计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.181202256

面向云端的安全高效的电子健康记录

屠袁飞　张成真
南京工业大学计算机科学与技术学院　南京 211816

摘　要　随着移动设备的发展和普及,基于体域网(Body Area Network,BAN)的电子健康记录正变得越来越流行。人们将从体域网中获取的医疗数据备份到云端,导致几乎任何地方的医疗人员都能够使用移动终端来访问用户的医疗数据。但是对于一些病患来说,这些医疗数据属于个人隐私,他们只想让拥有某些权限的人查看。文中提出了一种高效、安全的细粒度访问控制方案,不仅实现了授权用户对云存储中医疗数据的访问,而且还支持某些特权医生对记录进行修改。为了提高整个系统的效率,加入了先匹配再解密的手段,用于执行解密测试而不解密。此外,该方案将双线性配对操作外包给网关,而不会泄露数据内容,因此在很大程度上消除了用户的解密开销。性能评估显示所提解决方案在计算、通信和存储方面的效率得到了显著提高。

关键词:电子健康记录;体域网;医疗数据;隐私;访问控制
中图法分类号　TP309.7

Secure and Efficient Electronic Health Records for Cloud

TU Yuan-fei and ZHANG Cheng-zhen
College of Computer Science and Technology,Nanjing University of Technology,Nanjing 211816,China

Abstract　With the development and popularty of mobile devices,Electronic Health Record-based BAN is becoming more and more popular. People can back up the medical data acquired by the Body Area Network(BAN) to the cloud,which makes it possible for medical workers to accessed the user's medical data using mobile terminals almost anywhere. However,for some patients,these medical data are personal privacy and they only want to be accessed by someone with some rights. This paper proposed an efficient and secure fine-grained access control scheme,which not only enables authorized users to access medical data stored in the cloud,but also supports some privileged doctors to write records. In order to improve effciency of whole system,a method of matching before decryption is added to perform decryption tests without decryption. In addition,this scheme can outsource the bilinear pairing operation to the gateway without leaking the data content so that eliminates the user's computation overhead. Performance evaluation shows that efficiency of proposed solution in computating,communication and storage has been significantly improved.

Keywords　Electronic health record,Body area network,Medical data,Privacy,Access control

1　引言

随着云计算技术和物联网的发展与成熟,为了提高电子健康记录(Electronic Health Record,EHR)的存储能力与检索记录互操作性,越来越多的专家提出将云计算技术和物联网与健康记录进行整合(如谷歌健康记录[1]),即基于云的健康记录。这样不仅能够增加 EHR 的存储能力,还能够提高病患医疗数据的可分享性。然而,第三方云始终不是百分之百的可靠,尽管在数据分享与存储的过程中,云环境能够提供很大的便利,但病患的医疗记录能够被许多用户访问,这必定会引起病患敏感数据安全和隐私泄露的问题[2-3]。

一些学者提出跨学科合作,将加密技术应用于基于云的电子健康记录。然而,已经存在的电子健康记录系统,要么是数据根本不受保护,要么只进行简单的批量加密[4]。在过去,研究者都是使用目标单一的基于身份的加密(Identity-Based Encryption,IBE)方案加密数据,数据拥有者想要分享数据

到稿日期:2018-12-04　返修日期:2019-04-06　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61572263,61272084);江苏省高校自然科学研究重大项目(11KJA520002);高等学校博士学科点专项科研基金(20113223110003);中国博士后科学基金(2015M581794);江苏省博士后科研资助计划(1501023C)
This work was supported by the National Natural Science Foundation of China (61572263,61272084),Major Natural Science Research Projects in Colleges and University of Jiangsu Province(11KJA520002),Special Research Fund for Doctoral Discipline Points in College and Universities (20113223110003),China Postdoctoral Science Foundation(2015M591794),Jiangsu Postdoctoral Research Grant Scheme(1501023C).
通信作者:屠袁飞(yuanfeitu@163.com)

