doi:10.3969/j.issn.1000-436x.2014.08.010

面向敏感数据共享环境下的融合访问控制机制

闫玺玺[1]，耿涛[2]
(1. 河南理工大学 计算机科学与技术学院，河南 焦作 454003；2. 中国科学院 信息工程研究所，北京 100093)

摘 要：为解决敏感数据共享应用中的数据分发问题和提高数据共享的安全性，将属性基加密机制和使用控制技术相结合，提出一种融合访问控制机制。该机制一方面采用属性基加密机制保证了数据在存储和分发过程中的机密性，通过灵活且可扩展的访问控制策略控制敏感数据的共享范围；另一方面，通过使用控制技术实现对用户的权限控制，防止合法用户对敏感数据进行非法操作，解决共享用户中的权限滥用问题。最后，对机制的安全性和性能进行了分析，显著地降低了服务端的工作负荷，并通过实验测试了该机制的有效性。

关键词：数据共享；访问控制；属性基加密；使用控制
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)08-0071-07

Fused access control scheme for sensitive data sharing

YAN Xi-xi[1], GENG Tao[2]
(1. School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China;
2. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: In order to improve security of sensitive data sharing and distributing, fused access control scheme based on the mechanism of attribute-based encryption (ABE) and usage control (UCON) was proposed. The scheme could ensure data confidentiality in the storage, distribution process and control sensitive data sharing scope with dynamic access policies. Additionally, the scheme can prevent legal users operating sensitive data illegally and prohibit privilege abuse for domain user.The results of security analysis and efficiency analysis show that fused access control scheme alleviates the administering burdens on data management server and realizes secure storage and distribution for sensitive data.

Key words: data sharing; access control; attribute-based encryption scheme; usage control

1 引言

当前，在分布式网络环境下，资源共享和协作的需求越来越强烈，促使学者们将敏感数据分发方面的注意力从一对一的通信模式转移到一对多的通信模式上。然而，针对一对多的通信模式下实施合理的访问控制是相对困难的。传统的访问控制机制侧重于封闭系统环境中数据的授权保护，系统根据用户的身份或角色赋予用户访问相应数据的权限，仅仅能起到验证用户的功能，不能很好地适应开放式环境下敏感数据的分发，更不能进行动态授权。另外，数据都以明文形式存储在可信服务器上，一旦服务器受到攻击，数据资源将被泄露。为了适应大规模开放式环境下访问控制机制的安全性需求，如何以密码机制为基础构建更为安全的访问控制机制得到了众多学者的关心。

2005 年，Sahai 和 Waters[1]首次在欧洲密码学会议中提出属性基加密(ABE, attribute-based encryption)机制。随后，出现了很多对使用 ABE 实现密文访问控制的研究，文献[2]基于属性基加密机制设计和实现了一个适用于发布/订阅系统的密文访问控制解决方案。文献[3]针对大数据集采用属性基

收稿日期：2013-08-27；**修回日期**：2014-05-05
基金项目：国家自然科学基金资助项目(61300216)；河南理工大学博士基金资助项目(B2013-043)；中国科学院信息工程研究所密码研究专项基金资助项目(Y3Z0032104)
Foundation Items: The National Natural Science Foundation of China (61300216); Research Fund for the Doctoral Program of Henan Polytechnic University(B2013-043); IIE's Research Project on Cryptography (Y3Z0032104)

加密方法提出一种隐私和匿名处理方案。文献[4]针对云存储中敏感数据的机密性保护问题，在基于属性的加密基础上提出了一种高效的密文访问控制方法。属性基加密机制的应用实现了一对多通信模式下资源提供方对数据资源共享范围的控制，但是由于对用户共享域的陌生性和不完全的信息程度，将属性作为单纯的访问控制判决依据并不充分，无法解决共享用户对数据资源的访问控制问题[5~7]。

另外，其余的基于密码学方法实现访问控制方法也存在很多。Crampton 提出基于层次密钥生成与分配策略实施访问控制的方法[8]。Malek 和 Miri 在用户密钥或密文中嵌入访问控制树的方法[9]。针对权限撤销问题，文献[10]提出为密钥设置失效时间，每隔一定时间，用户从认证中心更新私钥。文献[11]对其加以改进，引入了一个在线的半可信第三方维护授权列表。文献[12]提出基于用户的唯一 ID 属性及非门结构，实现对特定用户进行权限撤销。但是上述这些方法在带有时间或约束的授权、权限受限委托等方面仍存在许多有待解决的问题[13,14]。

