doi:10.11835/j.issn.1000-582X.2020.013

电力终端基于信任和信誉的灵活数据访问控制

王凌宇[1],傅　宏[1],杨　云[2]
(1. 国网重庆市电力公司 客户服务中心,重庆 400000;2. 国网重庆市电力公司 信息通信分公司,重庆 400014)

摘要:为了解决当前电力缴费终端身份认证和访问控制中存在的口令嗅探、重放攻击、越权操作等问题,提出了一种基于信任和信誉的灵活数据访问控制方案,结合云计算技术将其应用到电力终端设备数据访问控制中。该方案通过使用基于属性的加密和代理重加密、终端设备评估的信任级别和由多个信誉中心生成的用户信誉来共同控制电力终端的数据访问,将用户信任级别和信誉评估的概念集成到加密系统中,以支持各种控制方案和访问策略。通过对所提出方案的安全性和性能分析,证明该方案访问控制的细粒度,数据保密性良好,通信开销灵活可控,计算复杂度低,减少了电力终端设备的负担。

关键词:访问控制;云计算;数据安全;电力终端安全
中图分类号:TP393　　**文献标志码**:A　　**文章编号**:1000-582X(2020)08-117-10

Flexible data-access control based on trust and reputation of power terminals

WANG Lingyu[1], *FU Hong*[1], *YANG Yun*[2]
(1. Customer Service Center, State Grid Chongqing Electric Power Company, Chongqing 400000, P. R. China; 2.Information & Telecommunication Branch, State Grid Chongqing Electric Power Company, Chongqing 400014, P. R. China)

Abstract: In order to solve the problems of password sniffing, replay attack and unauthorized operation in the current power payment terminal identity authentication and access control, in this paper a flexible data-access control scheme based on trust and reputation is proposed, which is applied to the power-terminal equipment data-access control in combination with cloud computing technology. The scheme controls the data access of the power terminal jointly by using attribute-based encryption and proxy re-encryption, the trust level evaluated by the terminal device and the user reputation generated by multiple reputation centers, and integrates the concept of user trust level and reputation evaluation into the encryption to support various control schemes and access strategies. Through the security and performance analysis of the proposed scheme, the fine-grained access control is proved, the data confidentiality is good, the communication overhead is flexible and controllable, the computational complexity is low, and the burden of the power terminal equipment is reduced.

Keywords: access control; cloud computing; data security; power terminal security

收稿日期:2020-03-05
基金项目:国家电网重庆市电力公司电力缴费终端安全防护技术研究项目(SGCQKH00JSJS1800056)。
Supported by Security Protection Technology Research Project on Payment Terminal of the State Grid Chongqing Electric Power Company (SGCQKH00JSJS1800056).
作者简介:王凌宇(1993—)男,助理工程师,主要从事网络与信息安全、大数据安全及智能电网等研究,(E-mail) allon168888@gmail.com。

数据访问通常由数据所有者自己控制。但是在许多情况下,数据所有者不能够或者不知道如何控制,在这种情况下,预置访问控制代理可以降低数据所有者在个人数据管理中的风险。考虑到实践中的上述两种需求,需要设计出能够灵活控制的数据访问方案。目前已有多种用于保护数据访问的解决方案。基于访问控制列表(ACL)的解决方案的缺点是计算复杂度随着数据组的数量[1]或 ACL 中的用户数量线性增长[2]。基于角色的访问控制(RBAC)不能灵活地支持依赖信任的各种数据访问需求[3]。近年来,基于属性加密(ABE)的访问控制方案被提出并用于基于属性控制的云数据访问,以增强灵活性[4-6]。然而,由于属性结构的复杂性,这些解决方案的计算成本通常很高。重要的是,大多数现有方案不支持由数据所有者或访问控制代理以及两者共同控制数据访问,这极大地影响了现有方案的实际部署。使用数据所有者评估的信任度或由可信第三方如信誉中心(RC)以及两者共同评估生成的用户信誉[7]进行访问控制的方式,可以减少存储在云服务供应商(CSP)中数据的访问控制的工作量,但是目前对于多方控制的数据访问的研究还不成熟。

数据安全是云计算中的一个重要问题[8]。用户的私有数据存储在 CSP 的数据中心,以减少设备的存储和计算负担,但 CSP 可能会泄露个人隐私[9]。因此,存储在 CSP 中的关键个人数据通常是已加密的,并且数据的访问受到控制。由于存储在 CSP 的数据可以通过云服务被其他实体访问,如何在 CSP 上控制数据访问是一个重要问题。

综上所述,现有的数据访问控制方案计算复杂度和成本较高,灵活性低,在实际应用中耗费大量资源。针对电力终端数据访问安全,笔者提出一种云计算中基于信任和信誉的可灵活控制数据访问的方案,该方案由电力终端设备设置访问策略,提出对云数据访问的多维控制。终端设备以对称加密方式加密其数据密钥,将该加密密钥分成多个部分,以支持各种控制策略。数据所有者可以基于个体信任评估或由多个 RC 生成的信誉来控制其数据访问,以便在各种情况下确保数据安全性和隐私。

