云存储服务中一种高效属性撤销的AB-ACCS方案

乔 毛 秦 岭

(南京工业大学计算机科学与技术学院 南京 211816)

摘 要 为了提高云存储访问控制(Access Control for Cloud Storage,ACCS)的安全性、高效性,目前国内外云储存服务技术在身份验证、用户授权、数据完整性和加密手段等方面提供了安全性支持,但只是在通信过程中采用https协议对报文进行加密或者引入第三方代理机构对数据文件重加密,导致在跨域共享中存在数据安全隐患,并且在加密过程中存在计算开销大、效率低的问题。为了解决以上问题,提出了云存储服务中一种高效属性撤销的AB-ACCS(Attributes-Based of Access Control for Cloud Storage)方案。该方案通过一种改进的CP-ABE(Ciphertext Policy Attribute Based Encryption))进行访问控制,在不引用第三方代理机构的情况下,云服务提供商(Cloud Storage Provider,CSP)执行密文重加密操作,减少了权威机构和用户的通信负担。同时为了提高该方案在访问控制时的效率,在控制算法上加入新文件创建、新用户授权、属性撤销、文件访问的过程设计,并且结合了懒惰重加密技术,实现了云存储服务中一种高效属性撤销的AB-ACCS方案。实验结果验证了此方案在云存储服务中是有效可行的,并且安全性分析表明其具有向前和向后的双向保密性。

关键词 云存储访问控制,CP-ABE,属性撤销,懒惰重加密

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.07.015

AB-ACCS Scheme for Revocation of Efficient Attributes in Cloud Storage Services

QIAO Mao QIN Ling

(College of Computer Science & Technology,Nanjing Technology University,Nanjing 211816,China)

Abstract In order to improve the security and efficiency of cloud storage access control (ACCS),cloud storage service technologies at home and abroad provide security support for authentication,user authorization,data integrityand encryption methods,but they only use https in the communication process. The protocol encrypts the packet or re-encrypts the data file by a third-party agency,resulting in data security risks in cross-domain sharing. In the encryption process,there are some problems such as large computational overhead and low efficiency. In order to solve the above problems,this paper proposed an AB-ACCS scheme for revocation of efficient attributes in cloud storage services. The solution uses an improved CP-ABE for access control. Without referring to a third-party agency,the CSP performs ciphertext re-encryption operations,which reduces the communication burden between authorities and users. At the same time,in order to improve the efficiency of the program in access control,new file creation,new user authorization,attribute revocation,and file access process design are added to the control algorithm,and a lazy re-encryption technology is combined to implement the proposed scheme. Experiment results verified that this scheme is effective and feasible in cloud storage services,and it shows forward and backward two-way confidentiality in security analysis.

Keywords Access control of cloud storage,CP-ABE,Attribute revocation,Lazy-revocation

1 引言

云计算的快速发展和广泛应用给人们带来了许多便利。云存储[1-2]是云计算的重要服务之一,它为互联网上的数据拥有者提供了灵活的在线数据存储服务,并且将数据外包给云服务器,从而使用户享受按需扩展服务。但与此同时,人们对数据安全的担忧也随之出现。基于属性的加密(Attribute Based Encryption,ABE)[3]是解决数据访问控制的一种有效方案。密文政策属性基加密(CP-ABE)[4]作为公钥加密的一个衍生分支,利用用户密钥与属性的绑定、密文与访问结构的绑定[5],只有与用户密钥绑定的属性集合满足与密文绑定的访问结构时方可解密,使得加解密的对象面向属性,从而极大

到稿日期:2018-05-31 返修日期:2018-08-21

乔 毛(1994—),男,硕士生,主要研究方向为数据挖掘、信息安全与密码学,E-mail:1239494039@qq.com;秦 岭(1980—),男,硕士,讲师,主要研究方向为工业信息化、工业系统集成、计算机应用技术,E-mail:ql@njtech.edu.cn(通信作者)。

地增加了加解密的灵活性。但是，当 CP-ABE 部署在云存储系统中时，动态用户和属性撤销[6-7]对传统的 CP-ABE 方案而言是一个挑战，因而衍生出属性撤销概念。属性撤销在属性基加密中扮演着极为重要的角色，且在权限、访问控制方面发挥着相当重要的作用，其主要是通过撤销属性来影响拥有相关属性的用户权限[8]，从而达到权限控制的目的。该算法方案由于其细粒度的访问控制、实用性高、应用范围广等特点[9]引起了相关研究者的广泛关注。

