_2\to\{0,1\}^n$，H_3: $\{0,1\}^n\times\{0,1\}^n\to Z_q^*$，$H_4$: $\{0,1\}^n\to\{0,1\}^n$。

由上述步骤可知，明文空间为 $\{0,1\}^n$，密文空间为 $G_1\times\{0,1\}^*$；系统的主密钥是 s，公共参数 $params=<q, g, P_{\text{pub}}, H_1, H_2, H_3, H_4, n>$。

② 目的树表的建立：根据需求建立目的树和目的树表，具体过程如下。

步骤 1　系统根据医疗业务的实际需求确定目的集合 P，再根据 P 中目的之间的关系建立目的树 PT。

步骤 2　根据目的树 PT 建立目的树表，典型的目的树表由 6 个字段构成[28]，如表 2 所示。

表 2　　**目的树表结构**

标识 *id*	目的名 *name*	父节点标识 *parent*	目的编码 *code*	允许目的编码 *aip_code*	禁止目的编码 *pip_code*

标识：每个目的在目的树中的唯一编号，由对目的树的广度优先遍历顺序确定，从 1 开始编号。

目的名：目的的名称。

父节点标识：该目的在目的树中的父节点的编号。

目的编码：该目的位串形式的十六进制编码。编码算法如算法 1 所示，其基本思路是用 1 个二进制位表示目的树中的一个目的。

允许目的编码（*aip_code*）：当该目的为允许目的时计算出的 $AIP^{\downarrow}$ 编码值。假设目的为 p，那么 p 在树中所有后代节点和 p 本身构成一个集合，该集合中所有目的的编码 *code* 相加，得到的结果即 *aip_code*。

禁止目的编码（*pip_code*）：当该目的为禁止目的时计算出的 $PIP^{\updownarrow}$ 编码值。假设目的为 p，p 在树中所有祖先节点和后代节点以及 p 本身构成了一个集合，将集合中的所有目的的编码相加得到结果作为 *pip_code*。

③ 角色集合的建立：根据需求建立角色表，分析并设定相应的访问目的。

算法 1　目的树表构建算法

输入：n 个节点的目的树 PT

输出：数组 p: array[1,…,n] of struct{ *id*, *name*, *parent*, *code*, *aip_code*, *pip_code*}

步骤：

1) // 阶段 1　basic information collection

2) Assign 1 to variable *id*

3) FOR each *node* in *PT* according to breadth-first order

4)　Assign *id* to *p*[*id*].*id*

5)　Assign the name of current *node* to *p*[*id*].*name*

6)　Assign current *node*'s parent ID to *p*[*id*].*parent*, 0 if its parent dose not exist

7)　Increment *id* by 1

8) END

9)

10) // 阶段 2　*code* computation

11) Assign 1 to variable *code*

12) FOR *id* = *n* to 1

13)　Assign *code* to *p*[*id*].*code*

14)　Bitwise left shift *code* by 1

15) END

16)

17) //阶段 3　*aip_code* computation

18) FOR *id* = 1 to *n*

注1　http://tools.ietf.org/html/rfc5091

19)　Define *nodeset* as empty set
20)　Add *p*[*id*] to *nodeset*
21)　REPEAT
22)　　Expand *nodeset* with children of each node in *nodeset*
23)　UNTIL *nodeset* keep unchanged
24)
25)　Assign 0 to variable *aip_code*
26)　FOR each *node* in *nodeset*
27)　　Add *node.code* to *aip_code*
28)　END
29)　Assign *aip_code* to *p*[*id*].*aip_code*
30) END
31)
32) // 阶段 4　*pip_code* computation
33) FOR *id* = 1 to *n*
34)　Define *nodeset* as empty set
35)　Add *p*[*id*] to *nodeset*
36)　REPEAT
37)　　Expand *nodeset* with parent & children of each node in *nodeset*
38)　UNTIL *nodeset* keep unchanged
39)
40)　Assign 0 to variable *pip_code*
41)　FOR each *node* in *nodeset*
42)　　Add *node.code* to *pip_code*
43)　END
44)　Assign *pip_code* to *p*[*id*].*pip_code*
45) END