1 系统模型概述

电力终端灵活数据访问控制方案的设计模型如图 1 所示,设计模型主要涉及电力终端、云服务供应商(CSP)、信誉中心(RC)及用户 4 种不同的实体。

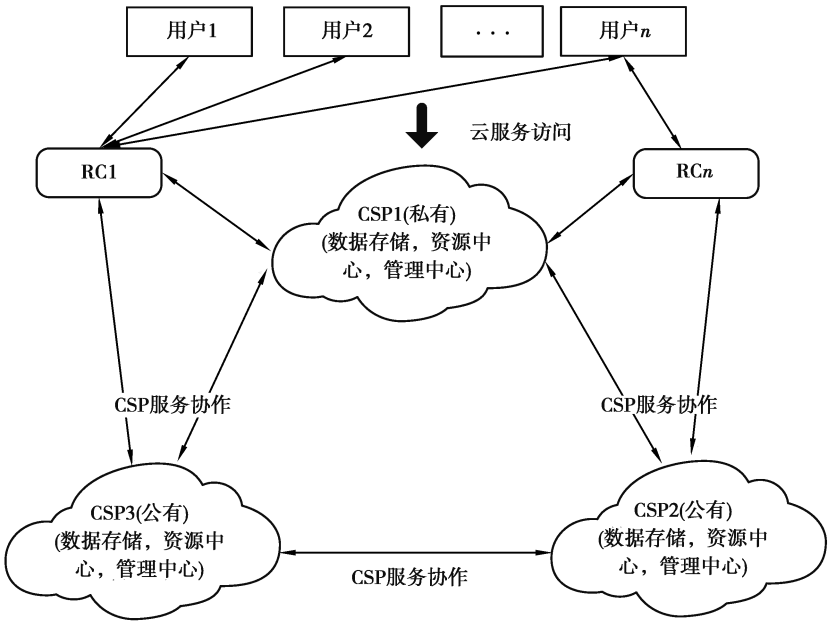


图 1 电力终端灵活数据访问控制系统模型图

Fig. 1 Model of power-terminal flexible data-access control system

1)电力终端:即数据所有者拥有的可信赖的个人设备,可以基于对不同系统实体的个体信任评估来直接控制个人数据访问。有电力服务需求的用户通过终端查询主服务获取电力信息,执行各项操作。

2）CSP：每个 CSP 都有自己的数据存储中心用于存储用户电力数据，是提供各种服务的资源中心以及负责服务请求和提供的管理中心。多个 CSP 可以一起协作以提供用户请求的服务。

3）RC：根据历史行为数据对不同数据访问的系统实体进行信誉评估，生成和提供信誉证书，作为实体数据访问控制中的重要属性。

4）用户：电力数据访问申请者，通过电力终端查询个人或其他实体相关电力数据。

在电力终端灵活数据访问控制系统模型中，RC 作为受信任方在不同数据访问上下文中收集足够的信息进行准确的信誉评估，从而提供每个系统实体的准确信誉信息，系统中可能存在多个 RC。电力设备终端具有可信赖的个人设备，可以基于对不同系统实体的个体信任评估来直接控制个人数据访问。CSP 提供数据存储服务，根据 RC 和终端设备的指令向请求者提供存储的数据。RC 用于数据访问权限的注册和授权，但是不允许 RC 通过 CSP 访问存储的数据。

2　电力终端灵活数据访问控制方案

2.1　相关定义

1）线性映射：设 G 和 G_T 是 2 个具有相同素数阶 q 的循环乘法组，即 $|G|=|G_T|=q$，g 是 G 的生成器。则可得到一个具有以下属性的双线性映射 $e:G\times G\rightarrow G_T$：

a）双线性，对所有 $u,v\in G$，$a,b\in Z_q$，$e(u^a,v^b)=e(u,v)^{ab}$；

b）非退化，对生成器 g，$e(g,g)\neq 1$；

c）可计算，任意 $u,v\in G$，存在有效算法计算 $e(u,v)$。

2）个人信任级别（T_L）是由电力终端基于个人交互和体验评估的信任级别。在此将信任划分为离散级别，例如 T_{Li} 表示 T_L 的第 i 级，$i\in(0,I_{TL}]$，I_{TL} 是 T_L 的最高级别。

3）信誉值（R_V）是信誉中心根据公众反馈和广泛的绩效监控评估的信任值。$R_e(t)$ 表示实体 e 在时间 t 的声誉值。$R_e(t)\in[0,1]$ 表示声誉最坏到声誉最好。

4）代理重加密 PRE 方案表示为多项式时间算法的元组 $(K_G;R_G;E;R;D)$[10]：

a）$(K_G;E;D)$ 是底层公钥加密方案的标准密钥生成、加密和解密算法。当输入安全参数 1^k 时，K_G 输出实体 A 的公钥和私钥对 (k_{pA},k_{sA})。输入 k_{pA} 和数据 M，E 输出密文 $C\_A=E(k_{pA};M)$。输入 k_{sA} 和密文 C_A 时，D 输出明文数据 $M=D(k_{sA};C\_A)$，其中 E 为加密算法，D 为解密算法。

b）输入 $(k_{pA};k_{sA};k_{pB})$，重加密密钥生成算法 R_G 输出实体 B 的重加密密钥 $k_r\_A\rightarrow B$。

c）输入 $k_r\_A\rightarrow B$ 和密文 C_A 时，重新加密函数 R 输出 $R(k_r\_A\rightarrow B;C\_A)=E(k_{pB};M)=C\_B$，可以使用私钥 k_{sB} 解密。

2.2　相关算法

本系统设计主要由密钥生成、密钥切分、代理重加密、解密等几个部分组成，每个算法基本定义如下。

1）Setup：Setup 算法将隐式安全参数 1^k 作为输入。它选择一个带有生成器 g 的素数阶 q 的双线性乘法组 G 和一个映射 $e:G\times G\rightarrow G_T$，选择随机点 $P\in G$ 和随机指数 $y\in Z_q$，然后输出公钥 $K_P=\{G,G_T,e,g,P,e(g,g)^y\}$ 和主密钥 $K_M=g^y$。该过程在用户设备或可信赖的用户代理处进行，同时，每个 RC 生成其公钥 k_{pRC} 和私钥 k_{sRC}。

