云环境中基于信任分散策略的数据共享方案

作者	张光华，刘会梦，陈振国，许向阳
机构	西安电子科技大学 综合业务网理论及关键技术国家重点实验室；河北科技大学 信息科学与工程学院；华北科技学院 河北省物联网数据采集与处理工程技术研究中心
发表期刊	《计算机应用研究》
预排期卷	2018 年第 35 卷第 3 期
访问地址	http://www.arocmag.com/article/02-2018-03-044.html
发布日期	2017-03-21 09:21:15
引用格式	张光华，刘会梦，陈振国，许向阳. 云环境中基于信任分散策略的数据共享方案[J/OL]. [2017-03-21]. http://www.arocmag.com/article/02-2018-03-044.html.
摘要	针对不完全可信云环境中数据共享的安全问题，提出基于信任分散策略的数据共享方案。将原始数据拆分成动态数据和静态数据，动态数据采用在用户私钥内添加全局标志的密文策略属性基加密算法加密存储于一个云端，并在用户撤销时利用代理重加密技术改变访问结构。静态数据采用对称加密算法加密，存储于另一云端。安全性分析和实验表明，文中方案能有效防止动态数据的串谋攻击并保证用户撤销的后向安全性，满足实际云环境中数据安全共享需求。
关键词	数据共享，信任分散，云环境，属性加密，代理重加密
中图分类号	TP309.2
基金项目	国家自然科学基金资助项目（61572255）；中国博士后科学基金资助项目（2015M582622）；物联网信息安全技术北京市重点实验室开放课题（J6V0011104）；河北省科技计划支撑项目（15210338）

云环境中基于信任分散策略的数据共享方案 *

张光华[1,2]，刘会梦[2]，陈振国[3]，许向阳[2]

(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，西安 710071；2. 河北科技大学 信息科学与工程学院，石家庄 050000；3. 华北科技学院 河北省物联网数据采集与处理工程技术研究中心，河北 三河 065201)

摘 要：针对不完全可信云环境中数据共享的安全问题，提出基于信任分散策略的数据共享方案。将原始数据拆分成动态数据和静态数据，动态数据采用在用户私钥内添加全局标志的密文策略属性基加密算法加密存储于一个云端，并在用户撤销时利用代理重加密技术改变访问结构。静态数据采用对称加密算法加密，存储于另一云端。安全性分析和实验表明，文中方案能有效防止动态数据的串谋攻击并保证用户撤销的后向安全性，满足实际云环境中数据安全共享需求。

关键词：数据共享；信任分散；云环境；属性加密；代理重加密

中图分类号：TP309.2

Data sharing scheme based on trust decentralization in cloud environment

Zhang Guanghua[1,2], Liu Huimeng[2], Chen Zhenguo[3], Xu Xiangyang[2]

(1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China; 2. College of Information Science & Engineering, Hebei University of Science & Technology, Shijiazhuang 050000, China; 3. Hebei Engineering Technology Research Center for IOT Data Acquisition & Processing, North China Institute of Science & Technology, Sanhe Hebei 065201, China)

Abstract: According to the security problem of data sharing in the environment of incomplete credible cloud, this paper proposed a data sharing scheme based on the decentralization strategy of credit. This scheme divided the original data into dynamic and static data. The dynamic data's encryption used ciphertext-policy attribute-based encryption algorithm that added the personal identification in the user's private key, and then a cloud stored it. At the same time, this scheme used the proxy re-encryption technology to change the access structure when the user revoked. The static data's encryption used a symmetric encryption algorithm, and another cloud stored it. The security analysis and experiments show that the proposed scheme can effectively prevent the collusion attack of dynamic data and guarantee the backward security of users, which can meet the requirement of data security sharing in the real cloud environment.