2) 数据提供阶段

数据提供阶段的流程如图 3 所示，主要包括以下 4 步工作。

① 采集病患信息并对其进行预处理，形成原始数据和泛化数据 2 个版本；

② 病患根据自己的意向设置这些数据的预期目的 *IP*；

③ 系统将病患身份号 *PID*（31 bit 的全局唯一数串）、条件获取位 *CondBit*（0 表示原始数据，1 表示泛化数据）和预期目的 *IP* 编码进行拼接，得到 IBE 加密的公钥；

④ 对原始数据、泛化数据 2 个版本的数据信息分别使用不同 *CondBit* 位的公钥进行加密，并保存到数据平台中。

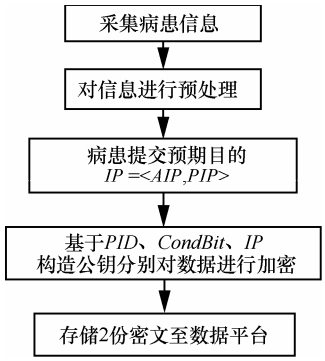


图 3　数据提供流程

数据提供阶段的核心操作是对病患信息进行基于 IBE 的加密，具体操作如下。

步骤 1　对于预期目的 $IP=<AIP, PIP>$，假设 $AIP=\{aip_1, aip_2, \cdots, aip_m\}$，$PIP=\{pip_1, pip_2, \cdots, pip_n\}$。对 *AIP* 和 *PIP* 中的目的查询目的树表，分别获得 aip_i 对应的 *aip_code* 和 pip_i 对应的 *pip_code*。如下计算 *AIP_code* 和 *PIP_code*，其中计算式中的 | 表示按位或。

$$AIP\_code = aip\_code_1 \mid aip\_code_2 \mid \cdots \mid aip\_code_m$$

$$PIP\_code = pip\_code_1 \mid pip\_code_2 \mid \cdots \mid pip\_code_n$$

步骤 2　针对 *CondBit* = 0 和 1 这 2 种情况，分别建立公钥。

$$pub0 = PID + \text{‘0’} + AIP\_code + PIP\_code$$

$$pub1 = PID + \text{‘1’} + AIP\_code + PIP\_code$$

这里的“+”为连接符号。由于公钥中包含了病患的身份信息，因此每个公钥都对应了一个特定的病患及其设置的特定的预期目的；系统用户只有拥有针对该病患信息的访问权限，并且访问目的符合预期目的才能获取私钥并解密该病患的信息。

针对公钥 *pub*0/原始数据 d_0 和公钥 *pub*1/泛化数据 d_1 分别进行后续步骤。

步骤 3　将公钥 *pub* 映射到群 G_1 的一个点上，得到 $Q_{\text{pub}}=H_1(pub)$。

步骤 4　选择一个随机数 $\sigma \in \{0, 1\}^n$。

步骤 5　计算得到 $r=H_3(\sigma, d)$，其中 *d* 表示要被加密的数据，$d \in M$。

步骤 6　计算得到密文 $C=<U, V, W>$，$U=rg$，$V=\sigma \oplus H_2(g_{\text{pub}}^r)$，$W=d \oplus H_4(\sigma)$，其中 $g_{\text{pub}}^r = e(Q_{\text{pub}}, P_{\text{pub}})$。