云存储访问控制(ACCS)[10]是合法访问数据和保护机密数据的重要手段之一。用户通过云服务器接口向云服务器提交访问请求，一旦云服务器接收到用户的访问请求，将识别用户的身份并确定用户的访问权。其工作原理是：数据拥有者在将数据文件存储到云服务器之前对数据文件进行加密，云服务器控制用户对密钥的访问权限，以达到安全访问控制的目的。因此，如何实现高效的密文访问控制和动态属性撤销成为安全云存储服务的首要问题。文献[11]提出了 CP-ABE 中的属性撤销方案，允许授权机构更新密文并生成包含新版本的密钥，然而该方案给权威机构带来了沉重的计算负担，并导致权威机构和用户之间的通信成本增加。文献[12]提出了一种云存储中基于多授权机构可撤销的 ABE 访问控制方法，由各属性授权机构和数据属主分别产生各部分密钥组件，从而建立分散授权结构模型。当发生属性撤销时，不需要修改访问树或者相应密文组件来达到访问控制，但是这种模型用各属性授权机构来代替传统的中央授权机构，导致属性授权机构的数量与用户属性集成正比，对于每个数据属主，都要产生新的参数，加大了系统的计算代价，因此该模型不利于推广使用。

针对以上不足，本文在一种改进的可撤销属性的 CP-ABE 控制访问算法的基础上，加入新文件创建、新用户授权、属性撤销、文件访问的过程设计，并且结合了懒惰重加密[13]，实现了云存储中基于 AB-ACCS 高效可撤销属性的控制访问算法。本文所提方案中，在云服务器不引入第三方代理机构的情况下，当权限被撤销时，CSP 执行大部分重新加密计算[14-15]，减少了权威机构和用户的通信负担，大大降低了数据拥有者的计算成本，同时其不需要为非撤销(持有已撤销属性但未被删除)用户生成更新秘钥，从而不影响其他用户使用该属性的访问权限。此外，该算法实现了向前和向后的双向保密性，且性能分析表明本文所提方案是有效可行的。

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，G_2 都是 q 阶上的循环群，其中 q 为素数。如果映射 $e:G_1\times G_1\rightarrow G_2$，满足以下 3 条性质：

1)双线性(Bilinear)：对于任意的 $a,b\in\mathbb{Z}_p$ 和 $u,v\in G_1$，都有 $e(u^a,v^b)=e(u,v)^{ab}$。

2)非退化性(Non-Degenerate)：存在 $g_1,g_2\in G_1$，使得 $e(g_1,g_2)\neq 1$。

3)可计算性(Computable)：对于任意的 $P,Q\in G_1$，都存在有效的算法计算 $e(P,Q)$。

则称 e 是一个双线性映射。

2.1.2　线性秘密共享方案

一个定义在实体集合上的线性秘密共享机制 Π 满足以下两点：

1)所有实体的共享组成$\mathbb{Z}_q$上的一个向量。

2)存在一个 l 行 n 列的共享矩阵 M。矩阵 M 的每一行由 $\rho(i)$ 标记，其中 $\rho(i)$ 是矩阵的行号 i 到属性的映射。随机选取 $v=\{s,r_2,\cdots,r_n\}$，其中 $s\in\mathbb{Z}_q$ 是要被共享的秘密，$r_2,\cdots,r_n\in\mathbb{Z}_q$，$Mv$ 是根据 Π 得到的关于 s 的 l 个共享组成的向量，其中 (Mv) 属于实体 $\rho(i)$，记作 λ_i。

假定 Π 是访问结构 A 的线性秘密共享方案[16]。对于任何授权 $S\in A$，定义 $I=\{i:\rho(i)\in S\}\subset\{1,2,\cdots,l\}$，存在常数 $\{w_i\in\mathbb{Z}_q\}_{i\in I}$，使得 $\sum_{i\in I}w_i\cdot\lambda_i=S$。而任何非授权集都不存在这样的常数。

2.1.3　懒惰重加密(lazy-revocation)

在可撤销属性的密文访问控制中，当用户撤销其某个属性或属性集时，会导致数据的访问权限发生变化，这意味着需要对数据文件进行重新加密，而对数据文件频繁地重加密通常会造成巨大的计算开销。鉴于此，引入 lazy-revocation 即懒惰重加密的概念，指出如果仅权限撤销则并不进行重加密，只有当云服务器响应用户对数据文件访问的请求时才进行重新加密。