2）ABEUserKeyGeneration(K_P,K_M,u)：该算法将公钥 K_P、主密钥 K_M 和唯一用户身份 u 作为输入。选择一个随机密钥 $k_{mu}\in Z_q$ 输出公钥 $k_p\_u=g^{k_{mu}}$，将用于为 u 分发加密属性密钥和加密用户密钥 $k_s\_u=K_M\cdot P^{k_{mu}}=g^y\cdot P^{k_{mu}}$，用于解密密文，并从散列函数族中均匀地随机选择散列函数 $H_{k_s\_u}:\{0,1\}^*\rightarrow Z_q$，该过程也在用户设备或可信赖的用户代理处进行。

3）PREUserKeyGeneration(u)：该算法为 PRE 生成公钥 k_{pu} 和私钥 k_{su}[11]。

$$k_{pu}=(Z^{a_1},g'^{a_2}),k_{su}=(a_1,a_2)。\tag{1}$$

系统参数是随机生成器 $g'\in G$，$Z=e(g,g)\in G_T$，$a_1,a_2\in Z_q$。k_{pu} 用于在 RC 为 u 生成重加密密钥。该算法仍然在用户设备或可信赖的用户代理处进行。

4）CreatEncryptionKey()：该算法生成用于数据加密的对称密钥 K，在电力终端执行。在实现中应用

AES(advanced encryption standard)加密算法。

5)DivideKey(K,n):该算法将 K 分成 $n+1$ 部分,$n\geqslant 0$。

6)CombineKey(K_0,K_1,…,K_n):该算法将所有的部分密钥聚合得到完整的密钥 K。

7)CreatIndividualTrustPK(K_P,T_L,k_s_u):当终端要基于个人信任评估来控制其数据的访问时,该算法检查 T_L 相关策略,由设备执行。若符合条件,算法输出用户 u 的 T_L 公共属性密钥,表示为 $k_p\_(T_L,u)$,该密钥由两部分组成:

$$k_p\_(T_L,u)=<k_p\_(T_{Li},u)'=g^{Hk_{s\_u}(T_{Li})},\ k_p\_(T_{Li},u)''=e(g,g)^{yHk_{s\_u}(T_{Li})}>, \tag{2}$$

否则输出为空。其中 $k_p\_(T_L,u)=\{k_p\_(T_{Li},u)\}$,$(i\in[0,I_{TL}])$,$I_{TL}$是 T_L 中的最高等级。

8)IssueIndividualTrustSK(K_P,T_L,k_s_u,k_p_u'):检查 u'的合格性,该算法检查具有公钥 k_p_u'的 u'是否符合属性 T_L 的条件(即它检查 u'位于哪个信任级别)。如果 u'位于信任级别 V_{TL}(V_{TL}是整数且 $V_{TL}\in[0,I_{TL}]$),则 u'有资格获得属性 T_{Li},$i\leqslant V_{TL}$。然后算法输出用户 u'的加密 T_L 密钥 $k_s\_(T_{Li},u,u')$,否则,算法输出为空。

$$k_s\_(T_{Li},u,u')=k_p\_u'^{Hk_{s\_u}(T_{Li})}=g^{k_{mu'}Hk_{s\_u}(T_{Li})},\ (i=V_{TL})。 \tag{3}$$

9)Encrypt0(K_P,K_0,A,$k_p\_(T_L,u)$):该算法将部分密钥 K_0 和公钥 $k_p_(T_L,u)$作为输入,对应于数据中发生的个人信任用户 u 的访问策略 A。该算法用策略 A 加密 K_0 并输出密钥 K_{C0}。访问策略 $A=\vee_{j=1}^{m}T_L\_j$,其中 m 表示所选 T_L 的数量。T_{Lj} 表示由 u 设置的用于控制访问的单个信任级别。$T_L\_j=T_{Lj}$ 意味着 u 给予具有 T_{Li} 级别的用户授权解密密钥。例如,$I_{TL}=5$,$A=T_{L4}\vee T_{L5}$表示 $T_L\geqslant 4$ 的用户可以被授予访问权限。Encrypt0 算法迭代所有 $j=1,2,...,m$,它为策略中的每个所需 T_L 级别 T_{Li} 生成随机值 $R_i\in Z_p$,并生成 K_{C0}^i:

$$K_{C0}^i=\langle E_i=K_0\cdot k_p\_(T_{Li},u)^{nR_i},\ E_i'=P^{R_i}E''_i=k_p\_(T_{Li},u)'^{R_i}\rangle。 \tag{4}$$

此过程在终端设备上进行。所有者将算法的输出及其加密数据发布到 CSP。

10)Decrypt0(K_P,A,K_{C0},$k_s\_(T_L,u,u')$):Decrypt0 算法将 Encrypt0 算法为 u'产生的密钥和密钥环 k'_{su}和 $k_s_(T_L,u,u')$作为输入。如果属性满足用于加密的策略 A,则解密加密密钥 K_{C0}并输出相应的普通密钥 K_0,否则输出为空。

$$K_0=E_i\cdot\frac{e(E_i',k_s\_(T_{Li},u,u'))}{e(E''_i,k_s\_u')}。 \tag{5}$$

验证解密是否正确[12]。

$$a_i:=H_{k_{s\_u}}(T_{Li}),E_i=K_0\cdot e(g,g)^{ya_iR_i},E''_i=g^{ya_iR_i}; \tag{6}$$

$$E_i\cdot\frac{e(E_i',k_s\_(T_{Li},u,u'))}{e(E''_i,k_{s\_u}')}=K_0\cdot e(g,g)^{ya_iR_i}\cdot\frac{e(P^{R_i},g^{k_{mu'}a_i})}{e(g^{ya_iR_i},g^{y}\cdot P^{k_{mu'}})}=$$

$$K_0\cdot e(g,g)^{ya_iR_i}\cdot\frac{e(P,g)^{R_ik_{mu'}a_i}}{e(P,g)^{R_ik_{mu'}a_i}\cdot e(g,g)^{ya_iR_i}}=K_0。 \tag{7}$$