Key Words: data sharing; trust distribution; cloud environment; attribute encryption; proxy re-encryption

0 引言

云计算是一种以并行与分布式计算以及虚拟化技术为基础的计算模式，供用户通过网络访问共享资源池，以最少投入为用户提供灵活便捷的多种服务[1]。用户将原始数据上传后，通过资源虚拟化的方式共享存储资源，避开了冗杂的管理环节，不足之处是用户失去对数据的完全控制权，共享数据的安全性依赖于云服务商。目前云服务提供商能力有限，其可信度并未达到百分之百，不断爆出的安全事故使用户对云环境中的数据安全性和隐私性产生质疑[2]。为了满足数据安全性要求，用户将共享数据以密文形式集中存储在一个云端，仅授权用户有权获得共享数据，在一定程度上降低了数据泄露风险系数，同时也引入了其他问题。

a）数据属主将上传数据集存储于一个云端，若该云服务商由于谋取私利或其他原因泄露共享数据，则攻击者未经授权获取全部原始数据，共享数据全部泄露。

b）数据共享方案中，密钥管理是保证数据安全的重要环节。如果非法用户之间采用联合属性私钥的方式获取解密密钥，则非法用户就能通过串谋解密共享数据。另外，当系统中用户需要撤销时，若数据加密密钥保持不变则撤销用户可以继续访问

基金项目：国家自然科学基金资助项目（61572255）；中国博士后科学基金资助项目（2015M582622）；物联网信息安全技术北京市重点实验室开放课题（J6V0011104）；河北省科技计划支撑项目（15210338）

作者简介：张光华（1979-），男，河北深州人，副教授，博士，主要研究方向为信任管理、无线网络安全（xian_software@163.com）；刘会梦（1991-），女，河北石家庄人，硕士，主要研究方向为网络安全；陈振国（1976-），男，山东冠县人，副教授，博士，主要研究方向为网络安全、物联网；许向阳（1966-），男，河北承德人，副教授，硕士，主要研究方向为信息网络管理.

并解密共享数据，无法保证用户撤销时的后向安全性。

针对以上数据共享中存在的安全隐患，本文提出云环境中基于信任分散策略的数据共享方案，解决数据存储过程中的信任集中问题，防止数据共享过程中的串谋攻击并且保证用户撤销时后向安全性[3]。根据信任分散策略，将属主的原始数据拆分成动态数据和静态数据分别进行加密处理，存储于不同云服务器上，即使一方数据泄露，攻击者也无法获取完整数据，降低数据泄露风险。其中静态数据采用对称加密算法进行加密处理，存储于某一云端。动态数据则采用 CP-ABE（Ciphertext-Policy Attribute-Based Encryption, 密文策略属性基加密）算法加密，服务器生成用户私钥，通过在用户私钥内嵌入用户的全局标志，使得每个用户使用自己的私钥加密数据时带有全局唯一的标志信息，以抵抗串谋攻击。云环境中用户撤销是频繁的，动态数据为发生撤销时本文算法只重加密的数据部分，其密文经常处于动态变化。静态数据为每次发生撤销时并不会重加密的数据部分，使得该部分数据在云端的变化频率较低。此外，使用代理重加密技术根据需撤销的属性列表生成代理重加密密钥，在服务器中重加密动态数据，以改变动态数据解密时的属性访问结构，保证系统用户撤销的后向安全性[4]。

1 相关工作

在云环境中，大量用户的敏感数据以共享的方式存储在不完全可信的云服务器上，若没有高效的加密技术和访问控制机制，非授权用户就能够轻易获取数据属主的共享信息，产生数据泄露、丢失等威胁。目前，云环境中数据共享安全问题分两个方面[3]：一是存储数据中存在信任集中问题，二是基于属性的访问控制方法中存在串谋攻击和后向安全问题。

针对第一个研究点，Loftus 等人[5]提出在基于传统的数据加密方案中加入数据分割方法，通过分割将数据划分加密等级，以期达到用较低开销实现数据安全存储在云环境中的目的。Damiani 等人[6]提出一种隐私保护方案，即在上传数据时，将数据分别存储在云服务器和客户端两个平台上，利用分级加密来限制共享数据的访问。文献[3，4，7]采用在加密方案中添加数据分割方法，对数据分级加密，有效减少了系统的计算开销。由上述分析可知，云环境中的数据属主无法对存储在云中的数据完全掌控，迫切需要解决云环境中数据存储的信任集中问题[8]。本文根据信任分散策略，不绝对相信任何一个云平台，将原始数据拆分为动态、静态数据分别处理后存储于不同云端，保证即使一方发生数据泄露，攻击者也无法获取全部共享信息，提高了数据在存储过程中的安全性。