因此，本文将属性基加密机制和使用控制技术相结合，提出一种面向敏感数据共享环境下的融合访问控制机制，解决大规模开放式环境下敏感数据安全分发问题和提高数据共享的安全性。下文将首先介绍共享环境下敏感数据融合访问控制机制思想，然后描述该机制的具体实现和应用，最后对安全性和性能进行分析，并通过实验测试该机制的有效性。

2 共享环境下敏感数据融合访问控制机制

共享环境下敏感数据融合访问控制架构中，主要涉及 3 个实体，三者关系如图 1 所示。

1) 数据属主(data provider)。数据属主产生敏感数据资源，并将加密后的数据密文上传至内容服务器让其他共享用户进行存取访问，并设定访问规则。

2) 服务端(server)。服务端主要包括内容服务器、授权服务器、密钥管理服务器。内容服务器主要负责对数据密文进行存储、打包封装等操作。授权服务器用于对用户进行注册授权，并对文件的使用权限进行授权管理，设定使用控制策略。密钥管理服务器主要对用户进行密钥的生成、分发和管理。

3) 数据使用者(data user)。只有符合一定属性要求的终端用户才能查看数据，同时，在数据使用者客户端嵌入权限使用监视器对用户进行监视和控制，当用户的使用超出了权限范围时，该监视器会联合授权服务器端对用户进行责任追究，这样既可减少服务器的压力又能防止用户隐私被非法侵犯。

3 融合访问控制机制的具体实现

3.1 符号定义与描述

1) 实体标识符定义

实体标识符定义如表 1 所示。

表 1 实体标识符定义

实体标识符	描述
AU	用户，包括数据属主、数据使用者
RS	授权服务器
CS	内容服务器
O	数据属主
U	数据使用者
F	文件

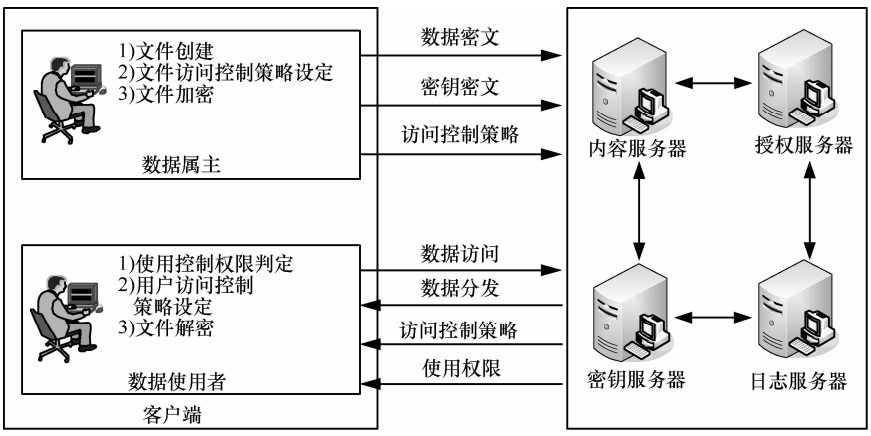


图 1 共享环境下敏感数据融合访问控制架构

2) 相关参数定义

相关参数定义如表 2 所示。

表 2　　相关参数定义

符号	描述
PK	系统公钥
MK	系统私钥
ID_u	用户的身份信息
ID_f	文件的相关编号信息
A_u	属性证书
SK_u	用户属性私钥
k_f	文件内容加密密钥
C_f	文件密文
C_k	内容加密密钥密文
A_c	属性集合，表示访问控制策略
R_u	文件的使用权限
sp	内容服务器的公钥
ss	内容服务器的私钥
$E_x(y)$	采用秘钥 x 加密数据 y
$D_x(y)$	采用秘钥 x 解密数据 y

3.2　协议描述

1) 系统初始化

系统初始化过程通过密文策略属性基加密算法生成系统公钥、主密钥和用户属性密钥，并对用户密钥进行分发，这种方式的优势在于密钥分发是一次性的，访问控制策略的变更不会影响密钥的变化。

①选取 p 阶的双线性群 G_0、G_1，g 表示 G_0 的生成元，$e:G_0\times G_0\to G_1$ 是双线性映射。$\Delta_{i,s}(X)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$ 为拉格朗日参数，S 是一个在 Z_p 的集合，d 为门限参数。