11)ReencryptionKeyGeneration(k_{pRC},k_{sRC},$k_{pu'}$):该算法在文献[11]中定义,输出 $k_r\_RC\rightarrow u=g'^{b_2a_1}=k_{pu'a_1}$,$a_1$ 是 k_{sRC}的一部分,b_2 是 $k_{su'}$的一部分。输入 k_{pRC},k_{sRC}和 $k_{pu'}$,如果算法基于 RC 的最新信誉评估满足电力终端设备的访问策略,则算法为 u 生成重加密密钥 $k_r\_RC\rightarrow u$,然后 RC 将 $k_r\_RC\rightarrow u$ 转发给 CSP。

12)Encrypt1(k_{pRC},K_n):如文献[11]中所定义,终端使用 RC 的公钥加密其部分密钥 K_n($n\geqslant 1$),通过 k_{pRC}获得加密的 K_n,表示为 $E(k_{pRC},K_n)$。

$$E(k_{pRC},K_n)=(g'^{x},K_nZ^{a_1x}), \tag{8}$$

式中:Z^{a_1}是 k_{pRC}的一部分,且 $x\in Z_q$。终端将 $E(k_{pRC},K_n)$及其加密数据发布到 CSP。

13)RE($k_r\_RC\rightarrow u$,$E(k_{pRC},K_n)$):如果 u'被允许访问数据,CSP 产生:

$$RE(k_r\_RC\rightarrow u,E(k_{pRC},K_n))=E(k_{pu'},K_n)=(Z^{b_2a_1x},K_nZ^{a_1x})=K_{Cn}, \tag{9}$$

并发给 u'。用户 u'使用其私钥 $k_{su'}$解密 $E(k_{pu'},K_n)$以获得 K_n。在提出的方案中,CSP 在 PRE 方面起代理作用[11],它间接地将部分加密密钥 K_n 分发给授权实体,而不了解这些密钥的任何信息。

14）Decrypt1($k_{su'}$，$E(k_{pu'},K_n)$)：该算法将 RE 算法生成的密钥和 $k_{su'}$ 作为输入，并解密密钥 $E(k_{pu'},K_n)$。

$$K_n=\frac{K_nZ^{a_1x}}{(Z^{b_2a_1x})^{\frac{1}{b_2}}}。\tag{10}$$

15）Encrypt(K，M)：该算法将输入 K 和数据 M 加密得到密文 C_T。终端将 C_T 发布到 CSP。在实现中应用了 AES。

16）Decrypt(C_T，K)：该算法将加密算法产生的密文 C_T 和完整的加密密钥 K 作为输入，输出明文 M。

2.3　系统方案设计

2.3.1　方案概述

笔者提出了电力终端灵活数据访问控制方案并实现在云服务期间由一个或多个 RC 评估公共信誉。以二维控制为例，电力终端设备使用对称密钥 K 对其数据进行加密，它将 K 分为 2 部分：K_1 和 K_0。分别用 RC 的公钥 k_p_RC 加密 K_1，公共属性密钥 k_p_T_L 加密 K_0，上传加密数据和以上 2 个加密的部分密钥到 CSP。当用户请求访问数据时，CSP 检查用户（即请求者）是否在黑名单中，若检查结果为否定，则 CSP 会根据访问策略将其请求转发给 RC 和电力终端。RC 检查用户的信誉，如果符合策略（例如，用户 e 在 t 时刻的信誉超过预定义的阈值 $R_e(t)>\text{thr}$），则为用户生成重加密密钥解密 K_1，同时，电力终端向请求者发出个性化密钥，以允许其在其信任级别满足访问策略时获得 K_0。得到 K_1 和 K_0 后，请求者可以访问加密数据。

2.3.2　算法流程

图 2 显示了所提出方案的数据访问控制过程。假设电力终端设备在 CSP 上保存了用户 u_1 的个人数据，而用户 u_2 请求在 u_1 和一个 RC 的授权下访问它。

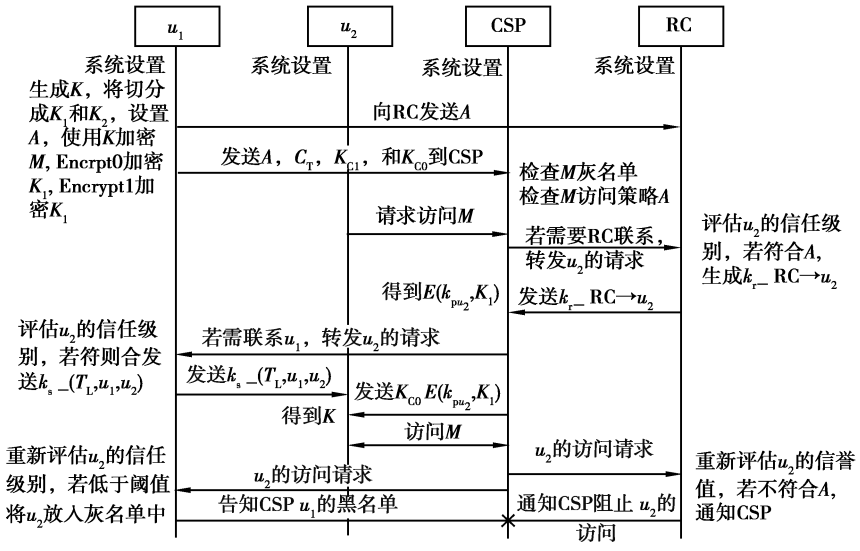


图 2　数据访问控制过程图

Fig. 2　Diagram of data access control process

1）通过调用 Setup 进行系统设置。

2）u_1 生成加密密钥 K 并将其分成 K_0 和 K_1 两部分。使用密钥 K 加密数据 M 以得到 C_T。根据个人信任级别阈值和访问 M 的公共信誉阈值生成数据访问策略 A。u_1 将加密数据 C_T、策略 A 和通过 Encrypt1 加密的 K_1（K_{C1}）、通过 Encrypt0 加密的 K_0（K_{C0}）发送到 CSP，同时 u_1 也将 A 发送到 RC。