时，必须了解数据用户的身份。因此，传统的加密技术不能够有效地迎合云环境下存在大量用户记录以及复杂运算的实际情况，同时不能够保证数据的安全和细粒度访问控制的共存[5]。为了确保数据的机密性，应严格限制云服务商以及非权威人士对数据进行非法访问。另外，医疗数据对于病患来说是隐私，如果要对医疗记录进行修改，需要经过相关机构或者医患人员自身的认证。

在保护数据安全、提供灵活的资源分享以及细粒度的访问控制方面，基于属性加密（Attribute-Based Encryption，ABE）访问控制是一种十分有效的方法[6]。ABE 算法被分为 KP-ABE 和 CP-ABE[7]。在电子医疗记录中，学者偏爱于后者，因为它能够随着系统的需求构造出灵活多变的访问策略。在 CP-ABE 机制中，用户的密钥是和一系列的属性相关联的，并且访问策略都是通过属性集合嵌入到密文之中的[8]。

为了完美地解决医疗云环境下患者记录的数据安全和隐私问题，并且实现细粒度的访问控制，研究者们提出了医疗背景下的许多 CP-ABE 变形体。文献[9]提出了一种支持属性撤销的访问机制。文献[10]提出了允许访问权限委托的变形体，它能够实现对加密数据的灵活访问控制。但是，以上变形体无法在医护人员与其他专家在云环境下共享诊断结果的前提下，保护患者的医疗隐私。文献[11]提出了一种多权威的 CP-ABE 安全机制，它能够多方面保护病患的医疗记录。文献[12]引进一个新的密钥和 CP-ABE 算法相融合，提出了一种灵活多变的访问控制策略，但加解密的过程中仍然需要进行大量的多项式运算，并且这种运算消耗会随着访问策略复杂程度的上升呈现递增的趋势。文献[13]提出一种病人控制的基于属性的加密，为病人提供细粒度的加密方案。该方案不仅采用属性权威，而且增加了将密钥生成过程拆分为两个阶段验证的权威中心，减轻了操作的负担并降低了运算的复杂度。然而，这两个权威中心必须是完全可信的，这在安全性要求方面增加了很大的阻力。

本文基于云端的电子医疗记录提出了一种高效且安全的细粒度访问控制策略，它不仅限制了非法用户对病患数据记录的访问，还支持一些获得授权的医疗专家对数据进行有效修改。为了提高解密的效率，在解密算法中加入了先匹配后解密的功能，即在解密之前进行属性的验证，如果不能够有效匹配，就直接退出整个系统，不必进行繁琐的解密行为。

2 预备知识及系统模型

2.1 预备知识

2.1.1 双线性映射

设 G_1 和 G_2 是两个 p 阶循环群，其中 p 为一大素数。设 p 为 G_1 的生成元，定义双线性映射 $e:G_1\times G_1\rightarrow G_2$ 满足如下条件。

1）双线性：对任意的 $P,Q\in G_1$，$a,b\in Z_p$，满足 $e(P^a,Q^b)=e(P,Q)^{ab}$。

2）非退化：$e(P,P)\neq 1$。

3）可计算：对任意的 $P,Q\in G_1$，$a,b\in Z_p$，存在一个有效的多项式时间算法计算出 $e(P,Q)$。

2.1.2 线性秘密共享方案

一个基于成员集 P 的秘密共享方案 Π 在 Z_p 上是线性的需要满足两个条件：

1）每个成员所分得秘密的一部分构成一个 Z_p 上的矩阵。

2）Π 中存在一个 $l\times(n+1)$ 的秘密共享矩阵 $\boldsymbol{M}$。对于 $i=1,\cdots,l$，$\boldsymbol{M}$ 的第 i 行表示第 i 个成员 $x_i\in P$。设一个列向量 $\boldsymbol{v}=(s,r_1,r_2,\cdots,r_n)$，其中 $s\in Z_p$ 是待分享的秘密，是随机的，则 $\boldsymbol{M}\cdot\boldsymbol{v}$ 根据 Π 把秘密 s 分成 l 个部分。$(\boldsymbol{M}\cdot\boldsymbol{v})_i$ 属于成员 x_i。

2.2 系统模型

如图 1 所示，系统包含 4 个实体：医疗中心（Healthcare Center，HC）、云服务器（Cloud Server，CS）、数据用户（Data Consumers，DC）和体域网。