3) 目的匹配阶段

目的匹配阶段的流程如图 4 所示，主要包括 3 步工作。

① 在用户（如医生、护士、卫生管理人员等）

成功登录系统后，系统首先判断该用户角色是否有访问权限，并根据用户所进行的医疗活动生成用户的访问目的 *ap*。

② 判断该访问目的 *ap* 是否符合数据提供者（即病患）所设立的预期目的 *IP*。

③ 根据目的匹配的结果，判断用户能否获得加密数据，并将相应版本的数据密文返回给用户。

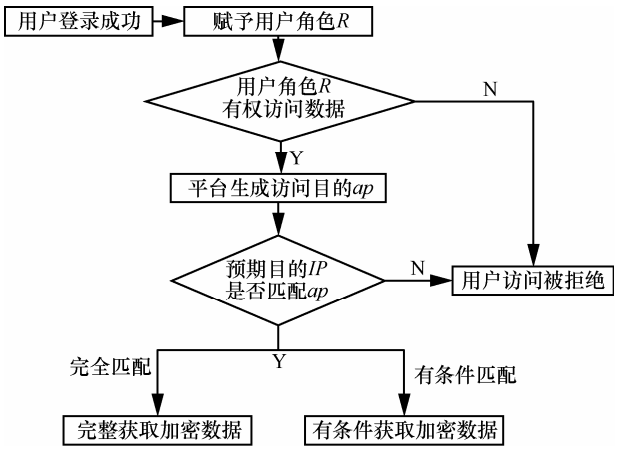


图 4　目的匹配流程

这个过程中的核心步骤是目的匹配，需要判断用户是能够完全获取数据、有条件获取数据还是禁止获取数据。目的匹配算法形式化描述如下。

算法 2　目的匹配算法

输入：预期目的 $IP=<AIP, PIP>$，访问目的 *ap*

输出：*result*: enum{Permit, CondPermit, Deny}

步骤：

1) Assign the code of *AIP* to variable *AIP_code*

2) Assign the code of *PIP* to variable *PIP_code*

3) Assign the code of *ap* to variable *ap_code*

4) Denote the code of *IP** as IP^*_code, the code of IP^+ as IP^+_code

5) Assign *PIP_code* to IP^x_code // $IP^x = PIP^{\updownarrow}$

6)

7) //阶段 1　Compute IP^*_code ($IP^* = AIP^{\downarrow} - PIP^{\updownarrow}$)

8) Assign *AIP_code* to IP^*_code

9) FOR each *bit* of *PIP_code*

10)　IF *bit* equals to 1

11)　　Set corresponding bit of IP^*_code to 0

12)　END

13) END

14)

15) //阶段 2　Compute IP^+_code ($IP^+ = P - IP^* - IP^x$)

16) Sum the code of all purposes to variable IP^+_code

17) FOR each *bit* of IP^*_code

18)　IF *bit* equals to 1

19)　　Set corresponding bit of IP^+_code to 0

20)　END

21) END

22) FOR each *bit* of IP^x_code

23)　IF *bit* equals to 1

24)　　Set corresponding bit of IP^+_code to 0

25)　END

26) END

27)

28) //阶段 3　Match *ap* with *IP**, IP^+ and IP^x

29) IF *ap_code* & IP^*_code not equal to 0

30)　*result* = Permit

31) ELSEIF *ap_code* & IP^+_code not equal to 0

32)　*result* = CondPermit

33) ELSE

34)　*result* = DENY

35) END

4) 数据获取阶段

该阶段主要包括 2 步工作。

① 用户向系统（PKG）申请私钥，该过程与目的匹配阶段步骤类似（可同步处理），系统同样需要根据用户角色判断其 *AP*，并根据 *AP* 和 *IP* 匹配结果确定是否返回私钥以及哪个版本的私钥（*CondBit* = 0 或 1）。

② 用户利用获得的私钥对目的匹配阶段获取的医疗数据密文进行解密处理，最终获取数据明文。

5　方案的验证

5.1　功能测试

为了更好地说明流程，并对正确性进行验证，本文对所提方案进行了实现和测试。实验环境如下。

硬件环境：Intel Core i7-3770 3.40 GHz CPU；4GB 内存；Win7 x64 系统类型。

软件环境：JDK SE 1.8.0_11-b12 开发环境；MySql 5.6 数据库；Jpair 1.03 开发包、MySql JDBC 驱动。

下面对方案中的重要环节进行说明和验证。

1) 目的树表的建立

本文采用如图 5 所示的医疗目的树进行实验，根据算法 1 得到表 3 所示的目的树。

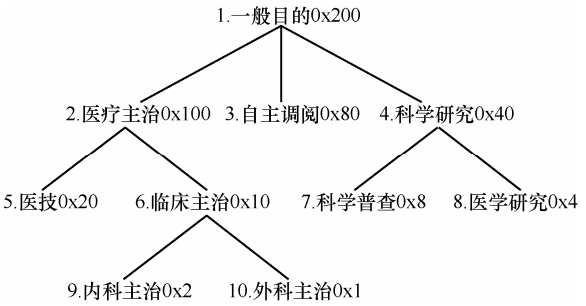


图 5　实验目的树

以“临床主治”目的为例，根据广度优先遍历顺序，该目的为所有 10 个目的中的倒数第 5 个，因此，有

code(临床主治) = $(0000010000)_2$ = 0x10

aip_code(临床主治) = *code*(临床主治) + *code*(内科主治) + *code*(外科主治) = 0x13

pip_code(临床主治) = *code*(临床主治) + *code*(内科主治) + *code*(外科主治) + *code*(医疗主治) + *code*(一般目的) = 0x313

