文章编号：2095-2163(2020)09-0033-03 中图分类号：TP309.2 文献标志码：A

基于无线体域网的轻量级细粒度访问控制方案

房保纲，张家磊，牛广利，贾媛媛，方 凯
（上海工程技术大学 电子电气工程学院，上海 201620）

摘 要：随着无线通信技术、嵌入式医疗传感器技术的迅速发展，无线体域网（WBAN）技术得到了广泛的应用，如何有效地保护 WBAN 中数据共享时数据的安全是一个亟待解决的关键问题。考虑到 WBAN 中传感器节点资源的有限性和访问用户具有动态性的特点，本文提出了一种基于外包计算的基于密文策略的属性加密方案（CP-ABE）。与其他已有的方案对比，该方案具有加解密速度更快、通信开销更小、实现了细粒度访问控制并且能保证一定的安全性的特点。

关键词：无线体域网；细粒度访问控制；属性加密；外包计算

Lightweight and fine-grained access control scheme based on wireless body area network

FANG Baogang, ZHANG Jialei, NIU Guangli, JIA Yuanyuan, FANG Kai
（Electronic Institute of Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China）

【Abstract】 With the rapid development of wireless communication technology and embedded medical sensor technology, wireless body area network (WBAN) technology has been widely used. How to effectively protect data security during data sharing in WBAN is a key issue to be solved urgently. Considering the limited resources of WBAN sensor nodes and the dynamic characteristics of accessing users, an attribute encryption scheme based on ciphertext strategy (CP-ABE) and outsourcing computing is proposed. Compared with the existing schemes, this scheme has the characteristics of faster encryption and decryption speed, lower communication overhead, fine-grained access control, and certain security.

【Key words】 wireless body area networks (WBANs); fine-grained access control; attribute-based encryption; outsourced computing

0 引 言

随着医疗传感器技术与互联网技术的迅速发展，无线体域网技术正成为一种常用的新型数字医疗技术。无线体域网技术是一种以人体为中心，通过在人体体内植入或者在体表安装各种医疗传感器的方式组成无线通信网络。无线体域网可以通过各式的医疗传感器实时的采集患者的生理数据（如体温、血压、血糖、心电图等），并将收集到的病人生理数据通过邻近的数据节点（如网关、手机等）及时的上传到医疗服务器中[1]。经过授权的医护人员可以查看患者的生理数据信息，从而实现对患者实时诊断。但是，传统的无线医疗传感器由于资源受限，需要借助云服务器来解决数据存储和加密运算，提高数据传输的实时性和保密性。

保护 WBAN 数据隐私的一种常用的方法是对传感器节点采集的数据先加密再传输。传统的对称密码体制和公钥密码体制并不适用于加密传感节点众多和“一对多”通信的场景。传统的 WBAN 资源受限，大量的高频率个人健康信息、医疗数据采样需要可扩展的存储和计算需求，基于云计算的属性加密系统满足上述要求，它能很好地连接资源受限的医疗传感器和超级计算机（云服务器），延长传感器的生命周期，特别是在紧急情况下，提供低延迟的辅助医疗服务[2]。

1 理论基础

1.1 双线性对

设 G_1 为一个阶为素数 q 的加法循环群，P 为其生成元；G_2 为同阶的乘法循环群，设映射为：$e:G_1 \times G_2 \rightarrow G_2$ 且该映射满足以下 3 条性质[3]：

（1）双线性。对任意 $P,K,Y \in G_1$，都有 $e(P,X+Y)=e(P,X)\,e(P,Y)$，且对于任意的 $a,b \in Z_q^*$，满足 $e(aP,bP)=e\ (P,P)^{ab}=e(abP,P)=e(P,abP)$。

（2）非退化性。存在 $X,Y \in G_1, e(X,Y) \neq 1$。

（3）可计算性。存在 $X,Y \in G_1, e(X,Y)$ 能够通过一个算法在多项式时间内计算出来。

1.2 访问树

假设 T 代表一个访问树形式的访问结构。定义访问树的每个非叶子节点代表一个陷门，它代表的内容通过它的叶子节点和一个门限值描述出来。如

作者简介：房保纲（1994-），男，硕士研究生，主要研究方向：无线体域网络安全。

收稿日期：2020-06-06

果用 num_x 表示节点 x 拥有的叶子节点的数目，k_x 表示其被赋予的门限值，那么这两者之间被要求满足关系式 $0 < k_x \leqslant num_x$。当 $k_x = 1$，此时的限门选择即为 OR 门；而当 $k_x = num_x$ 时，陷门的选择即为 AND 门。一个具体的叶子节点 x 就由一个真正的属性值和陷门值 $k_x = 1$ 来表达。