3）用户 u_2 向 CSP 发送请求访问 u_1 的数据。CSP 检查其 ID 的有效性和加密 K 的包，以决定是否将此请求转发给 u_1 或 RC（如果 u_2 不在黑名单中）。根据 A 中的内容，CSP 决定是否联系 u_1 或 RC。

4）如果联系 RC，RC 会评估 u_2 的声誉，并检查它是否满足 M 的访问策略 A。根据声誉级别，如果允许访问，RC 生成 k_r_RC→u_2，同时，如果联系 u_1，它会检查 u_2 的合格性，以便为 u_2 生成个性化的密钥 k_s_(T_L，

u_1,u_2)解密 。

5)RC将k_r_RC→u_2发送到CSP重新加密K_{C1}得到$E(k_{pu2},K_1)$;与此同时,u_1向u_2发送k_s_(T_L,u_1,u_2)。CSP允许u_2通过提供相应的加密数据C_T和加密密钥(K_{C1}和K_{C0})来访问所请求的数据。

6)u_2使用u_1发送的密钥及其私钥解密K_{C1}和K_{C0}。通过组合K_1和K_0,u_2可以获得完整的K来解密C_T并获得M。

7)u_1基于过去和新累积的关于数据访问上下文的经验来重新评估u_2,如果u_2已经签发了密钥并且目前失去资格,u_1会将其放入其底层数据访问黑名单并通知CSP。RC可以基于新收集的数据重新生成不同实体的声誉。若RC指示u_2不满足访问策略A,则RC将通知CSP阻止u_2访问u_1的数据。黑名单是面向数据的,因为不同的数据访问可能会请求不同的信任级别。其内容基于及时的信任和信誉评估进行动态升级。

2.3.3 信任评估与信誉生成

用户信任级别可以基于移动社交网络中的数据来评估,笔者应用基于移动社交网络的自动信任评估的具体方法,使信任评估可用。文献[13]中提出了在移动社交网络中计算u_i和u_j两个用户信任值$T_L(u_i,u_j)$的函数,也可以应用其他方法并与所提出的方案合作。

用户反馈、性能监控和报告有助于评估用户信誉。文献[14]提出了一种支持云计算中数据访问控制的具体算法,通过对用户历史数据的分析完成用户的信任评估和信誉生成,对具体的数据访问类型直接评估信任级别并生成信誉。

2.3.4 权限撤销

由于信任和声誉是动态变化的,现应用3种撤销方式动态管理数据访问权限。

1)若数据请求者的信任或信誉级别不满足访问策略,则CSP遵循数据所有者和RC的通知来阻止数据访问,如文献[13]中,每个CSP的信誉都根据用户的反馈进行评估并发布,以确保CSP的良好行为。

2)如果关于K_0的策略发生变化,使用新的T_L属性公钥重新加密K_0并发送新的K_{C0}到CSP。数据所有者还将通知RC更新有关K_n($n\geqslant1$)的新政策。

3)电力终端设备刷新数据加密密钥K并应用新密钥K_0来加密存储在CSP中的新数据。

3 安全性分析

3.1 访问控制的细粒度

本研究中提出的方案可以实现细粒度的访问控制,定义和实施关于信任和信誉的各种访问策略,通过使用基于信任信誉的访问控制替换来消除基于层次属性的细粒度访问控制[7]的复杂性。信任级别的评估包含多种因素,并通过仅考虑一个属性,即信任级别来简化ABE属性结构。信任评估的计算比将信任因子相关属性嵌入到ABE方案的属性结构中复杂得多,信誉生成在RC执行可以减少电力终端设备的计算负担。

3.2 数据保密性

PRE理论、ABE理论、对称加密理论和公钥加密理论确保该方案的安全性,并且应用信任和信誉以异构方式控制数据访问增强了安全性和灵活性。

数据保密性通过对称密钥加密(例如AES)、ABE和PRE来实现。假设对称密钥算法是安全的,所提出的方案的安全性依赖于基于PRE和ABE的架构设计的安全性。即使在$K_n\neq K_0$,$K_0\neq$null的情况下数据请求者持有部分加密密钥(参考$E(k_{pRC},K_n)$),RC也无法访问存储在CSP中的用户数据;同时,用户数据的明文也对CSP隐藏,而CSP无法单独重新委托解密权限,例如k_r_RC→A和k_r_A→B生成k_r_RC→B,因为PRE的非传递属性,即使CSP与已经获得解密权的用户B串联,也只能恢复不完全密钥g^{a1}而不是RC的私钥k_{sRC}。文献[11]证明了标准安全和主密钥安全性,这表明所提出方案中使用的PRE是安全的。此外,当RC为数据请求者发布重加密密钥时,还可以通过根据数据请求者的信誉级别设置惩罚率来实现用户责任[14]。

4　性能分析

4.1　通信开销

通信主要成本包括密文的传输以及 T_L 私钥和重加密密钥的发布。密码文本传输在加密方法中不可避免；私钥和重加密密钥发布的成本是合理的，因为 T_L 私钥仅包含一种类型的属性，如果用户的访问权限是合法的，并且数据所有者不撤销用户权限，则不需要每次在 RC 和 CSP 之间分发重加密密钥，即在 RC 和 CSP 之间分发重加密密钥，若已发出重加密密钥且用户仍然符合条件，则不会重复操作。另外，可以通过选择不同的访问控制方法灵活调整通信成本。