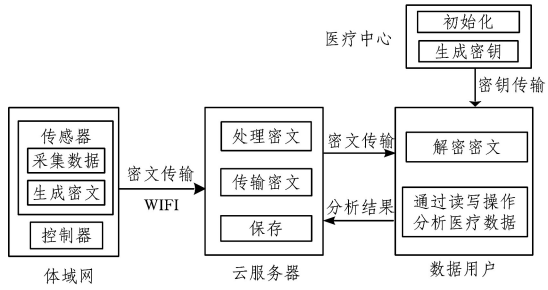

图 1 系统模型

Fig. 1 System model

2.2.1 医疗中心

医疗中心主要负责系统初始化和用户授权工作。它是可信任的实体，负责给用户分发私钥并生成系统公钥，同时能够根据数据用户的属性授予相应的细粒度访问权限。

2.2.2 云服务器

云服务器拥有足够的存储能力，主要用于存储数据的密文，并将其发送给授权用户。

2.2.3 数据用户

数据用户主要是指需要访问患者数据的专家或者医疗人员。每个用户都会根据系统的设定，拥有一系列与自身有某种关联的属性和一个与他们属性相关的密钥。如果用户的属性与嵌在密文上面的访问结构相匹配，那么他能够通过匹配环节进而解密；否则，匹配出错，退出整个系统。

2.2.4 体域网

体域网主要由一个控制器和一系列可穿戴或者可嵌入的传感器组成。控制器主要用来控制访问结构，医疗患者能够通过控制器来构造访问结构。传感器用来收集和检测人体内部的重要参数，例如血压等。另外，我们可以将压缩和加密技术联合引用，将一些医疗图片的密文进行压缩传输，以降低整个系统的传输压力和能量消耗。

2.3 访问控制结构

在本文系统中，患者可以让部分医疗专家或其他用户通过手机或者电脑随时随地访问自己的医疗数据，但是当遇到特殊的数据或者记录改动时，系统往往需要通过访问结构对

用户的属性进行严格的限制，以防止非专业的访问者对数据进行误改；即使某些用户的属性能够满足访问策略，其也仅可以进行读操作，不能对数据进行篡改。

本文的访问控制模型如图 2 所示。

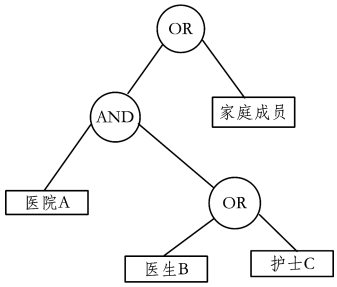

图 2 访问控制结构

Fig. 2 Access control structure

3 本文算法的方案构造

3.1 算法描述

算法 1 系统初始化 Setup(l,U)

系统初始化算法是一种随机化算法，它以一个随机的安全系数 λ 和一个属性域 U 作为输入，输出系统公钥 PK 和主密钥 MK。

该算法选择一个阶为大素数 p、生成元为 g 的乘法循环群 G 和一个哈希函数 H。哈希函数 H 用来生成群元素 $h_1,\cdots,h_U\in G$；另外，它随机生成指数 $\alpha_1,\alpha_2,\beta,a\in\mathbb{Z}_p$，让 $\alpha=(\alpha_1+\alpha_2) \bmod p$。生成系统的公钥为 $PK=\{g,e(g,g)^a,g^a,h_1,\cdots,h_U\}$，主密钥为 $MK=\{\alpha,\alpha_1,\alpha_2,\beta\}$。

算法 2 私钥生成算法 KeyGen(MK,S)

私钥生成算法输入主密钥 MK 和用户属性集 S，选取随机数 $t\in\mathbb{Z}_p$。算法输出的用户私钥分为两部分，一部分为属性密钥 AK，作为匹配阶段的输入；另一部分为私钥 SK。

$AK:\{K_1=g^{\alpha_1}g^{\alpha t},L=g^t,Kx=h_x^t(\forall x\in S)\}$

$SK:\{K_2=g^{\alpha_2}g^{\alpha t}\}$

算法 3 加密算法 Encrypt(PK,m,(M,ρ))