②随机选取随机数 $y(t_1,t_2,\cdots,t_n\in Z_p)$，计算系统公钥为 $PK=(T_1=g^{t_1},\cdots,T_n=g^{t_n},Y=e(g,g)^y)$，主密钥为 $MK=(y,t_1,t_2,\cdots,t_n)$。

2) 用户注册

①用户 AU 向授权服务器 RS 请求注册并提交自己的个人信息 ID_u 以及属性证书 A_u。

$$AU\to RS:register\,\|\,ID_u\,\|\,A_u$$

②授权服务器 RS 验证用户的身份信息是否存在于用户列表中，如存在，则继续验证用户属性证书是否合法，如果不合法，则拒绝用户申请，否则继续

$$\begin{cases}1, & (ID_u=\text{true})\cup(A_u=\text{true})\\ \perp, & \text{其他}\end{cases}$$

③授权服务器 RS 生成属性密钥 SK_u，为用户随机选择一个 $(d-1)$ 次多项式 q，令 $q(0)=y$，并为用户计算属性私钥 $SK_u=\left\{D_i=g^{p(i)/t_i}\right\}_{\forall i\in A_u}$。

④授权服务器 RS 将系统公钥 PK 和用户属性私钥 SK_u 分发给用户

$$RS\to AU:PK,SK_u$$

3) 文件创建及授权

①数据属主 O 创建一个新文件 F，随机生成一个对称密钥 k_f，采用对称加密算法加密文件，得到密文文件 C_f

$$O:C_f=E_{k_f}(F)$$

②为文件 F 制定一个访问结构树 T(代表访问控制策略)，将属性集合 A_c 作为加密的密钥，对对称密钥 k_f 进行加密，得到密钥密文 C_k，具体过程如下：随机选择 $s\in Z_p$，则密文为

$$C_k=(A_c,E=Y^sM=e(g,g)^{ys}M,\{E_i=g^{t_is}\}_{\forall i\in A_c})$$

③计算上述内容的散列值 MD，即 $MD=H(C_f\,\|\,C_k)$。

④采用私钥对 MD 进行签名，即 $FS=Sig_{os}(MD)$。

⑤数据属主 O 采用非对称加密算法和内容服务器的公钥 sp 对 FS、MD、C_f、C_k 进行加密得到 C，将 C 发送给内容服务器 CS。同时，数据属主需要提交文件的相关申请信息，供服务器做参考

$$O\to CS:C=E_{sp}\left(FS\,\|\,MD\,\|\,C_f\,\|\,C_k\right)$$

⑥内容服务器 CS 收到 C 后，通过自己的私钥 ss 解密获得 FS、MD、C_f、C_k

$$CS:FS\,\|\,MD\,\|\,C_f\,\|\,C_k=D_{ss}(C)$$

⑦根据自己的公钥对 FS 进行验证，若验证为 true，则表明消息的真实性。

⑧计算 C_f 和 C_k 的散列值得到 MD'，比较 MD 与 MD'，若相等，则表明消息未被篡改过。

⑨内容服务器 CS 为 C_f 设置一个编号 ID_f，同时存储相应的 C_k。

⑩授权服务器 RS 依据用户提交的文件相关信息，对文件做出等级划分 Lev_f，分为 Lev1、Lev2、Lev3。Lev1 是指最重要的秘密文件，Lev2 是指重

要的秘密文件，Lev3 是指一般的秘密文件，依据文件的等级不同，权限管理办法也不同，包括设置使用操作权限 *use_op*，使用次数 *use_t*，使用期限 *use_d*，使用条件 *use_c* 等具体限制。

$$R=\left(ID_f \| lev_f \| Use\_op \| Use\_t \| Use\_d \| Use\_c\right)$$

4) 文件分发

当文件使用者 U 请求对编号 ID_f 的文件进行访问时，处理过程如下。

①文件使用者 U 生成数据请求信息发送给内容服务器 CS，包括机器信息 ID_c 以及文件编号 ID_f

$$U\rightarrow CS: Request\left(ID_c \| ID_f\right)$$

②内容服务器 CS 收到用户的访问请求后，由解析出 ID_f，检查用户请求的数据是否存在，另外，授权服务器 RS 依据文件的级别 Lev_f 设置相应的使用控制策略 R_u