为了实现访问树的功能描述，将先给出一些相关函数的定义。$parent(x)$ 表示节点 x 在访问树中上一层次的节点。当且仅当 x 为一个叶子节点时，$att(x)$ 被定义为节点 x 的属性值。访问树还为每一个节点的叶子节点定义一个序列函数，是指每一个节点的叶子节点被从 1 到 num 进行了排序。用 $index(x)$ 反馈回排序结果。如果 T_x 表示 T 取自节点 x 的子树。当属性集合 S 满足 T_x 时，标记为 $T_x(S) = 1$。需要说明的是属性集合与访问树的满足关系通过一个递归程序实现。

1.3 DBDH 问题

给定两个阶都为 p 的循环加法群 G_1 和循环乘法群 G_T、一个双线性映射 $\hat{e}: G_1 \times G_1 \rightarrow G_T$ 和一个群 G_1 的生成元 P，判定双线性 Diffie－Hellman（decisional billnear Diffie－Hellman，DBDH）问题是 (P, aP, bP, cP) 和 $z \in G_T$，判断 $z = \hat{e}(P,P)^{abc}$ 是否成立[4]，这里的 $a, b, c \in \mathbb{Z}_p^*$ 是未知数的整数。

2 方案设计

2.1 系统模型和框架

本文主要对基于密文策略的访问控制方案进行部分的外包计算，系统分为 4 个部分：可信任授权机构 TA、云服务提供商 CSP、数据拥有者 DO、数据访问者 DU。基于属性加密医疗数据传输方案系统模型，如图 1 所示。A 负责初始化系统参数，根据 DU 的属性生成对应的私钥；CSP 负责数据的加密、解密及存储；DO 和 DU 将大量的加密和解密运算外包给 CSP 进行运算，从而能够极大地减少设备的运算量；DO 负责将从人体采集的生理数据用访问控制策略部分加密后上传至 CSP，如果 DU 想访问某些数据时，则向 CSP 发出申请，当 DU 的密钥符合访问控制策略才能正确的解密数据。

外包加密方案主要有以下 8 个算法构成：

（1）$Setup(\lambda, \mathbb{U})$：由 TA 执行初始化算法，输入安全参数 λ 和属性集 $\mathbb{U}$，得到公共参数 $params$ 和主密钥 MSK。

（2）$User.KeyGen(params, MSK, id_u, Att_u)$：该算法由 CSP 执行，输入公共参数 $params$、主密钥 MSK 和对应地用户 id_u 得到对应用户的 SK_u。

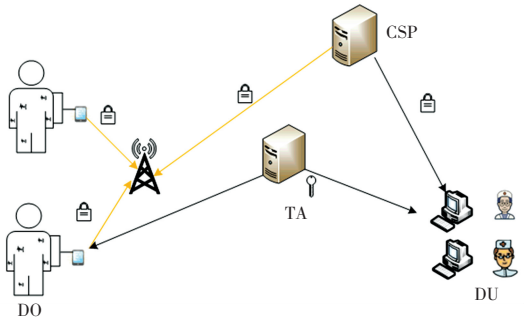

图 1 基于属性加密医疗数据传输方案系统模型

Fig. 1 System model of medical data transmission scheme based on attribute encryption

（3）$Owner.KeyGen(params)$：该算法由 TA 执行，输入公共参数 $params$，输出一对公私钥 (SK_O, PK_O)。

（4）$Part.Enc(params, T, SK_O, M)$：该算法由 DO 执行，输入公共参数 $params$、访问树 T、DO 的密钥 SK_O 以及信息 M，得到部分密文 PCT_T。

（5）$Full.Enc(params, PCT_T, PK_O)$：该算法由 CSP 执行，输入公共参数 $params$、部分密文 PCT_T 以及 DO 的的公钥 PK_O，输出全部密文 CT_T。

（6）$TokenGen(params, id_u, SK_u, CT_T)$：该算法由 DU 执行，输入公共参数 $params$、DU 身份 id_u、密钥 SK_u、以及密文 CT_T，输出一个私钥 k 以及一个解密令牌 TK_u 或者输出一个错误信息 $\perp$。