加密算法输入公共密钥 PK、明文 m，以及 LSSS 访问结构(M,ρ)，输出密文 CT。令 $\boldsymbol{M}$ 为 $l\times n$ 阶的矩阵，l 为用户属性数，n 为访问策略中的属性数，函数 ρ 将 $\boldsymbol{M}$ 中的每一行映射到一个用户属性。在 Z_p 上随机选择一个矢量 $\vec{v}^{\mathrm{T}}=(s,y_2,y_3,\cdots,y_n)\in\mathbb{Z}_p^n$ 用于分享加密元素 s，对 $i=1,2,\cdots,l$，计算 $\lambda_i=M_i\vec{v}$，其中 $\boldsymbol{M}_i$ 为 $\boldsymbol{M}$ 的第 i 行，再随机选取 $r_1,\cdots,r_l\in\mathbb{Z}_p$，$k\in\mathbb{Z}_p$，得到如下密文。

$CT:\{C=me(g,g)^{\alpha s},C'=g^s,C_i=g^{a\lambda i}h_{\rho(i)}^{-ri},D_i=g^{r_i}\}$

算法 4 转换算法 TransformDecrypt(CT,AK)

转换算法以属性私钥 AK 以及密文 CT 为输入，假设用户的属性列表 S 满足访问结构(M,ρ)，令$\{\omega_i\in\mathbb{Z}_p\}_{i\in I}$始终为常量，那么要使得等式 $\sum_{i\in I}\omega_i\lambda_i=s$ 成立，则存在秘密 s 的有效份额$\{\lambda_i\}$，其中，$I=\{i:\rho(i)\in s\}$，$I\subset\{1,2,\cdots,l\}$。

匹配阶段：这个阶段主要是通过下面的这个等式来检测用户是否能够进入转换阶段。

$\sum_{i\in I}M_i w_i=(1,0,\cdots,0)$

如果它输出 true，就进入转换阶段，否则输出⊥。

生成 CT' 阶段：一旦进入这个阶段，密文 CT 就会被转化为 CT'。

$$CT'=e(C',K_1)/(\prod_{i\in I}(e(C_i,L)e(D_iK_{\rho(i)}))^{w_i})^2$$
$$=e(g^s,g^{\alpha_1}g^{at})/(e(g,g)^{ats})^2$$
$$=e(g,g)^{\alpha_1 s}/e(g,g)^{ats}$$

算法 5 解密算法 Decrypt(SK,CT')

该算法以私钥 SK 和转化密文 CT' 为输入，计算结果如下：

$$e(SK,C')=e(g^{\alpha_2}g^{at},g^s)e(g,g)^{\alpha_1 s}/e(g,g)^{ats}$$
$$=e(g,g)^{\alpha_2 s}e(g,g)^{ats}e(g,g)^{\alpha_1 s}/e(g,g)^{ats}$$
$$=e(g,g)^{\alpha s}$$

明文 $m=C/e(g,g)^{\alpha s}$。

算法 6 重加密算法 ReEnc(CT,x')

重加密算法以一个待更新的属性 x' 以及密文 CT 的部件 D_i 为输入，计算：

$\forall i=1,2,\cdots,l$；

若 $\rho(i)\neq x'$，$\tilde{D_i}=D_i=g^{r_i}$；

若 $\rho(i)=x'$，$\tilde{D_i}=D_i^{1/v_{\rho(i)}}=(g^{r_i})^{1/v_{\rho(i)}}$。

重加密之后的密文为：

$\tilde{CT}=\{\tilde{C},C,\{C_i,\tilde{D_i}\}_{i=1,\cdots,l}\}$

3.2 系统机制的应用

本节将详细介绍如何通过调用算法来实现对电子医疗记录的访问控制。

3.2.1 密文格式

ABE 算法自身的局限性，使得其并不适合对大型文件进行加密，因此本文同时使用对称和非对称两种加密方式。首先，用户体域网的控制器随机选取一个对称密钥 K，利用对称加密算法 AES(K,D)对传感器采集的数据 D 进行加密。之后，根据患者对数据用户的分类情况，利用 ABE 算法定义该文件的访问结构，调用算法 3 加密上述对称密钥 K，得到密钥密文 CT，再按照图 3 的存储格式将文件发送至云存储器。