$$RS: R_u=\left(ID_c \| ID_f \| Use\_op \| Use\_t \| Use\_d \| Use\_c\right)$$

③授权服务器将文件 ID_f 的使用控制策略发送给内容服务器

$$RS\rightarrow CS: R_u$$

④内容服务器 CS 对使用控制策略、访问控制策略以及文件密文打包封装后，发送给文件使用者 U

$$CS\rightarrow U: D=\left(R_u \| A_c \| C_k \| C_f\right)$$

5) 文件访问控制

文件使用者 U 成功接收到文件及策略后，由客户端根据访问控制策略解密文件，按照使用控制策略执行相应的操作，具体过程如下。

Step1 文件使用控制过程

①文件使用者 U 客户端从数据分组 *D* 中解析出文件的使用控制策略 R_u，检测用户机器 ID_c，若与使用控制策略允许的机器序列号不一样，则立即关闭文件，否则继续。

②客户端继续判断用户对文件的操作 *op*、使用次数 *T*、使用时间 *D* 和使用条件 *C* 是否满足使用控制策略所规定的操作权限 *use_op*，使用次数 *use_t*，使用期限 *use_d*，使用条件 *use_c*，若不满足条件则立即关闭文件，否则正常使用文件。

$$Ver=\begin{cases}1, & op\in use\_op \cap T \leqslant use\_t \cap D \\ & <use\_d \cap C\in use\_c \\ \perp, & \text{其他}\end{cases}$$

③由客户端解密模块负责采用属性基解密算法对文件进行解密。

Step2 文件解密控制过程

①文件使用者 U 客户端从数据分组 *D* 中解析出文件的访问控制策略 A_c，根据用户的属性证书 A_u，检验用户属性集与密文属性集相交的元素是否达到系统规定的门限参数 *d*，如满足条件，则继续，否则不响应该请求。

$$Ver=\begin{cases}1, & \left|A_u \cap A_c\right| \geqslant d \\ \perp, & \text{其他}\end{cases}$$

②客户端解密 C_k 得到明文 k_f，选择 *d* 个属性 $i\in A_u \cap A_c$，计算 $e\left(E_i, D_i\right)=e\left(g,g\right)^{p(i)s}$，利用拉格朗日插值找到 $Y^s=e\left(g,g\right)^{p(o)s}=e\left(g,g\right)^{ys}$，得到 $k_f=\dfrac{E}{Y^s}$。

③文件使用者 U 采用对称加密算法解密获得文件明文 F

$$F=D_{k_f}\left(C_f\right)$$

客户端相应的监视器根据用户的操作对用户当前的使用次数做出改动（如次数减 1，$use\_t=use\_t-1$），并对当前的使用时间以及日期做出记录，启动日志系统。

3.3 应用

现以某企业为例对敏感数据的融合访问控制机制进行阐述。假定公司研发部某员工创建了一份新的技术文件，规定只有满足集合{研发一部，经理，3 年以上}3 个条件中 2 个以上条件的员工才可以正常使用文件，同时该文件被公司管理部门认定为重要的秘密文件（Lev2），仅仅可以在上班的时间在办公室的电脑上阅读 2 次，且每次阅读时间为 3 min。现有 3 个不同的员工分别向公司申请查看该文件，用户 1 是研发一部工作 2 年的普通员工，上班时间使用办公室的电脑申请打开该文档，由于不能满足打开该文件的条件，无法正常打开该文件。用户 2 是公司研发二部经理且已工作 5 年，他在加班时间想查看该文件，由于不是上班时间，因此他无法阅读文件。用户 3 是研发一部新上任的经理，上班时间在自己的办公室电脑上可以正常的阅读该文件，但是只能阅读 2 次，且每次阅读时间为 3 min。具体实现如下。

函数定义。

Sebject={*Ower*,*user*1,*user*2,*user*3} //主体对应的集合

Object={ ID_f } //客体对应的集合

Attr(*S*)={ ID_u , A_u , lev_u }//主体对应的属性集合

Attr(*O*)={ ID_f , A_u , lev_u }//客体对应的属性集合

A_c ={*Department*1, *manager, at least* 3 *years working experience*}//文件对应的访问控制策略；

d=2；门限参数；

用户和文件权限设置：

A_{u1} = { *Department*1, *worker*, 2 *years working experience*}//表示用户 1 的属性；

A_{u2} = { *Department*2, *manager*, 5 *years working experience*}//表示用户 2 的属性；

A_{u3} = { *Department* 1, *manager*, 1 *year working experience*}//表示用户 3 的属性

$$R_u=\begin{pmatrix} ID_c,ID_u,ID_f,Use\_op=\{read\},Use\_t=4, \\ Use\_d=2013/08/12, \\ Use\_c=\{ip\in 192.168.100.*,8:00<time<18:00\} \end{pmatrix}$$