表 3　　**实验目的树表**

id	*name*	*parent*	*code*	*aip_code*	*pip_code*
1	一般目的	0	0x200	0x3FF	0x3FF
2	医疗主治	1	0x100	0x133	0x333
3	自主调阅	1	0x080	0x080	0x280
4	科学研究	1	0x040	0x04C	0x24C
5	医技	2	0x020	0x020	0x320
6	临床主治	2	0x010	0x013	0x313
7	科学普查	4	0x008	0x008	0x248
8	医学研究	4	0x004	0x004	0x244
9	内科主治	6	0x002	0x002	0x312
10	外科主治	6	0x001	0x001	0x311

2) 医疗数据的提供

在实验中，假设采集到的病患信息如表 4 所示。同时假设 *PID*=120= $(1111000)_2$，为简化实验这里病患 ID 仅取为 7 位二进制数。

表 4　　**病患信息**

数据类型	姓名	年龄	常用住址	电话号码
原始数据	李刚	28~28	南京市江宁区东南大学路 2 号	138 12345678
泛化数据	李	20~30	南京市江宁区	138

假设病患设定的预期目的 *IP* = <{临床主治, 自主调阅}, {医学研究}>，因此有

AIP_code

= *aip_code*(临床主治) | *aip_code*(自主调阅)

= $(0010010011)_2$，该值对应于预期允许目的{临床主治, 内科主治, 外科主治, 自主调阅}

PIP_code

= *pip_code*(医学研究)

= $(1001000100)_2$，对应于预期禁止目的{医学研究，科学研究, 一般目的}

进一步，可以得到 2 个公钥

*pub*0 = *PID* + ‘0’ + *AIP_code* + *PIP_code*

= ‘1111000’+‘0’+‘0010010011’+ ‘1001000100’

= ‘11110000001001001110010001000’

*pub*1 = *PID* + ‘1’ + *AIP_code* + *PIP_code*

= ‘11110001001001001110010001000’

公钥的这 2 个二进制位串的第一个字节为 7 位 *PID* 和 1 位 *CondBit*，后续字节为 2 个等长位数的 *AIP_code* 和 *PIP_code*。

3) 基于身份的加密

本文采用 JPair 开发包[注2]实现基于身份的加密。在 IBE 方案的准备阶段，系统利用一个随机数生成随机生成元 g、系统主密钥 s 和系统公共参数 P_{pub}，这里采用的双线性对是修正的 Weil 配对。

下面分别用 *pub*0 和 *pub*1 对表 4 中原始数据和泛化数据进行 IBE 加密。这里假设仅对“常用住址”字段中的数据进行加密，分别得到“南京市江宁区东南大学路 2 号”和泛化信息“南京市江宁区”对应的 IBE 密文 *c*=<*U*, *V*, *W*>三元组。

身份 ID：11110000001001001110010001000

明文原始信息：南京市江宁区东南大学路 2 号

密文信息：*U*1, *V*1, *W*1 [数据略]

身份 ID：11110001001001001110010001000

明文泛化信息：南京市江宁区

密文信息：*U*2, *V*2, *W*2 [数据略]

4) 访问目的的匹配

用户在调阅病患信息时由系统根据其角色生成访问目的，并执行目的匹配算法将访问目的与预期目的进行匹配。根据之前设定，*AIP_code* = 0x093 = $(0010010011)_2$、*PIP_code* = 0x244 = $(1001000100)_2$，由目的匹配算法计算可得

注 2　http://jpair.sourceforge.net/

IP^{x}_code = 0x244 = $(1001000100)_2$

IP^{*}_code = $(0010010011)_2$ = 0x093

IP^{+}_code = $(0100101000)_2$ = 0x128

① 当用户访问目的 *ap* = 内科主治，则 *ap_code* = 0x002，有 *ap_code* & IP^{*}_code = 0x2 & 0x93 = 0x2，因此匹配结果为：Permit；