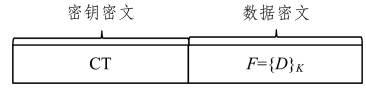

图 3 数据文件的密文格式

Fig. 3 Format of ciphertext

用户首先向 HC 声明其拥有的属性，根据算法 3 获得与其属性相对应的私钥；之后，从云存储器中获取数据密文，利用算法 4 得到会话密钥 K；最后，利用会话密钥 K 解密 $AES(K,D)$，得到原始数据 D。

3.2.2 密钥的生成与分配

诚信机构 HC 负责密钥的生成和分配，主要分为 3 个步骤。

步骤 1 当一个用户最初进入系统的时候，HC 会为其分配唯一的 ID，并对其进行哈希函数变换，得到 $H(ID)$。$H()$ 表示哈希函数。

步骤 2 通过运行密钥生成算法 KeyGeneration 来生成属性私钥 AK 和用户私钥 SK,SK 必须被用户保持私有。

步骤 3 为了节约存储空间,AES(K,D)与用户的 $H(ID)$粘贴在一起被保存在用户表中。

3.2.3 医疗数据的加密

在体域网中,可穿戴设备每天都会收集大量的患者医疗数据,如血压等。在本系统中,病人是这些数据的管理者。在公开的网络中,这些医疗信息可能会由于非法访问被泄露甚至篡改,那么病人就需要为这些医疗数据选择相应的访问结构来控制什么人能够访问信息。该过程主要分为以下 5 个步骤:

步骤 1 病人在控制器内部嵌入相应的访问策略;

步骤 2 利用对称加密算法对收集到的数据进行加密;

步骤 3 在访问结构下运行加密算法对对称加密算法生成的密钥进行加密;

步骤 4 将加密后的数据与加密的密钥一起上传到云服务器保存;

步骤 5 如果有数据进行修改,则运行算法 6,并对修改后的数据进行重加密后上传。

3.2.4 数据的访问

通常情况下,由于病人隐私要求以及终端用户的需要,医疗数据必须可以随时从云端下载到本地移动设备端。终端用户对医疗数据进行访问主要分为以下 7 个步骤:

步骤 1 用户需要向云端发出一个请求,并等待回应;

步骤 2 云端会做出相应的响应,并将密文发送到用户对应的网关;

步骤 3 网关利用用户的 AK 运行匹配过程,对用户的身份进行确认,即验证用户是否有权限对数据进行访问;

步骤 4 如果用户满足读的策略,网关执行算法 TransformEncrypt;

步骤 5 用户运行解密算法,得到明文和对称加密算法的密钥,进而得到医疗数据;

步骤 6 如果用户的属性经过网关确认用户拥有修改的权限,那么他就能够利用访问结构运行解密算法解密密文,并且对病人的数据进行修改与补充;

步骤 7 在对数据进行一定的修改和补充后,再次执行 3.2.3 小节的步骤 5 进行重加密,然后将加密修改后的文件再次上传到云服务器保存,并且对之前的记录进行覆盖。

4 方案分析

4.1 安全性分析

4.1.1 数据的机密性

在本文提出的方案中,医疗信息的机密性完全由对称加密算法 AES 决定,而对称加密算法的机密性则取决于对称密钥 K 的安全性。对于密钥 K,本文采用 CP-ABE 对其进行加密。该算法的安全性已经被证实,未认证用户(如攻击者)的属性集不满足访问策略,其无法在解密过程中恢复 $e(g,g)^{\alpha s t}$ 的值,从而不能访问数据文件。