2.2　系统模型

如图 1 所示，云存储服务中高效动态属性撤销的 AB-ACCS 方案的系统模型包含 4 个实体：权威机构(CA)、数据拥有者(DO)、云服务提供商(CSP)、数据用户(DC)。

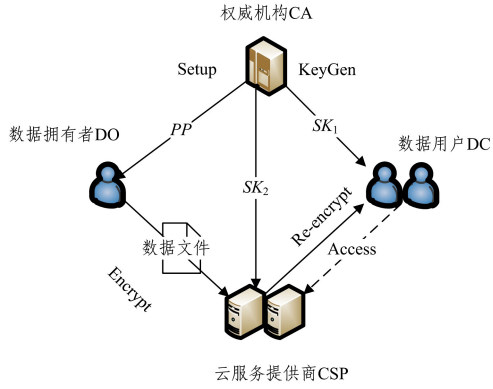

图 1　高效云存储模型

Fig. 1　Efficient cloud storage model

1)权威机构

CA 执行系统初始化程序，管理系统中的属性，生成公共参数和主密钥，公共参数被保存到 DO 中，主密钥发送给 CSP。

2)数据拥有者

DO 负责通过访问策略加密数据文件，执行加密算法。DO 根据输入的明文、访问结构和公共参数生成密文 CT，并将其发送给 CSP。

3)云服务提供商

CSP 负责存储数据拥有者的相关文件及数据信息以及在加密过程中生成的密钥。当发生属性撤销时,CSP 调用密文更新算法对密文进行重加密。在本系统中,只有当 CSP 响应 DC 的请求并且存在属性撤销时,才会调用重加密算法。

4)数据用户

DC 向云服务提供商发出访问请求来获取需要的原始密文或者相应的撤销重加密密文。当且仅当密文属性(去除已撤销的属性)满足与用户密钥绑定的访问结构时,用户才调用解密算法获取明文。

3 云存储服务中高效属性撤销的 AB-ACCS 方案

3.1 云存储中可撤销属性的基加密方案

可撤销属性的 CP-ABE 方案在密钥生成阶段,通过描述主密钥的一组属性集将主密钥随机分成密钥 SK_1 和委托密钥 SK_2,并将其分别发送给用户和云服务提供商,因此授权机构不需要为未撤销的用户生成密钥,从而提高了访问控制的效率。该方案主要包括 5 个算法,详细过程如下。

1)系统建立算法 $Setup(1^\lambda \rightarrow PP, MK)$

系统建立算法由权威机构运行,G 是一个阶为素数 p 的双线性群,g 是群 G 的一个生成元,双线性映射 $G\times G\rightarrow G_T$。过程如下:

选择随机指数 $\alpha_1, \alpha_2, a\in \mathbb{Z}_p$,$\alpha=\alpha_1+\alpha_2$。最后定义一个 hash 函数:$H:\{0,1\}^* \rightarrow G$。该算法取一个安全参数 λ,由式(1)和式(2)输出公共参数 PP 和主密钥 MK:

$$PP=\{g, e(g,g)^\alpha, g^a\} \tag{1}$$

$$MK=\{\alpha_1, \alpha_2, g^a\} \tag{2}$$

2)加密算法 $Encrypt(PP,(M,\rho),M\rightarrow CT)$

加密算法由数据拥有者 DO 运行,(M,ρ)中的 M 是 $l\times n$ 的秘密共享矩阵,其中 $\rho(i)$是矩阵的行号 i 到属性的映射。过程如下:

选取随机向量 $\vec{v}=(s, y_2, \cdots, y_n)\in \mathbb{Z}_p^n$和随机元 $r_1, \cdots, r_n\in \mathbb{Z}_p$,其中 s 是待分享的秘密指数。

对于 $i=1,\cdots,n$,计算 $\lambda_i=M_i\cdot v$,由式(3)生成密文 CT。其中,$\widetilde{C}=Me(g,g)^{\alpha s}$,$C=g^s$,$C_i=g^{a\lambda_i}H(\rho(i))^{r_i}$,$D_i=g^{r_i}$。

$$CT=\{\widetilde{C}, C, \{C_i, D_i\}_{i=1,\cdots,n}\} \tag{3}$$

3)密钥生成算法 $KeyGen(MK, S\rightarrow SK_1, SK_2)$

密钥生成算法也由权威机构运行,其中 S 是描述密钥的一组属性,过程如下:

首先,该算法取主密钥 MK 的部分 α_1,一组属性 S,并且选择一个随机元 $t\in \mathbb{Z}_p$,由式(4)生成用户的密钥 SK_1。其中,$K=g^{\alpha_1}g^{at}$,$L=g^t$,$K_x=H(x)^t$。然后,该算法取主密钥 MK 其余部分 α_2 由式(5)生成委托密钥 SK_2,并且将 SK_2 发送给云服务提供商。

$$SK_1=\{K, L, \forall x\in S, K_x\} \tag{4}$$

$$SK_2=\{D_c=g^{\alpha_2}\} \tag{5}$$

4)密文更新算法 $Re\text{-}encrypt(CT, SK_2\rightarrow \widetilde{CT})$

密文更新算法由云服务提供商运行,其将密文 CT 和委托密钥 SK_2 作为输入,过程如下:

将 ID_i 作为用户 i 的唯一标识,如果有属性 x'被撤销,则该算法需要取一个与撤销属性 x'相关的随机密钥 v_x',并且云服务提供商利用一个随机元 $k\in \mathbb{Z}_p$来加密委托密钥 SK_2,从而由式(6)生成新的密文$\widetilde{CT}$:

$$\widetilde{CT}=\{\{\widetilde{C}, C, C', \{C_i', D_i'\}_{i=1,\cdots,l}\}, D_C', \overset{\wedge}{CT}\} \tag{6}$$

其中,$\widetilde{C}=Me(g,g)^{\alpha s}$,$D_C'=(g^{\alpha_2})^k$,$C=g^s$,$C'=g^{s/k}$,$C_i'=g^{a\lambda_i}H(\rho(i))^{r_i}H(\rho(i))^k$。若 $\rho(i)\neq x'$,则 $D_i'=(g^{r_i}g^k)$;若 $\rho(i)=x'$,则 $D_i'=(g^{r_i}g^k)^{1/v_{\rho(i)}}$。$\overset{\wedge}{CT}$是随机密钥 v_x'在$(\boldsymbol{M},\rho)$访问结构下的密文。

5)解密算法 $Decrypt(\widetilde{CT}, SK_1\rightarrow M)$

解密算法由用户运行,将包含访问结构的密文$\widetilde{CT}$和用于描述属性集合 S 的用户密钥 SK_1 作为输入,得到明文 $\boldsymbol{M}$。过程如下:

如果用户 ID_j 有一个属性 x''撤销,对于用户 $ID_i(i\neq j)$来说,其拥有该撤销属性但是还未被吊销,并且该用户的属性 S 满足访问结构$(\boldsymbol{M},\rho)$,那么解密算法使用 SK_1 来解密$\overset{\wedge}{CT}$,同时获取来 v_x'更新密钥 K_x 从而得到$\widetilde{k_{x'}}=(H(x')^t)^{v_{x'}}$,否则该用户不能更新密钥 K_x。首先利用式(7)计算出 A,然后利用式(8)来表示明文 $\boldsymbol{M}$:

$$A=\prod_{i\in I}B_i=e(g,g)^{ats} \tag{7}$$

$$M=\frac{\widetilde{C}\cdot A}{e(C',D_C')e(C,K)} \tag{8}$$

其中,B_i 用式(9)或式(10)来计算:

$$\rho(i)\neq x'': B_i=\frac{e(C_i',L)^{w_i}}{e(D_i',k_{\rho(i)})^{w_i}} \tag{9}$$

$$\rho(i)=x'': B_i=\frac{e(C_i',L)^{w_i}}{e(D_i',\widetilde{K}_{\rho(i)}))^{w_i}} \tag{10}$$

正确性证明如下:

若 $\rho(i)\neq x''$,则:

$$\begin{aligned}B_i&=\frac{e(C_i',L)^{w_i}}{e(D_i',k_{\rho(i)})^{w_i}}\\&=\frac{e(g^{a\lambda_i}H(\rho(i))^{r_i}H(\rho(i))^k, g^t)^{w_i}}{e((g^{r_i}g^k), H(\rho(i))^t)^{w_i}}\\&=e(g,g)^{at\lambda_i w_i}\end{aligned}$$