针对第二个研究点，Sahai 和 Waters[9] 等首次提出 ABE（attribute-based encryption, 属性基加密）体制，即用一系列属性标志来表示用户的身份。Bethencourt[10] 等提出了 CP-ABE（ciphertext-policy attribute-based encryption, 密文策略属性基加密）方案，该方案将访问结构部署在密文中，依据用户的属性集合生成用户私钥，满足了云计算中数据共享“一对多”的需求。Wan 等人[11]提出了多层次的云环境下访问控制机制，利用不同等级的授权机构生成用户私钥，防止串谋攻击。Jung 等人[12]通过添加一个全局唯一标志来防止用户的串谋攻击。在这两个方案中，对共享数据进行对称密钥加密，使用 CP-ABE 算法控制用户获取对称密钥，实现访问控制的功能。Hur 等人[13]提出了利用可信第三方来管理属性撤销列表的即时属性撤销的数据外包属性基加密方案。Wang[14]等人通过采用分层域的方法分发密钥，以实现属性撤销。这两种方法对于可信第三方依赖较大，且对于密钥的管理即分发过程较复杂。Yu[15]等人提出了利用代理重加密技术对全部密文数据重加密实现密钥撤销方法，必须重新计算相关访问结构的密文，且计算量与属性的个数呈线性关系，计算所需开销大，对于云计算环境中越来越多的移动端用户来说占用资源高，不适合计算能力低的设备。Liang 等人[16]提出可以快速解密并支持关键字更新功能的基于属性可搜索加密方案。Liao[17]等提出加密方案，通过隐藏用户属性向量的方法来增强属性加密的安全性能。文献[11，12]的方法对于已经获得访问控制权限后的用户无法撤销其对数据的访问，即撤销用户仍然可利用获取的对称密钥解密共享数据，不能保证用户撤销的后向安全性。文献[13~15]中针对用户撤销问题提出解决办法，满足了后向安全性需求，在防止非授权用户根据属性串谋解密密文方面有待完善。文献[16，17]采用密钥策略的属性加密，数据属主无法对密文的访问策略进行设定，并且不支持用户的属性撤销。

本文中动态数据采用 CP-ABE 算法加密，通过在用户私钥内添加全局标志使得非授权用户无法根据公式还原共享文件，防止出现串谋攻击。并且在用户的私钥和密文中嵌入代理重加密技术，若系统用户需要注销则可信第三方对动态数据进行重新加密，撤销用户虽然可以继续访问解密静态数据，但由于不能通过数据完整性验证，最终无法获取原始文件，提高了数据共享的后向安全性。

2 背景知识

2.1 双线性映射

定义 1 双线性映射[18]。设置 $\mathbf{G}_1$、$\mathbf{G}_2$ 为 2 个 p 阶加法循环群，$\mathbf{G}_T$ 为 p 阶乘法循环群，p 为素数，m、n 是 $\mathbf{G}_1$、$\mathbf{G}_2$ 的生成元，$\mathbf{Z}_p$ 为模 p 的加法群。双线性对映射 $e:\mathbf{G}_1\times\mathbf{G}_2\to\mathbf{G}_T$ 应具备以下性质。

a）双线性：$\forall m\in\mathbf{G}_1$，$\forall n\in\mathbf{G}_2$，$\forall a,b\in\mathbf{Z}_p\times\mathbf{Z}_p$，有 $e\left(m^a,n^b\right)=e(m,n)^{ab}$ 成立。

b）非退化性：对于 m、n，有 $e(m,n)\neq 1$，其中，1 为 $\mathbf{G}_T$ 的单位元。

c）可计算性：$\forall m\in\mathbf{G}_1$，$\forall n\in\mathbf{G}_2$，可计算 $e(m,n)$。

2.2 访问结构

定义 2 访问结构[19]。首先给定属性集 $\{P_1,P_2,...,P_n\}$，访问结构为 T，$\Gamma\subseteq 2^{\{P_1,P_2,...,P_n\}}$ 为授权集，$\Gamma^C\subseteq 2^{\{P_1,P_2,...,P_n\}}\setminus\Gamma$ 为非授权集。T 是由多个属性和带有阈值的门限（如 AND、OR）组成的规则，若属性集合满足规则 T 则称为授权集，反之则称为