//表示文件 ID_f的使用权限

会话过程。

$GetUatt(U,att)=\{ID_c,op,T,D,C\}$ //客户端监视器检索用户所使用的机器序列号，以及操作权限 op，使用次数 *T*、使用时间 *D* 和使用条件 *C*

$GetFatt(F,att)=\{ID_f,A_c,R_u\}$ //获得文件 ID_f 的相关属性，包括访问控制策略和使用权限控制策略

1) 用户 1

$u1\_policy(u1,ID_f,op)$:

$(op="read")\wedge(T="1")\wedge(D="2013/08/11")\wedge$

$(ip=192.168.100.56,time=15:30)$

$\xrightarrow{\text{permiting}} permit(u1,ID_f,read)$

//用户 1 上班时间首次使用办公室的电脑申请打开该文档，满足文件 ID_f 所规定的使用策略

$u1\_att(u1,ID_f,decrypt)$:

$(A_u\cap A_c="department1")\wedge$

$(d="1")\xrightarrow{\text{not}} decrypt(u1,ID_f,decrypt)$

//用户 1 的属性无法满足文件的属性策略，因此，无法正常解密该文件

2) 用户 2

$u2\_policy(u2,ID_f,op)$:

$(op="read")\wedge(T="1")\wedge(D="2013/08/11")\wedge$

$(ip=192.168.100.56,time=19:30)$

$\xrightarrow{\text{not}} notpermit(u2,ID_f,read)$

//用户 2 加班时间首次使用办公室的电脑申请打开该文档，无法满足文件 ID_f 所规定的使用策略

3) 用户 3

$u3\_policy(u3,ID_f,op)$:

$(op="read")\wedge(T="1")\wedge(D="2013/08/11")\wedge$

$(ip=192.168.100.56,time=17:30)$

$\xrightarrow{\text{permiting}} notpermit(u3,ID_f,read)$

//用户 3 上班时间首次使用办公室的电脑申请打开该文档，满足文件 ID_f 所规定的使用策略

$u3\_att(u3,ID_f,decrypt)$:

$(A_u\cap A_c="department1"\text{and}"manager")\wedge$

$(d="2")\xrightarrow{\text{permiting}} decrypt(u3,ID_f,decrypt)$

//用户 3 的属性满足文件的属性策略，因此，用户 3 可以正常解密该文件

$update(T):T=T+1$//更新用户 3 的操作次数

4　安全性及性能分析

4.1　安全性分析

1) 机密性。数据属主首先采用 AES 加密算法对文件进行加密，其次对加密密钥采用属性基加密算法进行加密。数据属主将密钥密文 C_k 和文件密文 C_f 发送给服务端，服务端采用密文的形式进行存储，任何第三方需要用自己的属性私钥 SK_u 计算出密钥，从而获得原始文件明文。非法用户即使截获了密文，由于没有相应的属性解密密钥集，也无法获得密钥。只有合法用户都得能到授权服务器分发的属性私钥，同时只有拥有有效属性私钥的用户才能正常解密。另外，服务端即使被攻击，攻击者得到的也只是密文文件，无法解密获得明文。

2) 属性认证。任何合法用户都可以从内容服务器申请获得文件密文，授权服务端无需主动认证用户，只需要在用户客户端检验用户属性是否满足门限条件，只有满足条件 $|A_u\cap A_c|\geqslant d$ 的用户才能拥有属性相应的解密密钥，可以正确解密数据。用户的属性证书由授权服务器分发，不可伪造，又由于客

户端由监视器对用户的属性认证进行判断，只有拥有合法属性证书的用户才能得到属性解密密钥。

3) 匿名访问。授权服务器为用户颁发属性证书以及属性私钥，任何用户都可以从内容服务器获得文件密文，由用户客户端对属性进行判断，不关心用户的身份，只需要验证用户密钥 A_u 是否满足属性集 A_c。因此，该机制可以实现对数据的匿名访问。