本方案利用云服务器存储密文文件。虽然从某种程度讲服务器不被完全信赖,但是会诚实地执行终端用户提出的访问需求,所以数据的机密性不会受到影响。

4.1.2 抗合谋攻击

用户的联合攻击是基于属性加密算法的最大挑战。在 CP-ABE 中,秘密共享值 s 嵌入在密文中。为了解开密文,用户或者合谋攻击者需要将 $e(g,g)^{\alpha s t}$ 恢复出来。合谋攻击者必须利用密文中的组件 C_l,D_l 和其他合谋用户的私钥组件 L,$K_{\rho(i)}$ 做相应的双线性配对运算。但是,每个用户的私钥生成过程多会包含一个随机数 t,由于每个用户的 t 不同,因此即使用户合谋,$e(g,g)^{\alpha s t}$ 的值也不会被恢复。只有在用户具有的属性满足医疗患者定义的访问策略时,$e(g,g)^{\alpha s t}$ 值才会被恢复,密文才能被解密。

4.1.3 数据的完整性

在云存储环境中,数据已经被外包给第三方云服务器,用户失去了对数据的掌控,其会担心数据密文在云中是否完全按照自身要求的格式进行存储与读取。为了检测甚至防止这种情况的发生,需要定期审核云数据的完整性。因此,用户如何验证云数据的完整性,成为了云存储中须解决的一个关键问题。

该方案通过数据分块、分别编码及抽查文件随机子集技术来确保云服务系统中数据的持有性和可恢复性,能够进行无限多次的完整性验证,同时有效地确保了数据的内容不被验证者察知,用户甚至可以将繁琐的数据审计任务交由第三方管理者来完成。在数据完整性的自验证过程中,医疗中心可以对云服务商发起挑战,主要分为以下两个阶段。

1)初始化阶段

步骤 1 在该验证过程中,医疗中心会根据算法 1 另外生成一对验证密钥对$\{g^{\beta},\beta\}$。

步骤 2 医疗中心会将存储在云服务器的密文 F 有效划分为 $F=\{b_1,b_2,\cdots,b_n\}$,随机选择 $m_i\in\mathbb{Z}_p$,为上述每一数据块生成认证元数据集合 $\Phi=\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$,其中 $\sigma_i=(H(i)\cdot u^{m_i})^{\beta}$,$H(i)$为 i 对应的哈希运算。

步骤 3 医疗中心将$\{m_i\}$和$\{\sigma_i\}$附在密文之后发送到云中存储。

2)挑战阶段

步骤 1 医疗中心作为验证的发起者,会周期性地对云服务器提出挑战。从文件 F 的分块中随机选取 t 个索引编号,并为每一个编号选取一个随机数 $v_i\in\mathbb{R}_p$,将二者组合形成挑战请求$\{i,v_i\}_{i\in[1,n]}$,并将 v_i 发送到公有云作为挑战。

步骤 2 云服务器利用其存储的 v_i 做运算 $\mu=\sum_{i=i_1}^{i_t}v_i\cdot m_i$,$\sigma=\prod_{i=i_1}^{i_t}\sigma_i^{v_i}$,然后将$\{\mu,\sigma\}$发送给医疗中心进行验证。

步骤 3 医疗中心接收到$\{\mu,\sigma\}$后,判断等式 $e(\sigma,g)=e(\prod_{i=i_1}^{i_t}H(i)^{v_i}\cdot u^{\mu},v)$是否成立。若等式成立,则认为云服务器中存储的数据是完整的。

4.2 性能分析

4.2.1 实验建立

实验采用斯坦福大学开发的基于 JAVA 的双线性对密

码库(JPBC)[14]，椭圆曲线采用 Type A：$y^2=x^3+x$。实验环境为 Inter(R) Core(TM) i5-3230M 2.60GHz CPU，12.00GB 内存，Windows 7 64 bit 操作系统。实验中的对称加密采用 128 bit AES 加密算法，不计实际应用中的数据传输延时。

在 CP-ABE 方案中，解密时间和密文大小取决于密文策略的复杂度，它们会随着策略中属性数量的增加呈线性增长。为了说明这一点，我们选择 100 个最复杂的策略(A_1 AND A_2 AND …AND A_n)，其中 A_i 是一个属性，并且 n 的值从 1 增加到 100。这种方法保证了所有的密文组件都能够参与解密计算。在每种情况下，我们构造一个对应的标准解密密钥，其中包含精确的 n 个属性。