非授权集。

访问结构T可用访问树进行描述，例如{（（学院：信息）OR（专业：通信工程））AND（（年龄≤23）AND（身高≥175cm））}为访问结构$T1$，仅属性集满足访问结构$T1$的授权用户可访问全部共享数据。

2.3 复杂性假设

定义 3　判定性双线性 Diffie-Hellman（DBDH）假设[19]。定义 **G** 为素数 p 阶群，$g\in_R \mathbf{G}$ 是一个生成元，e 为一个双线性对，随机元素 $a,b,c,d\in_R \mathbf{Z}_p^*$，$A$ 为多项式时间算法。DBDH 问题：给定五元组 $(g,g^a,g^b,g^c,e(g,g)^d)$，判断等式 $e(g,g)^{abc}=e(g,g)^d$ 是否成立。DBDH 假设定义为：在一般情况下，多项式时间 A 内把 $\left[g,g^a,g^b,g^c,e(g,g)^{abc}\right]$ 从组 $\left[g,g^a,g^b,g^c,g^z\right]$ 内选出的概率约等于零，则称群 **G** 满足 DBDH 假设。A 解决 DBDH 问题优势为：$\left|\Pr\left[A\left(g,g^a,g^b,g^c,A=e(g,g)^{abc}\right)=0\right]-\Pr\left[A\left(g,g^a,g^b,g^c,A=R\right)=0\right]\right|\le\varepsilon(k)$式中，$k$ 为足够大的安全参数，$a,b,c,d\in_R \mathbf{Z}_P*$ 和 $\varepsilon(k)$是可忽略的。

定义 4　离散对数问题（DLP）假设。令 **G** 为 p 阶循环群，p 为素数，$g\in\mathbf{G}$ 为生成元，$e:\mathbf{G}\times\mathbf{G}\to\mathbf{G}_T$ 为双线性映射。随机选取 $x\in\mathbf{Z}_p^*$，给定六元组 $\left[\mathbf{G},\mathbf{G}_T,p,e,g,g^x\right]$，概率多项式时间算法 A 计算出 x 发生的概率约为零，事件发生的优势很小，称为离散对数问题（DLP）假设。A 解决对数优势为：$\left|\Pr\left[A\left(G,G_T,p,e,g,g^x\right)=x\right]\right|\le\varepsilon(k)$，式中 $\varepsilon(k)$可忽略。

2.4 CP-ABE 算法

一般的 CP-ABE 算法[10]主要由四个环节组成：Setup、Encrypt、KeyGen、Decrypt，各个环节描述如下。

1）Setup。算法输入系统的安全参数 K，生成并输出公钥 PK 和主密钥 MK。

2）Encrypt（PK，M，A）。算法输入加密公钥 PK、需加密的文件 M 和基于属性的访问结构 A，对 M 进行加密输出密文 CT，$CT=$Encrypt（PK，M，A）。

3）KeyGen（MK,S）。算法输入主密钥 MK 和用户属性集 S，输出用户私钥 SK，其计算公式为 $SK=$KeyGen（MK,S）。

4）Decrypt（PK,CT,SK）。算法输入输入公钥 PK、密文 CT 以及用户属性集 S 产生的私钥 SK。如果 S 满足访问结构 A，则解密成功。

3 基于信任分散策略的共享方案

3.1 总体方案

方案由数据属主、用户、云服务器和可信第三方共 4 类实体组成，基于信任分散策略的共享方案框架如图 1 所示。

方案中各组成实体及功能如下。

a）数据属主：提供共享数据，随机选择参数 ω，利用参数 ω 从原始文件中按字节分割数据，将原始文件拆分成动态数据和静态数据。动态数据抽取自原始文件的小块数据，静态数据为剩余的大块数据。对静态数据采用对称加密算法加密存储于云服务端 B 中，对于动态数据调用 Encrypt 算法加密上传到云服务端 A 中，实现数据的存储与共享。

b）用户：共享数据的使用方，从可信的第三方获取带有全局标志的私钥 SK，若属于云端 B 中的动态加密数据的授权集，则解密动态数据及静态数据，得到授权文件。

c）云服务器：提供可靠、大容量的存储环境，并负责机密信息的管理、运输等，并不排除其出于获利目的而泄露用户数据的可能性。

d）可信第三方：负责 Setup 和 KeyGen 算法的调用，其中在 KeyGen 算法中根据存储系统为用户注册的全局标志，生成相应用户的私钥，并且负责系统中动态数据加密部分访问用户的撤销。