4) 基于使用控制的权限管理。授权服务器对文件的访问权限进行授权管理，设置使用控制策略。在客户端嵌入权限使用监视器对用户进行监视和控制，当用户的使用超出了权限范围时，该监视器会联合授权服务器端对用户进行责任追究，这样既可减少服务器的压力又能防止用户隐私被非法侵犯。同时，通过使用控制技术可以实现对匿名访问的用户进行权限的管理，防止合法用户对文件进行非法操作，导致敏感数据泄露。

5) 客户端安全性。客户端主要负责对数据资源进行加解密和权限使用监视，由于用户的属性证书可以采用 USBkey 的方式存储或者加密存储在客户端，因此即使客户端遭到攻击，由于无法获得用户的属性证书，攻击者不能对敏感数据进行解密。即使客户端遭到攻击，攻击者获得用户的属性密钥，但是用户的权限是与个人的信息绑定的，由于无法确定用户的权限策略，攻击者同样无法正常使用文件。

4.2　性能分析

传统的数据资源访问控制机制中数据属性首先采用对称加密 AES 算法对文件进行加密，其次采用非对称加密算法对加密密钥进行加密。服务端收到密文后需要先采用非对称加密算法进行解密后，再采用数据使用者的公钥对密钥进行加密后发送给数据使用者，由数据使用者采用非对称加密算法进行解密。面向敏感数据的融合访问控制机制主要包括对数据属主、服务端、数据使用者 3 个实体，数据属主首先采用对称加密 AES 算法对文件进行加密，其次采用属性基加密算法对加密密钥进行加密。服务端收到密文后无需进行任何加解密操作，只需要将密文发送给数据使用者。数据使用者得到密文后，采用属性基解密算法对加密密钥进行解密。假定 E_s 表示对称加密操作，E_a 表示非对称加密操作，E_{ab} 表示属性基加密操作，D_s 表示对称解密操作，D_a 表示非对称解密操作，D_{ab} 表示属性基解密操作，具体计算开销比较如表 3 所示，从表 3 中可知本文所提方案大大减轻了服务端的工作负荷。

表 3　　**性能对比**

比较者	数据属主	服务端	数据使用者
传统方案	E_s+E_a	D_a+E_a	D_a+D_s
本文方案	E_s+E_{ab}	0	$D_{ab}+D_s$

4.3　实验分析

服务端为联想台式机，内存 2 GB，操作系统为 Windows XP，用 Microsoft VC++6.0 作为编译工具。由于操作都只与密钥密文有关，不受文件大小影响，现只对 1 MB 文件进行分析。

从表 3 可以看出，本文方案中服务端无需进行任何加解密操作，故只对数据属主和数据使用者进行分析。文件创建及授权阶段，数据属主采用属性基加密算法对密钥进行加密，其时间代价只与数据访问控制结构大小有关。文档解密时，数据使用者采用属性基解密算法，时间代价只与用户的属性数目有关。假定用户拥有的平均属性数目为 5，数据访问控制结构大小在 0~50 波动。数据属主加密时间与数据使用者解密时间代价曲线如图 2 所示。