② 当用户访问目的 *ap* = 医疗主治，则 *ap_code* = 0x100，有 *ap_code* & IP^{*}_code = 0x100 & 0x93 = 0 且 *ap_code* & IP^{+}_code = 0x100 & 0x128 = 0x100，因此匹配结果为：CondPermit；

③ 当用户访问目的 *ap* = 科学研究，则 *ap_code* = 0x040，有 *ap_code* & IP^{*}_code = 0x40 & 0x93 = 0, *ap_code* & IP^{+}_code = 0x40 & 0x128 = 0 且 *ap_code* & IP^{x}_code = 0x40& 0x244 = 0x40，因此匹配结果为：Deny。

5) 医疗数据密文的解密

如果访问目的匹配结果是 Permit，那么系统将原始医疗数据密文和 *pub*0 对应的私钥返回给用户；如果访问目的匹配结果是 CondPermit，那么系统将泛化医疗数据密文和 *pub*1 对应的私钥返回给用户。用户私钥及使用私钥解密得到的数据如下。

身份 ID: 11110000001001001111001000100

用户私钥：5800835224365257912396868885463974299165404088 46…

解密后的数据：南京市江宁区东南大学路 2 号

身份 ID：11110001001001001111001000100

用户私钥：7022930669934333518809816991088471922241883672 24…

解密后的数据：南京市江宁区

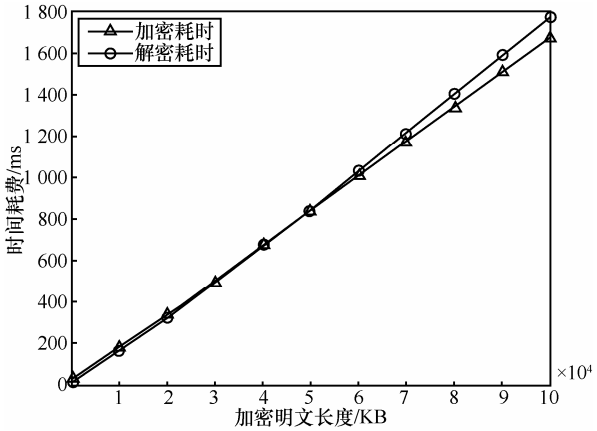
由上述测试结果可知，系统根据用户角色正确地返回了相应的私钥和加密数据，并且加密数据的解密也正常执行。

5.2　性能测试

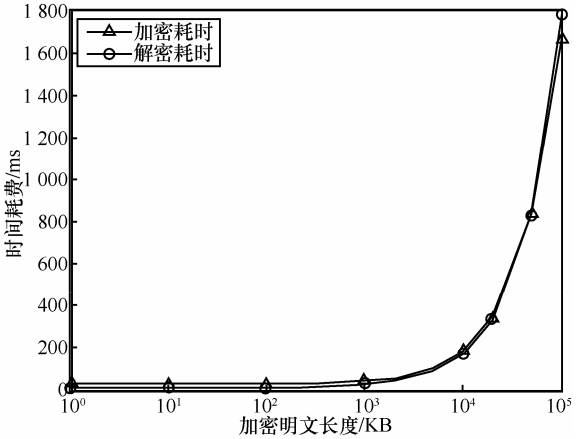
整个系统的性能主要取决于 IBE 算法的效率，因此本文针对方案中 IBE 加、解密操作进行性能测试。实验选择使用 Jpair 预定义对，加密的公钥设定为“11110000001001001111001000100”。

在该设置下，本文测试了在不同数据量明文情况下加、解密分别所需要的运算时间，明文长度分别设定为 1 KB、20 KB、50 KB、100 KB、200 KB、500 KB、1 000 KB、2 000 KB、5 000 KB、10 000 KB、20 000 KB、50 000 KB 和 100 000 KB 共 13 种情况。针对每个长度的明文，各进行 1 000 次实验。为了避免数据内容对加、解密性能测试的影响，每次实验时均完全随机地产生二进制明文数据，然后对其进行先加密、后解密的操作，分别统计 2 个操作的用时，取平均值作为最终测试结果。