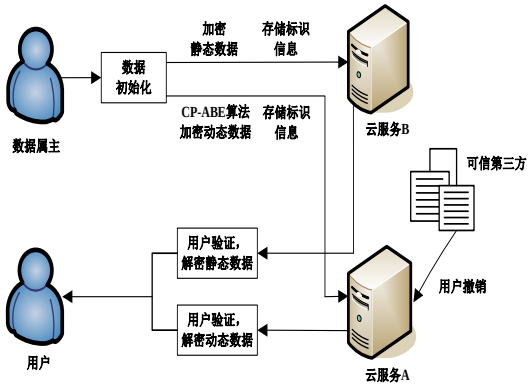

图 1 总体方案框架图

3.2 详述方案

首先对原始数据初始化，将其拆分为动态和静态数据，分别存储于云端 A、B 中。接下来针对这两类数据采用不同的加密策略，静态数据采用对称加密算法加密即可，动态数据进行 CP-ABE 加密以保证数据安全共享，并在动态数据内嵌入全局唯一的标志信息以抵抗串谋攻击。授权用户通过解密动态和静态数据获得共享的原始数据，实现云环境中数据安全共享。若系统中需撤销用户，采用代理重加密技术根据需撤销用户的属性列表生成代理重加密密钥，在服务器中重加密动态数据以实现用户属性撤销，提高后向安全性。

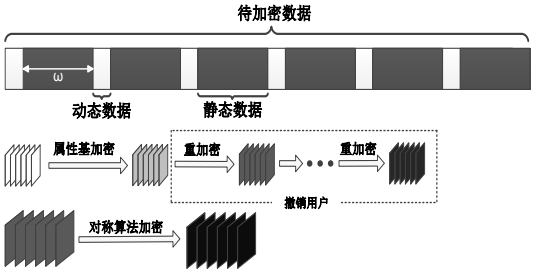

图 2 数据分割及加密示意图

动态数据和静态数据的划分以及各自的加密过程如图 2 所示。深灰色部分为静态数据，抽取自原始待加密数据，占原始加密数据的比例高，并采用对称加密存储于云端；白色部分为动态数据，采用 CP-ABE 加密存储于另一云端，占原始数据比

例低。本文仿真实验使用的待加密数据中，动态数据为搜狗输入法用户常用字词文本字符串按固定长度抽取的字符或者字符串。云环境下用户的撤销是频繁的，若每次发生用户撤销均对整个文件进行重加密，计算开销太高难以满足实际应用。本文算法在发生撤销时只重加密动态数据部分，因此动态数据的加密密文经常处于动态变化，而对于静态数据只需采用对称加密后存储其密文相对变化频率较低，从而降低了系统计算开销。