（7）$Part.Dec(params, CT_T, TK_u)$：该算法由 CSP 执行，输入公共参数 $params$，密文 CT_T，以及一个解密令牌 TK_u，输出部分被解密的密文 M'。

（8）$Full.Dec(params, M_O, k)$：该算法由 DU 执行，输入公共参数 $params$、部分被解密的密文 M'，输出 M。

2.2 方案具体构造过程

（1）系统初始化。TA 选择一个安全参数 λ 和一个属性集 $\mathbb{U}$，计算 $Setup(\lambda, \mathbb{U}) \rightarrow (params, MSK)$。

其中，$MSK = (x_0, P_1, X_1, \{sk_i\}_{i=1}^{m})$；$params = (\lambda, G_1, G_2, \hat{e}, P_0, P_2, E_1, E_2, \{pk_i\}_{i=1}^{m})$；$E_1 = \hat{e}(x_0 P_0, P_1)$；$E_2 = \hat{e}(P_0, X_1)$。

（2）密钥委托。DU 密钥产生算法 $User.KeyGen(params, MSK, id_u, Att_u)$。

其中，$SK_{i,u} = x_0 P_1 + X_1 + sk_i\, id_u$，对于每个 $i \in Att_u$，输出 $SK_u = \{SK_i, u\}_{i \in Att_u}$。DO 密钥产生算法 $Owner.KeyGen(params)$，选择 $d_o \leftarrow \mathbb{Z}_q$，计算 $PK_O^{(1)} = E_2^{d_o}, PK_O^{(2)} = d_o P_0, PK_O^{(3)} = d_o P_2, PK_{i,o} = d_o(PK_i - P_2)$，其中 $i \in \mathbb{U}$，返回 (SK_O, PK_O)。

（3）数据加密。CSP 部分加密算法 $Part.Enc(params,T,SK_O,M)$，选择 $\gamma \leftarrow \mathbb{Z}_q$，计算 $\{q_{v_i}(0)\}_{v_i\in L_T} \leftarrow Share_q(r+SK_O,T)$ 以及 $C_1 = E_1^{-r}M$，$\tilde{r} = r + SK_O$，输出部分密文 $PCT_T = (T, C_1, \tilde{r}, \{q_{v_i}(0)\}_{v_i\in L_T})$。CSP 完整加密算法 $Full.Enc(params,PCT_T,PK_O)$，输入部分密文 $PCT_T = (T,C_1,\tilde{r},\{q_{v_i}(0)\}_{v_i\in L_T})$ 和一个 DO 的公钥 $PK_o = (PK_O^{(1)},PK_O^{(2)},PK_O^{(3)},\{PK_{i,0}\}_{i\in\mathbb{U}})$，计算 $C_2 = \tilde{r}P_2 - PK_O^{(3)} = rP_2, C_3 = E_2^{-r}(PK_O^{(1)}) = E_2^{-r}$，$C_{v_i}^{(1)} = (q_{v_i}(0) - SK_o)P_o$，$C_{v_i}^{(2)} = (q_{v_i}(0) - SK_o)(PK_i - P_2)$，输出密文 $CT_T = (T,C_1,C_2,C_3,C_{v_i}^{(1)},C_{v_i}^{(2)})$。

（4）数据解密

① $TokenGen(params,id_u,SK_u,CT_T)$：输入 Du 的满足属性集 Att_u 的密钥 $SK_u = \{SK_i,u\}_{i\in Att_u}$，满足属性树 T 的密文 CT_T、身份 ID id_u，计算 $K = k\,id_u$，$K_i = k\,SK_{i,u}$，其中 $k \leftarrow \mathbb{Z}_q$，输出 $TK_u = (K,\{K_i\}_{i\in S})$。

② $Part.Dec(params,CT_T,TK_u)$：输入密文 $CT_T = (T,C_1,C_2,C_3,C_{v_i}^{(1)},C_{v_i}^{(2)})$ 和令牌 $TK_u = (K,\{K_i\}_{i\in S})$，首先计算 $L_i = \dfrac{\hat{e}(K_i,C_{v_i}^{(1)})}{\hat{e}(K,-C_{v_i}^{(2)})} = E_1^{kqv_i(o)}E_2^{kqv_i(o)}\hat{e}(id_u,P_2)^{kqv_i(o)}$，$L = E_1^{kr}E_2^{kr}\hat{e}(id_u,P_2)^{kr}$，返回 $M' = (C',C_1)$，其中 $C' = E_1^{kr}E_2^{kr}$。