4.2　计算复杂度

分析了以下操作的计算复杂性：初始设置、CP-ABE 用户密钥生成、PRE 用户密钥生成、个人信任公钥和密钥生成、重加密密钥生成和解密。

初始设置和密钥生成包括生成 CP-ABE 用户密钥对、PRE 用户密钥对和重新加密密钥，不受指定的访问策略或属性的影响。因此，上述操作的计算复杂度为 $O(1)$。在访问授权中考虑个人信任级别时，终端需要生成用于加密的单个信任级别公钥，并向符合条件的数据请求者发出私钥。T_L 公钥生成的计算复杂度取决于指定 T_L 级别的总数，因此复杂度为 $O(2I_{TL})$。T_L 私钥生成仅与授权属性相关，计算复杂度为 $O(1)$。

加密包含几个部分：Encrypt、Encrypt0 和 Encrypt1。Encrypt 使用对称密钥 K 加密数据，后两个加密算法使用 CP-ABE 或 PRE 加密部分密钥。Encrypt 的复杂度取决于底层数据的大小，并且在任何加密方法中不可避免。Encrypt0 和 Encrypt1 的复杂度由密钥划分策略以及访问策略中所需的 T_L 级别决定。对于每个 CP-ABE 加密操作，复杂度为 $O(L)$，其中 L 是指定访问策略中的连接数，$L \leqslant I_{TL}$。对包含两个指数的每个 PRE 加密操作，复杂度为 $O(1)$。对于 RC 管理的 n 个部分密钥，复杂度是 $O(n)$。

解密包含两部分，即解密分割的加密部分密钥和使用普通密钥 K 的解密数据。对于 CP-ABE 或 PRE 中的每个解密操作，复杂度为 $O(1)$。因此，解密的总计算复杂度取决于划分的部分密钥的数量，即 $O(n+2)$。

表 1 总结了所提出的方案中每个系统操作的计算复杂性，并将其与两个现有方案，即基于 KP-ABE 的方案[4]和基于 CP-ABE 的方案[6]进行比较。考虑到 n 和 L 的值在实际中很小，例如，$n=1$ 或 2，$L=5$，故本方案效率更高，且灵活性好。

表 1　算法复杂度对比

Table 1　Algorithm complexity comparison

操作	本方案	HABSE[6]	Yu 的方案[4]
初始设置	$O(1)$	$O(1)$	$O(\lvert Y \rvert)$
用户授权	$O(1+n)$	$O(2N_S+S)$	$O(\lvert Y \rvert)$
加密	$O(L+n)$	$O(2\lvert Y \rvert+\lvert X \rvert)$	$O(\lvert S \rvert)$
解密	$O(n+2)$	可变	$O(\max(\lvert Y \rvert, N))$

注：Y 为访问策略树的叶节点数；S 为属性集；N_S 为 S 中的属性数；X 为访问策略树的节点集；N 为乘法组运算的数量。

4.3　计算开销

笔者基于 PBC（Pairing-Based Cryptography）Library[15]、MIRACL 和 JHU-MIT Library 实现了所提出的方案。实验在具有 Intel Xeon CPU E31235 和 2 GB RAM 的服务器上进行，在 Oracle VirtualBox 上运行 Ubuntu 12.04。实验中，设置 $I_{TL}=5$。图 3 为 CP-ABE 设置、CP-ABE 密钥对生成、PRE 密钥对设置和生成、T_L 公钥/私钥生成（$I_{TL}=5$）以及重加密密钥生成的执行时间。除了 T_L 公钥生成之外，这些操作执行时间不受用户对密钥划分的个数或所需单个 T_L 的影响。PRE 密钥对生成比其他生成花费更长的时间，约 58 ms。

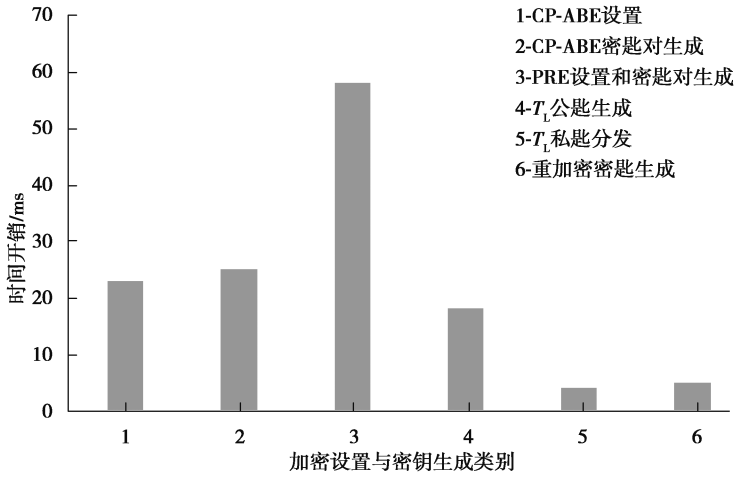


图3 CP-ABE和PRE设置及密钥生成，T_L公/私钥和重加密密钥生成时间

Fig. 3 Time of CP-ABE and PRE settings and key generation, T_L public/private key and re-encryption key generation