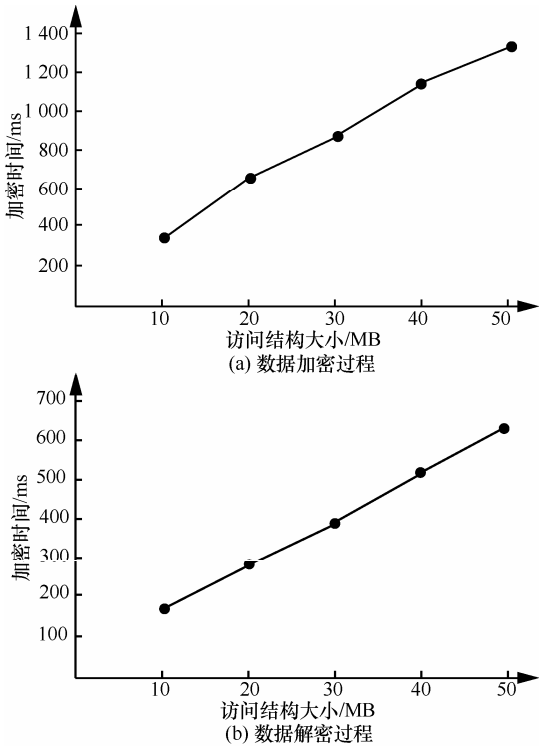


图 2　实验结果

从图 2 可以看出，数据属主加密时间与数据使用者解密时间代价与访问结构大小呈线性关系，访问控制策略越复杂，需要的时间越长。当访问控

制结构大小为 50 时，加密时间为 1 353 ms，解密时间为 638 ms，在可接受范围内，因此，整个方案是有效可行的。

5　结束语

针对共享环境下敏感数据访问控制的安全性要求，本文将属性基加密机制和使用控制技术相结合，提出一种整合访问控制机制，该机制具备以下 4 个优点：①通过属性基加密机制使敏感数据以密文形式存储和分发，保证了数据的机密性，放宽了对服务器的安全限制；②通过制定灵活且可扩展的访问控制策略来控制敏感数据的共享范围，确保只有满足条件的用户才可以获得数据明文；③授权服务端无需主动认证用户，数据使用者通过客户端对用户进行属性认证，大大降低了服务端的工作负荷；④通过使用控制技术实现对用户的权限控制，防止合法用户对敏感数据进行非法操作，解决属性基加密机制的密钥滥用问题。在后续的工作中，将继续研究以密码学为基础实现访问控制，解决大规模开放式环境下访问控制机制的安全性需求。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. Cryptology-EUROCRYPT 2005[C]. Berlin, Heidelberg: Springer-Verlag, 2005.457-473.

[2] MIHAELA I, GIOVANNI R, BRUNO C. Design and implementation of a confidentiality and access control solution for publish/subscribe systems [J]. Computer networks, 2012,56(7):2014-2037.

[3] MUNTES M V, NIN J. Privacy and anonymization for very large datasets[A]. Proc of the ACM 18th Int'l Conf on Information and Knowledge Management,CIKM 2009[C]. New York: Association for Computing Machinery, 2009. 2117-2118.

[4] WAN Z G, LIU J E, ROBERT H D. 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.

[5] NUTTAPONG A, JAVIER H, FABIEN L. Attribute-based encryption schemes with constant-size ciphertexts[J]. Theoretical computer science, 2012, 422(9):15-38.

[6] WANG Y T, CHEN K F, LONG Y. Attribute-based traitor tracing[J]. Journal of Information Science and Engineering, 2011, 27(1):181-195.

[7] WANG Y T, CHEN K F, LONG Y. Accountable authority key policy attribute-based encryption[J]. Science China, 2012, 55(7):1631-1638.

[8] CRAMPTON J, MARTIN K, WILD P. On key assignment for hierarchical access control[A]. Proc of the 19th IEEE Computer Security Foundations Workshop—CSFW 2006[C]. Venice, 2006. 5-7.

[9] MALEK B, MIRI A. Combining attribute-based and access systems[A]. Proc of IEEE CSE2009, the 12th IEEE Int'l Conf on Computational Science and Engineering IEEE Computer Society[C]. 2009.305-312.

[10] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[J]. SIAM Journal on Computing, 2003, 32(3):586-615.

[11] IBRAMI L, PETKOVIC M, NIKOVA S, *et al*. Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes[R]. Centre for Telematics and Information Technology, University of Twente, 2009.

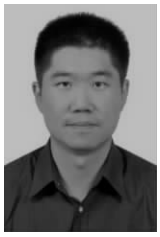
[12] ROY S, CHUAH M. Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption(CP-ABE) System for the DTN[R]. 2009.

[13] BLAZE M, BLEUMER G, STRAISS M. Divertible protocols and atomic proxy cryptography[A]. EUROCRYPT1998[C]. 1998.127-144.

[14] 闫玺玺, 马兆丰, 杨义先等. 多域环境下基于代理重加密的电子文档分发算法及协议分析[J]. 北京邮电大学学报, 2012, 35(5): 81-84
YAN X X, MA Z F, YANG Y X, *et al*. A distribution protocol based on proxy re-encryption in domain environment of E-document management[J]. Journal of Beijing University of Posts and Telecommunications, 2012, 35(5): 81-84.

作者简介：

闫玺玺（1985-），女，河南灵宝人，博士，河南理工大学讲师，主要研究方向为数字版权管理、数字内容安全、计算机网络安全。



耿涛（1983-），男，山东淄博人，博士，中国科学院助理研究员，主要研究方向为信息安全、安全多方计算、数字内容安全。