为了更好地展现实验结果，分别给出普通坐标和半对数坐标的性能测试结果。由图 6 可知，系统在数据量较小（≤100 KB）时，加/解密时间耗费基本保持不变，分别在 27 ms/17 ms 左右；随着数据量变大，时间耗费基本呈线性增长。



(a) 性能测试结果



(b) 性能测试结果(半对数坐标)

图 6　系统性能测试结果

通过实验发现，由于一些基本运算带来的时间消耗，加、解密 10 byte 数据、1 KB 数据和 100 KB 数据的耗时都是非常接近的。为了判断能取得较好时间效率的明文数据块的大小，本文分析了不同数据量情况下单位长度（KB）数据加、解密的平均耗时。如图 7 所示，数据量在 500 KB/200 KB 后加/解密耗时值的数量级保持不变；而当达到 20 000 KB 后该指标基本保持稳定。因此，本

文在设计系统时将数据尽量打包为 200 KB 以上再进行操作。

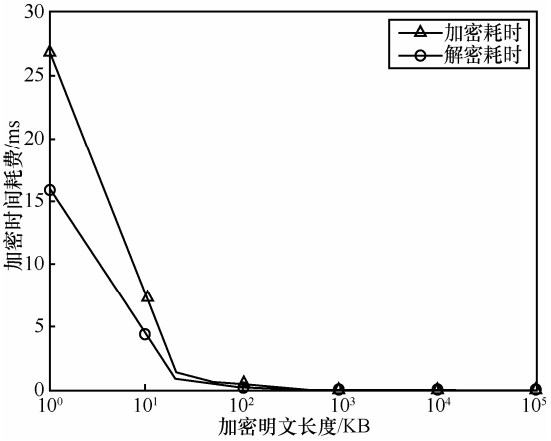


图 7 单位长度数据加解密耗时

此外，由上述实验也可以发现，当加解密大数据时，所需的时间耗费还是非常可观的，例如解密 100 000 KB 的数据需要耗时 1.777 s。由于通常医学影像文件都很大，针对这种情况，系统在 IBE 加密的数据中嵌入 AES、3DES 等对称加密密钥，再使用该密钥加密目标医学影像文件，可以取得较好的性能结果。

5.3 正确性分析

本文提出的访问控制方案是对基于目的访问控制和身份加密机制的一种综合应用，主要包含目的树表构建算法、目的匹配算法和 IBE 加密方案 3 个核心部分，下面依次分析其正确性或安全性。

1) 根据目的树表的定义，算法 1 首先在阶段 1 从根节点出发对目的树上的所有目的进行广度优先搜索并编号；随后在阶段 2，从编号最大的叶节点开始逆序进行目的编码，使目的树中的每一个目的都对应二进制位串上的 1 个比特位；在阶段 3，针对目的树中的每个节点，通过递归计算，将其本身和其所有后代节点均加入到初值为空的节点集合中，并进一步通过累加该集合中的节点编码获得该节点的允许目的编码；在阶段 4，同样针对目的树中的每个节点，通过递归计算，将其本身和其所有祖先节点、后代节点均加入到初值为空的节点集合中，并进一步通过累加该集合中的节点编码获得该节点的禁止目的编码。上述过程中，阶段 3 和阶段 4 是核心计算步骤，由于目的树上节点数有限，因此其中的递归计算必然能执行结束得到结果。并且这些计算步骤符合目的树表的定义[28]，正确性可以得到证明。

2) 在目的匹配算法中，阶段 1 和阶段 2 分别根据允许访问目的集合、禁止访问目的集合和条件目的集合的定义计算对应的目的编码；由定义 2，3 个目的集合相互没有交集并且实现了对目的树的全覆盖，所以在阶段 3 依据定义 1 进行访问目的匹配时，算法 2 必然返回 Permit、CondPermit 或者 Deny 结果之一。

3) IBE 加密以围绕目的树表构建算法计算获得的<*AIP*, *PIP*>预期目的编码构造的身份公钥为输入，在方案设计时并不依赖于特定的 IBE 技术。在实验中，采用 BF-IBE 方案实现基于身份的加密，该方案利用 BDH 假设，在随机预言模型下具有密文安全性[4]。具体实现时采用的 JPair 预定义修正 Weil 配对中的群 G_1 的阶为 160 bit，可以提供 1 024 bit RSA 加密的安全强度，能够保证普通用户的医疗数据的私密性，而更高的安全性可以通过使用自定义配对来获得。