在实际应用中，ABE 并不适合直接对数据进行加密。本文的实验仿真参照了文献[15-17]的相关工作，信息加密使用对称加密机制和非对称加密机制的混合加密。我们为不同的策略选择一个随机的 128 bit 对称密钥，然后使用正常的解密算法和外包解密算法解密 ABE 密文(在实验中，不考虑对称加密算法的影响)。

4.2.2 仿真结果

为了综合每次实验的误差，我们对每一个密文策略的实验重复进行 100 次，然后取得平均值。实验结果如图 4—图 8 所示。

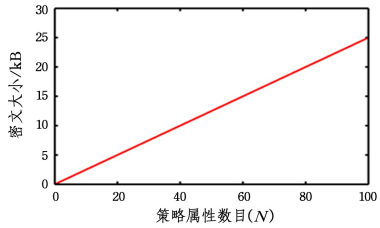

图 4 密文大小与策略属性数目的关系

Fig. 4 Relationship between ciphertext size and number of policy attributes

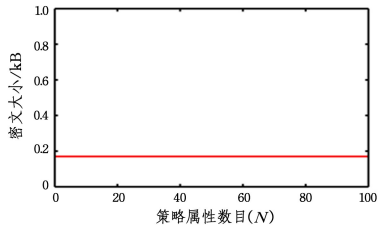

图 5 转换后密文大小与策略属性数目的关系

Fig. 5 Relationship between transformed ciphertext size and number of policy attributes

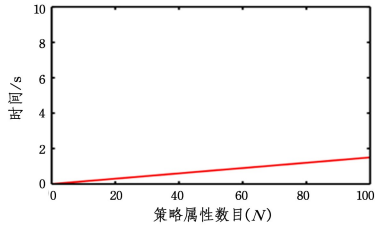

图 6 解密时间与策略属性数目的关系

Fig. 6 Relationship between decryption time and number of policy attributes

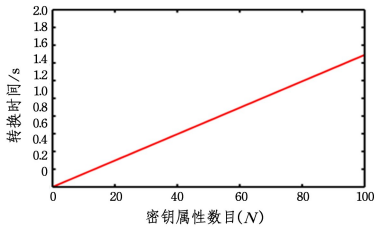

图 7 密文转换时间与密钥属性数目的关系

Fig. 7 Relationship between time of ciphertext transform and number of key attributes

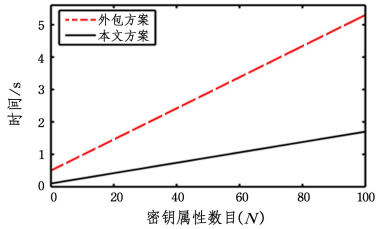

图 8 解密时间

Fig. 8 Decryption dime

4.2.3 实验分析

正如之前预期的那样，在计算资源有限的情况下，外包能够大大减少明文恢复所需的计算时间和能量消耗。现在大部分的解密操作由网关处理，转换密文不仅提升了解密效率高，而且减小了密文尺寸。在仿真实验中，如图 5 所示，每个经过转换的密文，不论其对应的密文策略的复杂性大小，密文都具有恒定的长度即 176 字节。

本方案将最复杂的解密计算委托给网关，只给用户留下一个配对计算。另外，在密文的代理转换之前，我们添加了一个匹配操作，用于检查用户是否可以对密文进行解密。它节省了大量的计算时间，因为如果不满足匹配操作，则网关不会变换相应的密文。因此，该过程缩短了用户从云端检索加密数据的整个响应时间。

由图 8 可以看出外包方案[18]与本文方案之间的差别。增加了随机数 Z，使用户的密钥盲目，但炸毁了密钥大小；同时，解密前没有匹配操作，用户会因无法解密密文浪费时间，因而效率不高。本文方案不仅通过匹配操作提高了效率，而且通过解密计算的外包节省了资源。

本文构造的基于属性基的加密算法各步骤的计算复杂度如表 1 所列。

表 1 算法复杂度

Table 1 Computational complexity

算法步骤	复杂度
系统建立	O(1)
加密文件	O($l*$n)
生成密钥	O($\|S\|$)+O(1)
转换密文	O((2+l)p)
解密	O(1)