若 $\rho(i)=x''$,则:

$$\begin{aligned}B_i&=\frac{e(C_i',L)^{w_i}}{e(D_i',(\widetilde{K}_{\rho(i)})^{w_i}}\\&=\frac{e(g^{a\lambda_i}H(\rho(i))^{r_i}H(\rho(i))^k, g^t)^{w_i}}{e((g^{r_i}g^k)^{1/v_{\rho(i)}}, (H(\rho(i))^t)^{v_{\rho(i)})^{w_i}}}\\&=e(g,g)^{at\lambda_i w_i}\end{aligned}$$

最后可以利用 B_i 来计算 A,并用 A 来计算明文 $\boldsymbol{M}$:

$$\begin{aligned}A&=\prod_{i\in I}B_i=\prod_{i\in I}e(g,g)^{at\lambda_i w_i}\\&=e(g,g)^{ats}\frac{\widetilde{C}\cdot A}{e(C',D_C')e(C,K)}\\&=\frac{Me(g,g)^{as}\cdot e(g,g)^{ats}}{e(g^{s/k},(g^{\alpha_2})^k)e(g^s,g^{\alpha_1}g^{at})}\\&=\boldsymbol{M}\end{aligned}$$

说明：若解密者对于第 i 行所对应的属性被撤销，则其只能恢复出 $e(D_i', \widetilde{K}_{\rho(i)})^{w_i}$ 或 $e(D_i', k_{\rho(i)})^{w_i}$ 这样一个随机值。因此，无论第 i 行所对应的属性是否被撤销，解密者都无法计算出 $e(C_i', L)^{w_i}$ 的值，即回复明文的信息片段是与用户的密钥绑定的。

3.2　云存储服务中一种高效属性撤销的 AB-ACCS 方案

为了实现对外包数据安全和细粒度的访问控制，在 3.1 节的基础上，通过写入对新文件的创建、新用户授权、属性撤销、文件访问的设计，并结合懒惰重加密的思想实现了 AB-ACCS 方案。但是由于在实际应用中单个数据文件通常较大且文件数量较多，如果直接采用属性基加密技术对其进行加密会产生大量的双线性对计算，因此本方案在新文件创建的过程中先采用对称加密机制[17]（Advanced Encryption Standard，AES）随机生成数据加密密钥，如图 2 所示，然后利用该密钥加密数据文件，具体方案如下所述。

1）系统初始化设置：在这个操作中，数据拥有者 DO 调用 3.1 节中的 Setup 算法。DO 随后对 PP 的每个组件进行签名，并将 PP 和这些签名发送给云服务提供商。

2）新文件创建：将文件上传到云服务提供商之前，DO 需要对数据文件进行如下预处理：①为这个数据文件选择一个唯一标识 ID，利用 AES 算法随机生成一个数据加密密钥 DEK（Data Encryption Key），并使用 $DEK(F,K)$ 来加密数据文件，其中 K 是密钥空间；②为这个数据文件定义一组属性 I，基于 3.1 节方案中的 $Encrypt(PP,(\boldsymbol{M},\rho),DEK\rightarrow CT)$ 算法用属性 I 加密 DEK。

3）新用户授权：如果有新用户想要加入系统进行访问时，DO 首先要验证申请的新用户，然后完成如下步骤：①为新用户分配唯一标识 w 和属性集 $S\subset I$；②调用 $KeyGen(MK,S\rightarrow SK_1,SK_2)$ 算法为新用户 w 生成用户密钥 SK_1；③用公共参数 PP 加密元组 $(PP,SK_1,S,\delta_{O,(PP,SK_1,S)})$；④将数据元组发送给云服务提供商并将密文 CT 发送给用户；⑤用户在接收到 CT 之后，先验证签名 $\delta_{O,(PP,SK_1,S)}$ 是否正确，如果正确，则用用户的私钥对其解密。

4）属性撤销：每当有用户的属性被撤销时，DO 首先确定一组最小的属性，不满足此属性访问结构的用户将不能进行控制访问，然后通过在 MK 中重新定义其对应的系统主密钥组件来更新这些属性，并且 DO 为可以进行控制访问的所有用户（除了被撤销的用户）更新 SK_1，最后调用 3.1 节方案中的 Re-encrypt 算法，对数据文件的 DEK 进行重新加密。