6 结束语

本文针对医疗卫生领域形成的医疗大数据隐私保护的需求，设计了综合应用 PBAC 模型和 IBE 加密技术的访问控制方案。该方案对 PBAC 模型进行了扩展，并选择以病患 ID、条件访问位和预期目的作为 IBE 身份公钥对病患数据进行加密，可以有效保证只有在通过认证并且访问目的符合预期目的的前提下，系统用户才能访问病患信息。实验结果表明，该系统既能对外提供较细粒度的访问控制，又能避免内部人员的信息泄密，并且具有较好的性能。

参考文献：

[1] 孟小峰, 慈祥. 大数据管理: 概念、技术与挑战[J]. 计算机研究与发展, 2013, 50(1): 146-169.
MENG X F, CI X. Big data management: concepts, techniques and challenges[J]. Journal of Compute Research and Development, 2013, 50(1): 146-169.

[2] 冯登国, 张敏, 李昊. 大数据安全与隐私保护[J]. 计算机学报, 2014, 37(1): 246-258.
FENG D G, ZHANG M, LI H. Big data security and privacy protection[J]. Chinese Journal of Computers, 2014, 37(1): 246-258.

[3] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Proc of CYPTO'84[C]. Springer Berlin Heidelberg, 1985. 47-53.

[4] BONEH D, FRANKLIN M. Identity based encryption from the Weil pairing[A]. Proc of CRYPTO'01[C]. Springer Berlin Heidelberg, 2001. 213-229.

[5] COCKS C. An identity based encryption scheme based on quadratic residues[A]. Proc of Cryptography and Coding[C]. Springer Berlin Heidelberg, 2001. 360-363.

[6] SAKAI R, KASAHARA M. ID based cryptosystems with pairing on elliptic curve[J]. IACR Cryptology ePrint Archive, 2003, 03/54.

[7] CANETTI R, HALEVI S, KATZ J. A forward-secure public-key encryption scheme[A]. Proc of EUROCRYPT'03[C]. Springer Berlin Heidelberg, 2003. 255-271.