③ $Full.Dec(params,M_O,k)$：输入部分密文 M' 和匹配的私钥 k，输出完整消息 $M = C'^{k^{-1}}C_1C_3$。

3　方案分析

3.1　安全性分析

（1）抵抗攻击的安全。本方案中每一个医护人员的属性相关的私钥都是通秘密值被盲目化。该机制具有抵抗合谋攻击的能力，敌手不可以通过组合不同的私钥来伪造更大的属性集来解密。

（2）细粒度访问控制。本方案可以通过使用 CP-ABE 实现对患者健康数据的细粒度访问控制。由于 CP-ABE 证明基于一般双线性群模型的自适应选择明文攻击(IND-CPA)是安全的，所以数据也是安全的。

3.2　性能分析及实验对比

本文列举了几个现有的外包计算 ABE 方案运算开销，并与改进的方案进行了对比分析。用于软件仿真的硬件环境为 Ubuntu 18.10，内存 1024 MB。硬件配置为 Inter(R) Core(TM) i5-7500U，主频 3.4 GHz，内存 8 192 MB，软件环境为 PBC。研究发现这些方案主要的运算时间开销是由某些比较耗时的密码学算法所产生的。所以，本方案在实验的开始阶段优先考虑表 1 所列举的各种运算。

表 1　符号表示

Tab. 1　Symbolic representation

符号	定义
$\lvert Att_u\rvert$	数据用户属性结合
$\lvert\mathbb{U}\rvert$	通用属性结合
$\lvert L_T\rvert$	一个访问数叶子节点数目
S	满足访问树的用户属性集合
T_{e_1}	G_1 中指数运算时间
T_{e_2}	G_2 中指数运算时间
T_p	线性对运算时间
l_{G_1}	G_1 中一个元素的长度
l_{G_2}	G_2 中一个元素的长度

几种基于属性加密的细粒度访问控制方案的运算开销对比，见表 2。Guo et al.提出的方案的解密密钥大小与属性数无关；Lin et al.提出的方案具有高效性和通用性；Lai et al.提出了可验证的外包解密的 ABE。对比结果表明本方案在加解密方面要优于其他方案。

表 2　数据拥有者和数据消费者运算开销对比

Tab. 2　Comparison of computing costs between data owners and data consumers

方案	加密	解密
Guo et al.	$(2\lvert\mathbb{U}\rvert - \lvert L_T\rvert + 3)T_{e_1}$	$(2\lvert\mathbb{U}\rvert - 2\lvert S\rvert + 3)T_{e_1} + 3T_p + T_{e_2}$
Lin et al.	$(2\lvert L_T\rvert + 1)T_{e_1}$	$(\lvert S\rvert + 2)T_{e_1} + T_{e_2}$
Lai et al.	$(6\lvert L_T\rvert + 4)T_{e_1} + 2T_{e_2}$	$(\lvert S\rvert + 4)T_{e_1} + T_{e_2}$
本文方案	T_{e_2}	$(\lvert S\rvert + 1)T_{e_1} + T_{e_2}$

4　结束语

随着数字医疗技术的发展，WBAN 能实时、广泛的产生大量的医疗数据。但是 WBAN 中数据的安全和隐私性一直是急需解决的问题。本文提出了一种 WBAN 环境下基于云计算的轻量级细粒度访问控制方案。在该方案中，数据拥有者通过访问树加密敏感数据，而满足访问策略的数据使用者可以解密此数据。在该方案中，较大部分的加解密运算外包给云服务器，使得数据拥有者和使用者在本地加密的运算开销大大减少。通过安全性和运算开销的对比分析表明，本文所提的方案效率和安全性较高，更具有实用性。

参考文献

[1] 刘毅，宋余庆. 无线体域网技术研究[J]. 小型微型计算机系统，2013，34(8)：1757-1762.

[2] 关志涛，杨亭亭，徐茹枝，等. 面向云存储的基于属性加密的多授权中心访问控制方案[J]. 通信学报，2015，36(6)：120-130.

[3] ODELU V, DAS A K, RAO Y S, et al. Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment[J]. Computer standards & interfaces, 2017, 54(PT.1)：3-9.

[4] PAAR C, PELZ J，马小婷. 深入浅出密码学：常用加密技术原理与应用[M]. 清华大学出版社：北京，2012：247-268.