3.2.1 数据初始化

数据属主在本地将原始数据拆分为动态数据和静态数据，具体流程如下。

a)数据属主上传数据，随机选择参数 ω，从原始数据中固定抽取小块数据作为动态数据，则剩下的大块数据为静态数据，抽取流程如图 3 所示。

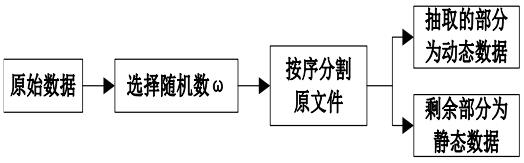

图 3 数据抽取过程

b)将动态数据发送到可信第三方，静态数据采用对称加密算法加密存储于云端 B。同时，存储动态数据和静态数据的相关标志信息。

3.2.2 CP-ABE 加密

可信第三方对动态数据进行带有全局标志的 CP-ABE 加密，具体流程如下。

a）初始化算法。设可信第三方生成系统安全参数 λ_0 作为 Setup 算法的输入，令 $U=\{1,2,...,n\}$ 为属性集空间，随机生成元 g 和阶为 p 的双线性群 $\mathbf{G}$、$\mathbf{G}_T$，双线性映射为 $e:\mathbf{G}\times\mathbf{G}\to\mathbf{G}_T$，同时选取抗碰撞散列函数 $H:\mathbf{G}\to\mathbf{Z}_p^*$，随机选择 $\alpha\in\mathbf{Z}_p^*$，$\beta\in\mathbf{Z}_p^*$，通过 $Y=e(g,g)^{\alpha}$、g^{β}，为每个属性选取随机值 $t_{i,j}\in Z_p(i\in[1,n],j\in[1,n_i])$，其中 $T_{i,j}=g^{t_{i,j}}$，输出主密钥 (g^{α},β) 和公钥 $(G,g,g^{\beta},H,e(g,g)^{\alpha})$，云存储系统生成属性全集 $\Omega=\{\lambda_1,\lambda_2,...,\lambda_n\}$。

b）密钥生成算法。云存储系统为注册用户生成唯一标志 g^{u_i} 和属性集 A，属性集 $A=\{\lambda_1,...,\lambda_i,...,\lambda_j\}$。用户将标志信息 g^{u_i} 和属性集 A 发送给第三方作为 KeyGen 算法的输入。

$$SK=\left(D=g^{\frac{u_i e}{\beta}}g^{\frac{\alpha}{\beta}};\forall\lambda_j\in A:D_k=g^{eu_i}H(\lambda_i)^{r_j},D_k^{'}=g^{r_j}\right)=\left(D=g^{\frac{\alpha+eu_i}{\beta}};\forall\lambda_j\in A:D_k=g^{eu_i}H(\lambda_j)^{r_j},D_k^{'}=g^{r_j}\right)\tag{1}$$

可信第三方使用式(1)为用户生成带有全局标志信息的私钥 SK，用户获取的私钥 SK 可由公式计算得 $SK_{u_i}=(D=g^{\frac{\alpha+u_i e}{\beta}};\forall\lambda_j\in A:D_k=g^{u_i}H(\lambda_j)^{r_j},D_k^{'}=g^{r_j})$。随机选取 $u_0\in\mathbf{Z}_p^*$ 为组私钥 GSK，并发送给注册用户，组公钥 $GPK=g^{u_0}$，其中 $v_n=0$。

c)加密算法。数据属主制定属性访问结构 $W=[W_1,W_2,...,W_n]$，选择动态数据 $m\in\mathbf{G}_T$，计算 $C_0=mY^s e(g,g)^{u_0 s}=me(g,g)^{\alpha s+u_0 s}$，$C_1=g^{\beta s}$，$C_2=g^{\delta s}$，随机选择 $s\in\mathbf{Z}_p^*$。令 s 为动态数据访问结构的根节点，设定根节点为已标志，子节点为未标志，未标志的非叶子节点通过递归运算得到。随机选择 $s_i\in\mathbf{Z}_p$，$1\le s_i\le p-1$，令最后的子节点值为 $s_j=s-\sum_{i=1}^{j-1}s_i \bmod p$，将该节点改为已标志。当为“或”门时，则该节点下的任意节点值为 s，同时将该节点改为已标志。对于叶子节点，通过计算 $C_{i,j,1}=g^{s_i}$，$C_{i,j,2}=T_{i,j}^{s_i}$，输出密文 CT 可由式（2）计算得出。

$$CT=\{C_0,C_1,C_2,\{C_{i,j,1},C_{i,j,2}\}\},\quad i\in[1,n],\ j\in[1,n_i]\tag{2}$$