结束语 本文为面向云端辅助的电子健康记录系统提供了一种高效且安全的基于属性的访问控制机制，该机制通过对用户身份的认证，解决了用户数据的机密性、完整性保护问

题。性能分析表明,该方案不仅能降低私钥消耗,还能加强对终端用户可操作的访问控制,能够十分有效地应用于电子健康记录问题。

参 考 文 献

[1] LI M,YU S C,CAO N,et al. Authorized private keyword search over encrypted data in cloud computing[C]// Proceedings of the 2011 31st International Conference on Distributed Computing Systems. Washington:IEEE Computer Society,2011:383-392.

[2] REZAEIBAGHA F,MU Y . Distributed clinical data sharing via dynamic access-control policy transformation[J]. International Journal of Medical Informatics,2016,89(10):25-31.

[3] QIAN H L,LI J G,ZHANG Y C,et al. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation[J]. International Journal of Information Security. 2015,14(6):487-497.

[4] AKINYELE J A,LEHMANN C U,GREEN M D,et al. Self-Protecting Electronic Medical Records Using Attribute-Based Encryption[J]. Faculty Publications,2010,2011(10):1-20.

[5] LIU X J,XIA Y J,YAN W,et al. Secure and Efficient Querying over Personal Health Records in Cloud Computing[J]. Neurocomputing,2018,274(24):99-105.

[6] SAHAI A,WATERS B. Fuzzy identity-based encryption[C]// Proceedings of the 24th Annual International Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer,2005:457-473.

[7] GOYAL V,PANDEY O,SAHAI A,et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. New York,ACM,2006:89-98.

[8] ZHANG Y H,ZHENG D,DENG R H. Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control[J]. IEEE Internet of Things Journal,2018,5(3):2130-2145.

[9] NARAYAN S,GAGNE M,SAFAVI-NAINI R. Privacy preserving EHR system using attribute-based infrastructure[C]// Proceedings of the 2010 ACM Conference on Computer and Communications Security. NewYork:ACM,2010:47-52.

[10] XHAFA F,WANG J F,CHEN X F,et al. An efficient PHR service system supporting fuzzy keyword search and fine-grained access control[J]. Soft Computing,2014,18(9):1795-1802.

[11] IBRAIMI L,ASIM M,PETKOVIC M. Secure Management of Personal Health Records by Applying Attribute-Based Encryption[C]// Proceedings of the 6th International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health. Norway:IEEE,2011:71-74.

[12] AKINYELE J A,PAGANO M W,GREEN M D,et al. Securing electronic medical records using attribute-based encryption on mobile devices[C]// Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. New York:ACM,2011:75-86.

[13] EOM J,LEE D,LEE K. Patient-Controlled Attribute-Based Encryption for Secure Electronic Health Records System[J]. Journal of Medical System,2016,40(12):253.

[14] LYNN B. Stanford Pairings-Based Crypto Library[OL]. http://crypto. stanford. edu/ pbc/.

[15] BETHENCOURT J,SAHAI A,WATERS B. Ciphertext-policy attribute-based encryption[C]// Proceedings of the 2007 IEEE Symposium on Security and Privacy. Washington: IEEE, 2007: 321-334.

[16] WATERS B. Ciphertext-policy attribute-based encryption:an expressive,efficient,and provably secure realization[C]// Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Crytography. Berlin:Springer,2011:53-70.

[17] HHENBERGER S,WATERS B. Attribute-based encryption with fast decryption [J]. Public Key Cryptography, 2013, 7778(10):162-179.

[18] GREEN M,HOHENBERGER S,WATERS B. Outsourcing the Decryption of Abe Ciphertexts[C]// Proceedings of the 20th USENIX Conference on Security. San Francisco: ACM, 2011: 34.

TU Yuan-fei, born in 1984, doctor of philosophy. His main research interests include the safety and access control of cloud computing.

ZHANG Cheng-zhen, born in 1992. His main research interests in clude, the security of information.