5）文件访问：在访问数据文件的过程中，本文结合懒惰重加密技术来减少计算开销，即只有当云服务器响应用户对数据文件访问的请求时，算法才更新新用户的密钥并重新加密所请求的数据文件。具体步骤如下：当用户接收到云服务器的响应时，用户需要验证数据拥有者的签名属性信息和相应公共参数的组件，如果验证成功，用户将调用 3.1 节中的 $Decrypt(\widetilde{CT},SK_1\rightarrow DEK)$ 算法，利用用户最新的密钥来解密 DEK，最后再用 DEK 解密数据文件。

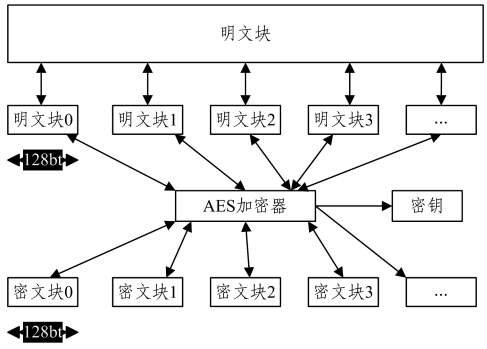

图 2　AES 算法整体结构图

Fig. 2　Overall structure diagram of AES algorithm

4　安全性与性能分析

4.1　安全性分析

1）数据文件的保密性。首先，如果用户的属性不能满足访问结构，显然该用户无法正确验证签名 $\delta_{O,(PP,SK_1,S)}$，故无法解密数据文件。其次，当用户从满足访问结构的属性集中撤销了某个属性时，由于更新了密钥，被吊销的用户也不能解密密数据文件。最后，我们假设云服务提供商是半诚实的，即它对加密的数据好奇但诚实地执行授权分配的任务，由于密文和用户的密钥绑定，而云服务提供商无法获取密钥，因此它不能解密数据文件。

2）正向保密。假设用户从满足密文访问结构的属性集中撤销了某属性，因为被吊销的用户无法满足密文的访问结构，所以不能获取该用户的密钥，即撤销的用户不能解密与其撤销后属性相关的数据文件。

3）向后保密。假设新用户加入了该系统进行访问，并且通过验证获取了该用户的密钥和以前的密文，当有属性被撤销时，该用户只能用之前的密钥 SK_1 来解密 $\widehat{CT}$ 而无法更新密钥 $\widetilde{k}_{x'}$，因此不能计算出 $e(C_i', L)^{w_i}$ 的值，从而不能恢复数据文件。

4.2　性能分析

实验环境为：VBOX 虚拟机上的 CentOS-6.3 操作系统，2 GB 内存，虚拟硬盘存储空间 10 GB，MATLAB2008a 平台，调用 Miracl 代码库来模拟实际运行情况并做出统计性能分析。

4.2.1　通信代价

表 1 列出了各方案通信代价的比较结果，其中，$|g|$ 和 $|g_t|$ 分别是 G 和 G_T 中元素的大小，n_a，n_u 分别代表该系统中属性和用户的总数，l_c 代表所有用于加密的属性数量，k 为授权机构的个数，对于用户 i 来说，$n_{k,i}$ 代表授权机构为其分配的属性个数。在本模型方案中，授权机构和数据属主只需要保存主密钥和公钥，所以授权机构和 DO、DC 之间的通信成本与文献[11]和文献[12]中的方案相比要小得多。而本方案的通信成本主要来自于密文的传输和密文重加密。服务器和 DO 之间的通信成本同文献[11]和文献[12]中的方案相比较低，同时服务器和 DC 之间的通信成本比文献[11]中的方案低，而与文献[12]方案的通信成本相差不大。因此，由表 1 可知，

本方案在总体上的通信成本更低。

表 1 各方案通信代价的比较

Table 1 Comparison of communication costs for each scheme

方案实体	文献[11]	文献[12]	本方案
AC/AA & DC	$(4+n_{k,i})\|g\|$	$2\sum n_{k,i}\|g\|+n_a\|g\|$	$(2+n(k,i))\|g\|$
AC/AA & DO	$(4+2n_a)\|g\|+\|g_t\|$	$(k+2)\|g\|+\|g_t\|$	$2\|g\|+\|g_t\|$
CSP & DC	$(3l_c+1)\|g\|+\|g_t\|$	$2(1+l_c)\|g\|+\|g_t\|$	$(2l_c+3)\|g\|+\|g_t\|$
CSP & DO	$(3l_c+1)\|g\|+\|g_t\|$	$2(1+l_c)\|g\|+\|g_t\|$	$(2l_c+1)\|g\|+\|g_t\|$