[8] CANETTI R, HALEVI S, KATZ J. Chosen-ciphertext security from identity-based encryption[A]. Proc of Cryptoloty-EUROCRYPT'04[C]. Springer Berlin Heidelberg, 2004. 207-222.
[9] BONEH D, BOYEN X. Efficient selective-ID secure identity-based encryption without random Oracle[A]. Proc of Cryptoloty-EUROCRYPT'04[C]. Springer Berlin Heidelberg, 2004. 223-238.
[10] BONEH D, BOYEN X. Efficient selective identity-based encryption without random oracles[J]. Journal of Cryptology, 2011, 24(4): 659-693.
[11] BONEH D, BOYEN X. Secure identity based encryption without random oracles[A]. Proc of Cryptology-Crypto'04[C]. Springer Berlin Heidelberg, 2004. 443-359.
[12] WATERS B. Efficient identity-based encryption without random Oracles[A]. Proc of Cryptology-EUROCRYPT'05[C]. Springer Berlin Heidelberg, 2005. 114-127.
[13] GENTRY C. Practical identity-based encryption without random oracles[A]. Proc of Cryptology- EUROCRYPT'06[C]. Springer Berlin Heidelberg, 2006. 445-464.
[14] WATERS B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions [A]. Proc of Cryptology-CRYPTO'09[C]. Springer Berlin Heidelberg, 2009. 619-636.
[15] GENTRY C, SILVERBERG A. Hierarchical ID-based cryptography[A]. Proc of Cryptology—ASIACRYPT'02[C]. Springer Berlin Heidelberg, 2002. 548-566.
[16] LEWKO A, WATERS B. New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts [M]. Theory of Cryptography. Springer Berlin Heidelberg, 2010.
[17] CHEN J, WEE H. Fully, (almost) tightly secure IBE and dual system groups[A]. Proc of Cryptology–CRYPTO 2013[C]. Springer Berlin Heidelberg, 2013. 435-460.
[18] CHOW S S M, DODIS Y, ROUSELAKIS Y, et al. Practical leakage-resilient identity-based encryption from simple assumptions[A]. Proc of the 17th ACM Conference on Computer and Communications Security, CCS'10[C]. Chicago, Illinois, USA, 2010. 152-161.
[19] YUEN T H, CHOW S S M, ZHANG Y, et al. Identity-based encryption resilient to continual auxiliary leakage[A]. Proc of Cryptology–EUROCRYPT 2012[C]. Springer Berlin Heidelberg, 2012. 117-134.
[20] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. Proc of Cryptology–EUROCRYPT'05[C]. Springer Berlin Heidelberg, 2005. 457-473.
[21] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation[A]. Proc of the 15th ACM Conference on Computer and Communications Security[C]. 2008. 417-426.
[22] SEO J H, EMURA K. Revocable identity-based encryption revisited: security model and construction[A]. Proc of Public-Key Cryptography– PKC 2013[C]. Springer Berlin Heidelberg, 2013. 216-234.
[23] LI J, LI J, CHEN X, et al. Identity-based encryption with outsourced revocation in cloud computing[J]. IEEE Transactions on Computers, 2015, 64(2): 425-437.
[24] ABDALLA M, BIRKETT J, CATALANO D, et al. Wildcarded identity-based encryption[J]. Journal of Cryptology, 2011, 24(1): 42-82.
[25] BEATO F, MEUL S, PRENEEL B. Practical identity-based private sharing for online social networks[J]. Computer Communications, 2015, http://dx.doi.org/10.1016/j.comcom.2015.07.009.
[26] WU X, XU L, ZHANG X. POSTER: a certificateless proxy re-encryption scheme for cloud-based data sharing[A]. Proc of the 18th ACM Conference on Computer and Communications Security, CCS'11[C]. 2011. 869-872.
[27] BYUN J W, BERTINO E, LI N. Purpose based access control of complex data for privacy protection[A]. Proc of the 10th ACM Symposium on Access Control Models and Technologies[C]. ACM, 2005. 102-110.
[28] BYUN J W, LI N. Purpose based access control for privacy protection in relational database systems [J]. The VLDB Journal, 2008, 17(4): 603-619.
[29] YANG N, BARRINGER H, ZHANG N. A purpose-based access control model[A]. Proc of the 3rd International Symposium on Information Assurance and Security (IAS)[C]. IEEE, 2007. 143-148.
[30] KABIR M E, WANG H. Conditional purpose based access control model for privacy protection[A]. Proc. of the 20th Australasian Conference on Australasian Database[C]. Australian Computer Society, Inc, 2009. 135-142.
[31] WANG Y, ZHOU Z, LI J. A purpose-involved role-based access control model[A]. Foundations of Intelligent Systems[C]. Springer Berlin Heidelberg, 2014.1119-1131.
[32] COLOMBO P, FERRARI E. Enforcement of purpose based access control within relational database management systems[J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(11): 2703-2716.
[33] SUN L, WANG H. A purpose‐based access control in native XML databases[J]. Concurrency and Computation: Practice and Experience, 2012, 24(10):1154-1166.
[34] JAFARI M, SAFAVI-NAINI R, FONG P W L, et al. A framework for expressing and enforcing purpose-based privacy policies[J]. ACM Transactions on Information and System Security, 2014, 17(1): 3.
[35] 渠世艳. 基于目的管理的医疗信息系统访问控制模型研究[D]. 上海: 上海交通大学, 2009.
QU S Y. Research of Purpose-Based Access Control Model for Hospital Information System[D]. Shanghai: Shanghai Jiaotong University, 2009.
[36] KABIR M E, WANG H, BERTINO E. A role-involved purpose-based access control model[J]. Information Systems Frontiers, 2012, 14(3):809-82.

作者简介：

张怡婷[通信作者]（1978-），女，安徽合肥人，东南大学博士生，南京邮电大学讲师，主要研究方向为网络安全及应用。E-mail: zyt@njupt.edu.cn。

傅煜川（1987-），男，江苏南京人，东南大学硕士生，主要研究方向为网络安全。

杨明（1979-），男，江苏常州人，博士，东南大学副教授，主要研究方向为网络安全。

罗军舟（1960-），男，浙江宁波人，博士，东南大学教授、博士生导师，主要研究方向为下一代网络体系结构、网络安全、云计算、无线局域网。