图4显示T_L公钥生成的时间随最大信任级别呈线性变化，T_L私钥生成的执行时间保持不变，大约为3 ms，说明T_L密钥生成效率高。

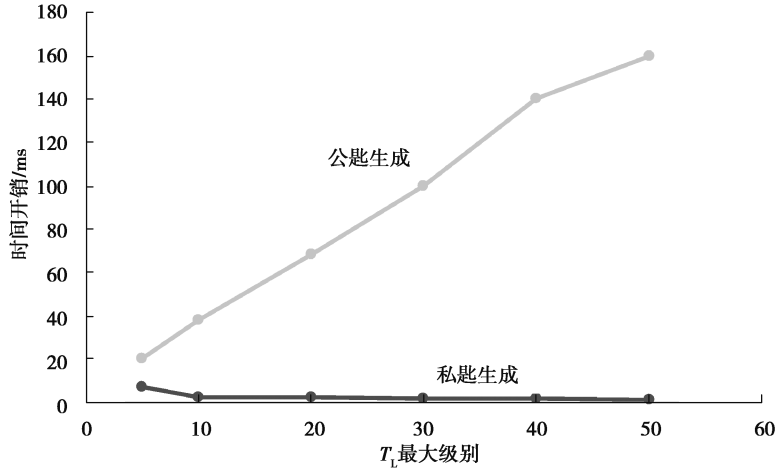


图4 不同T_L级别下CP-ABE T_L公/私钥生成时间

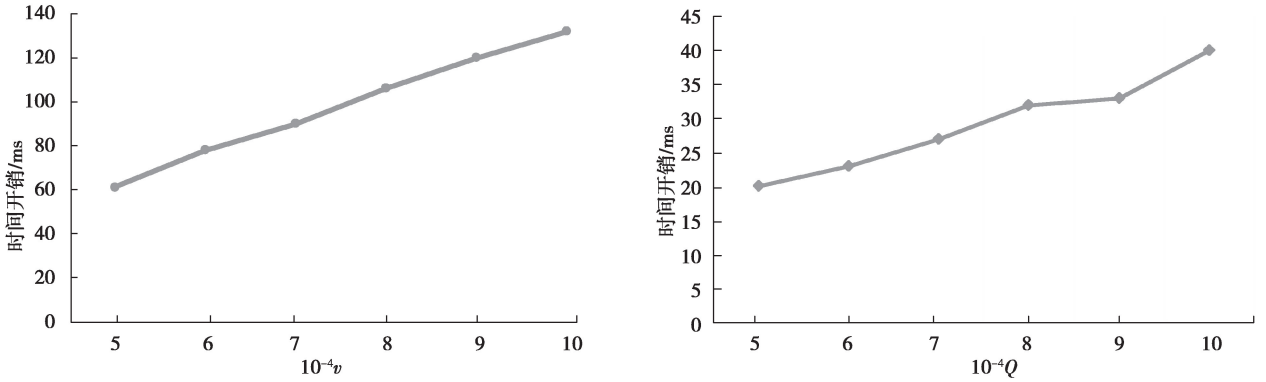
Fig. 4 Time of CP-ABE$T_L$public and private key generation under different maximum $T_L$levels

图5显示了应用文献[13]和[14]中描述的算法，通过策略检查和信任评估生成信誉的执行时间。由图可知投票数v主要影响RC的信誉生成执行时间，同时5(b)表明即使评估请求的数量Q非常大，对于终端设备来说计算负载也是合理的。

实验中，使用AES进行对称加密，测试了3种不同大小的AES密钥：128位、192位和256位。图6(a)(b)显示了关于不同访问策略(即授权的个体T_L)不同大小的AES密钥的CP-ABE加密和解密时间。实验表明AES密钥大小对CP-ABE加密和解密的性能没有太大影响。所需的T_L越高，加密过程花费的时间越少，如图6(a)所示。但是解密时间都是6.50 ms左右(见图6(b))。

图6(c)显示了PRE加密、解密和重加密的性能。由图可知PRE操作同样没受AES密钥大小的明显影响。故数据所有者可选择合适大小的对称密钥以满足其安全要求。

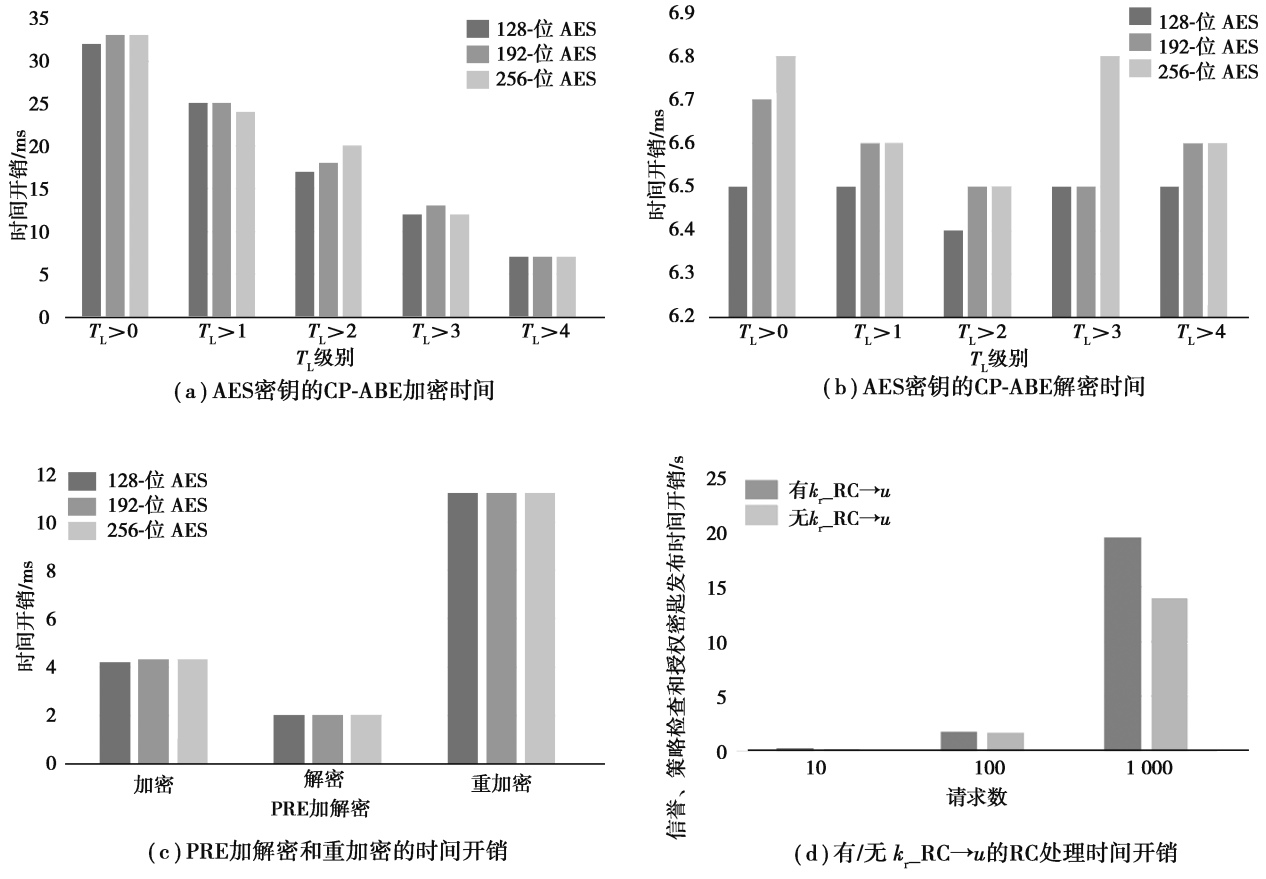
若已生成了重新加密密钥并且用户的信誉仍然存在，则可以在RC处跳过重新加密密钥生成。图6(d)比较了2种情况下RC的处理时间，来自具有RC发布的重加密密钥请求者的请求数越多，节省时间越多，大大提高方案的效率和容量。