4.2.2 计算代价

为了保证数据源的可靠性和实验结果的真实性，在文献[12]数据源的基础上，基于 0.5.12 的 PBC 版本库在不同的情况下进行加密实验比较，实验参数的设置如表 2 所列。

表 2 实验参数设置

Table 2 Experimental parameter setting

参数名称	参数值
用户属性数量	[0,20]
系统属性数量	[0,20]
用户的个数	(0,400]
AES 密钥/bit	128
加密文本大小/k	568

图 3 给出在访问控制的过程中，数据文件的大小为 568k，用户属性个数小于 20 时，密钥生成时间的对比。

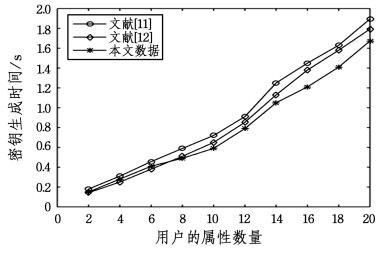

图 3 密钥生成时间与用户属性个数对比

Fig. 3 Comparison between key generation time and number of user attribute

通过图 3 可以看出，由于密钥与用户属性相关，因此当用户属性增加时，密钥生成的时间也随之增加。但是与其他两个方案相比，本方案重加密的密钥由主密钥随机生成，密钥生成时间相对要短，因此在用户属性到达一定数量时，本文的密钥生成的耗时更短。

图 4 给出在访问控制的过程中，数据文件大小为 568k，系统的属性个数小于 20 时，DC 解密数据文件的耗时对比。

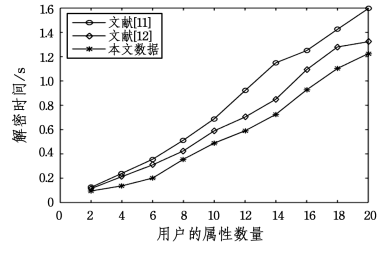

图 4 解密时间与系统属性个数对比

Fig. 4 Comparison between decryption time and number of system attributes

通过图 4 可以看出，随着系统属性个数的增加，本文方案解密数据文件的耗时小于文献[11]和文献[12]，这是因为本方案的密文组件较小，未撤销的用户不需要更新密钥的权限进行通信，所以解密耗时较小。

图 5 给出系统属性数量为 20，用户数小于 400，数据文件的大小为 568k 时 3 种算法在访问控制中权限变更的耗时对比。

通过图 5 可以看出，随着用户数量的增加，本方案在访问控制中权限变更的耗时明显小于其他两个方案，这是因为本方案在一种高效的 CP-ABE 控制算法中结合了懒惰重加密思想，只有当云服务器响应用户对数据文件访问的请求时，所提方案才更新新用户的密钥并重新加密所请求的数据文件，大大减小了计算开销，所以本方案更适用于云存储环境下用户数较大的系统。

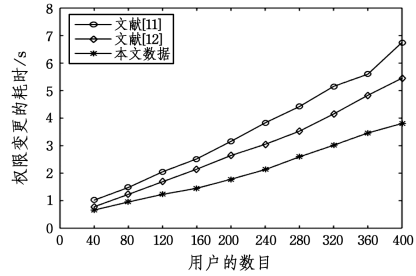

图 5 权限变更耗时与用户数目对比

Fig. 5 Comparison of time-consuming change of permissions and number of users

结束语 云存储中的访问控制一直是近几年的研究趋势和热点，随着研究的深入，其面临着许多挑战。本文基于可撤销属性基加密方案，加入新文件创建、新用户授权、属性撤销、文件访问的过程设计，并结合懒惰重加密技术，提出了一种高效属性撤销的 AB-ACCS 方案，大大降低了用户使用云存储时的存储开销，适用于云存储中用户数量较大的系统，更利于推广。下一步的研究重点是在本文研究的基础上，增加数据文件大小和个数，研究如何控制和减少其权限变更的耗时，实现更加灵活的访问控制。

参 考 文 献

[1] BELGUITH S, KAANICHE N, LAURENT M, et al. PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT[J]. Computer Networks, 2018, 133: 141-156.

[2] WANG F Y, ZHANG Y, GUO X, et al. Multiuser access control searchable privacy-preserving scheme in cloud storage[J]. International Journal of Communication Systems, 2018: 157-165.

[3] JIANG Y H, WILL Y, MU Y, et al. Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts[J]. International Journal of Information Security, 2017, 38(1): 463-475.

[4] ZUO B Y, HUI L, JIAN F M, et al. Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy upda-

ting[J]. Science China Information Sciences,2016,25(2):1-6.

[5] SHI R S,YOSHIAK I,NOMUR A,et al. Attribute Revocable Attribute-Based Encryption with Forward Secrecy for Fine-Grained Access Control of Shared Data[J]. IEICE Transactions on Information and Systems,2017,19(5):2432-2439.

[6] CHANG J W,JIA Y W,JING L,et al. Insecurity of Cheng et al. Efficient Revocation in Ciphertext-Policy Attribute-Based Encryption Based Cryptographic Cloud Storage[C]// Euromicro International Conference on Parallel, Distributed and Network-based Processing. 2017:1387-1393.

[7] WANG J H,WANG G B,XU K Y. Prove CP-ABE scheme supporting large-scale attribute set and attribute-level user revocation under standard model[J]. Journal of Electronics & Information Technology,2017,39(12):3013-3022. (in Chinese)
王建华,王光波,徐开勇. 标准模型下可证明安全的支持大规模属性集与属性级用户撤销的 CP-ABE 方案[J]. 电子与信息学报,2017,39(12):3013-3022.

[8] ZHANG W W,ZHANG Y Z,HUANG X,et al. Data Sharing Scheme for Wireless Body Area Network Supporting Secure Outsource Computing[J]. Journal on Communications, 2017, 38(4):64-75. (in Chinese)
张维纬,张育钊,黄焯,等. 支持安全外包计算的无线体域网数据共享方案[J]. 通信学报,2017,38(4):64-75.

[9] LIU Q,LIU X H,HU B S,et al. Fine-grained access control supporting user revocation in personal health records cloud management system[J]. Journal of Electronics & Information Technology,2017,39(5):1206-1212. (in Chinese)
刘琴,刘旭辉,胡柏霜,等. 个人健康记录云管理系统中支持用户撤销的细粒度访问控制[J]. 电子与信息学报, 2017, 39(5):1206-1212.

[10] ROHIT A,SRABAN K M. A Scalable Attribute-Based Access Control Scheme with Flexible Delegation cum Sharing of Access Privileges for Cloud Storage[C]// International Conference on Advanced Networking Distributed Systems and Applications. 2017:1-4.

[11] YANG K,JIA X. Security for cloud storage systems [M]. Springer:New York,2015:39-58.

[12] LI X H,LIU T,ZHOU M R. Releasable ABE access control method based on multi-authorities in cloud storage[J]. Application Research of Computers,2017,34(3):897-902. (in Chinese)
李谢华,刘婷,周茂仁. 云存储中基于多授权机构可撤销的 ABE 访问控制方法[J]. 计算机应用研究,2017,34(3):897-902.

[13] HAN T X,DING J Y. Revocation and Optimization Mechanism of Rights for Cloud Computing Storage Platform Based on Dynamic Re-encryption[J]. Science Technology and Engineering, 2015,15(20):108-115. (in Chinese)
韩同欣,丁建元. 基于动态重加密的云计算存储平台权限撤销优化机制[J]. 科学技术与工程,2015,15(20):108-115.

[14] SUN X N,JIANG H,XU Q L. Multiuser ORAM Scheme Based on Binary Tree Storage[J]. Journal of Software,2016,27(6): 1475-1486. (in Chinese)
孙晓妮,蒋瀚,徐秋亮. 基于二叉树存储的多用户 ORAM 方案[J]. 软件学报,2016,27(6):1475-1486.

[15] ZHENG Z H,ZHANG M Q,WANG X A. identity proxy re-encryption scheme for cloud data sharing[J]. Application Research of Computers,2016,33(11):3450-3454. (in Chinese)
郑志恒,张敏情,王绪安. 一种适合云数据共享的身份代理重加密方案[J]. 计算机应用研究,2016,33(11):3450-3454.

[16] YAN X L,ZHI X W,WEN Y Y. Linear (k,n) Secret Sharing Scheme with Cheating Detection[C]// International Computer Conference on Wavelet Actiev Media Technology and Information Processing(ICCWAMTIP). 2015:1-5.

[17] ACHMAD B M,RINA R. File encryption and hiding application based on advanced encryption standard (AES) and append insertion steganography method[C]// Communications Security Conference (CSC). 2018:1-8.