(a)信誉生成和策略检查执行时间　　(b)信任评价执行时间

图 5　时间开销图

Fig. 5　Execution time



(a)AES密钥的CP-ABE加密时间　　(b)AES密钥的CP-ABE解密时间

(c)PRE加解密和重加密的时间开销　　(d)有/无 $k_{r_RC\to u}$的RC处理时间开销

图 6　CP-ABE，PRE 加密和解密时间开销

Fig. 6　CP-ABE，PRE encryption and decryption time

5　结　论

笔者提出了一种电力终端基于信任和信誉控制数据访问的方案。该方案采用信任和信誉管理框架，通过应用 ABE、PRE 和基于信誉的撤销机制来保护数据。通过分析和实验证明该方案通信成本低、计算开销小，从而减小了电力终端设备的负担。笔者还基于 ABE 和 PRE 的安全性证明了该方案的安全性，故所提出

的电力终端访问控制方案高效、灵活、安全,具有实际应用价值。

参考文献:

[1] Keerthana S, Monisha C, Priyanka S, et al. De duplication scalable secure file sharing on untrusted storage in big data[C]// 2017 International Conference on Information Communication and Embedded Systems (ICICES), February 23-24, 2017, Chennai, India. IEEE, 2017: 1-6.

[2] 张易鸿, 邱瑞, 陶成义, 等. 访问控制列表 ACL 在网络精细化管理中的作用研究[J]. 无线互联科技, 2016(24): 120-122.
ZHANG Yihong, QIU Rui, TAO Chengyi, et al. Research on effect of the access control list in the network elaborate management [J]. Wireless Internet Technology, 2016(24): 120-122. (in Chinese)

[3] Wang Y, Ma Y, Xiang K Y, et al. A role-based access control system using attribute-based encryption[C]// 2018 International Conference on Big Data and Artificial Intelligence (BDAI), June 22-24, 2018, Beijing, China. IEEE, 2018: 128-133.

[4] Yu S C, Wang C, Ren K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]// 2010 Proceedings IEEE INFOCOM, March 14-19, 2010, San Diego, CA, USA. IEEE, 2010: 1-9.

[5] Zhou M, Mu Y, Susilo W, et al. Privacy-preserved access control for cloud computing[C]// 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, November 16-18, 2011, Changsha, China. IEEE, 2011: 83-90.

[6] Wan Z G, Liu J E, Deng R H. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 743-754.

[7] 许浩海. 基于信誉值的结构化数据访问控制模型研究[D].乌鲁木齐:新疆大学,2018.
XU Haohai. Research on structured data access control model based on reputation value [D]. Urumuqi: Xinjiang University, 2018.(in Chinese)

[8] 薛锐, 任奎, 张玉清, 等. 云计算安全研究专刊前言[J]. 软件学报, 2016, 27(6): 1325-1327.
XUE Rui, REN Kui, ZHANG Yuqing, et al. Foreword to the special issue of cloud computing security research [J]. Journal of Software, 2016, 27(6): 1325-1327.(in Chinese)

[9] Ardagna C A, Conti M, Leone M, et al. An anonymous end-to-end communication protocol for mobile cloud environments[J]. IEEE Transactions on Services Computing, 2014, 7(3): 373-386.

[10] Zhou Y Y, Deng H, Wu Q H, et al. Identity-based proxy re-encryption version 2: making mobile access easy in cloud[J]. Future Generation Computer Systems, 2016, 62: 128-139.

[11] Ateniese G, Fu K, Green M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage[J]. ACM Transactions on Information and System Security, 2006, 9(1): 1-30.

[12] Müller S, Katzenbeisser S, Eckert C. Distributed attribute-based encryption[C]// International Conference on Information Security and Cryptology ICISC 2008. Berlin: Springer, 2008: 20-36.

[13] Yan Z, Li X Y, Kantola R. Personal data access based on trust assessment in mobile social networking[C]// 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, September 24-26, 2014, Beijing, China. IEEE, 2014: 989-994.

[14] Yan Z, Li X Y, Kantola R. Controlling cloud data access based on reputation[J]. Mobile Networks and Applications, 2015, 20(6): 828-839.

[15] Lynn B. PBC library: the pairing-based cryptography library [CP/OL]. [2019-01-25]. http://crypto.stanford.edu/pbc/.

(编辑 罗 敏)