3.2.3 解密数据算法

静态数据采用对称加密算法加密，按传统算法进行解密，文中着重描述动态数据解密过程。数据用户从存储动态数据的云端获取密文 CT，从可信第三方获取私钥 SK，对比两者的版本号 v_n 是否一致，不一致则需更新私钥。使用嵌套方式计算访问树根节点的节点值，用根的节点值解密数据。

a)对于每个叶子节点 x，当用户不满足数据属主对动态数据设定的访问结构时 $T_x=0$，否则 T_x 计算公式如下。

$$\begin{aligned}T_x&=\frac{e(D_x,C_x)}{e(D_x^{'},C_x^{'})}=\frac{e(g^{u_i\varepsilon}H(\lambda_x)^{r_x},g^{f_x(0)})}{e(g^{r_x},H(\lambda_x)^{f_x(0)})}\\&=\frac{e(g^{u_i\varepsilon},g^{f_x(0)})e(H(\lambda_x)^{r_x},g^{f_x(0)})}{e(g,H(\lambda_x))^{r_x f_x(0)}}\\&=e(g,g)^{u_i\varepsilon f_x(0)}\end{aligned}\tag{3}$$

其中，f_x 是为每个叶子节点 x 定义的一个 (k_x-1) 多项式。

b)自下向上依次执行对于访问树的每个非叶子节点的解密操作。对于条件 $|(s\in N)\wedge(T_s\ne 0)|\ge K_y$，如果所有子节点集合 y 不满足，则令 $T_y=0$，否则计算 T_y 如下。

$$\begin{aligned}T_y&=\prod_{s\in N}e(g,g)^{u_i\varepsilon f_{p(s)}(q(s))\prod_{j\in N,j\ne N}\frac{q(j)}{q(s)-q(j)}}\\&=e(g,g)^{u_i\varepsilon\sum_{s\in N}(f_y(q(z)))\prod_{j\in N,j\ne N}\frac{q(j)}{q(s)-q(j)}}\\&=e(g,g)^{u_i\varepsilon f_y(0)}\end{aligned}\tag{4}$$

其中，$q(x)$ 为节点的编码值，对于根节点 R 的值 $f_R(0)=s$，$s\in Z_p$

为随机选取，对于非叶子节点 y，则有 $f_y(0)=f_{p(y)}(q(y))$。

c)结合计算出的节点值 T_R 和用户私钥可恢复共享数据 M，计算公式如下。

$$M=\frac{me(g,g)^{\alpha\varepsilon s}}{\left[\frac{e((g^{\beta})^{s},g^{\frac{\alpha+u_i\varepsilon}{\beta}})}{e(g,g)^{u_i\varepsilon s}}\right]^{\varepsilon}}$$

3.2.4 用户撤销算法

当需要撤销系统中的用户时，采用代理重加密技术对动态数据进行重加密并更新密钥，具体流程如下所示。

a)重加密算法。可信第三方重新选择随机值 $u_x\in Z_p^*$ 作为组私钥 GSK_x，通过线下通道发送给合法的需要访问数据的用户，同时更新授权用户的私钥部分 $D_{2,v_n}=(g^{1/\beta})^{\lambda x}$。存储动态数据的云服务端 A 向可信第三方发送重加密的操作请求，确保此时正在访问的授权用户能正确解密。密文版本更新 $v_n=x$，可信第三方计算重加密密钥 $CK_v=\{s^{\frac{u_x-u_0}{\delta}}\}$ 发送给存有动态数据的云服务端，云服务端计算版本号 $v_n=x$ 的更新动态密文为 CT_{v_n}，同时计算出 $C_{0,v_n}=C_0e(C_2,CK_{v_n})=me(g,g)^{\alpha s+u_0s}$，$e(g^{\delta s},g^{\frac{u_x-u_0}{\delta}})=me(g,g)^{\alpha s+u_xs}$，其中 s 为随机选择参数并且 $s\in Z_p^*$，计算更新后的密文 CT_{v_n} 为

$$CT_{v_n}=\{v_n=x,\hat{c},C_{0,v_n},C_1,C_2,\{C_{i,j,1},C_{i,j,2}\}\},$$

$$i\in[1,n],\ j\in[1,n_i]$$

b)转换钥生成算法。输入用户的私钥 SK 和系统的公共参数，可通过计算 TK 生成转换钥，并且保存 $HK=z$ 作为恢复钥，其中 TK 由如下方法计算

$$TK=\{D_0^{'}=D_0^{1/z},D_2^{'}=D_2^{1/z},\{D_{i,1}^{'}=D_{i,1}^{1/z},D_{i,2}^{'}=D_{i,2}^{1/z}\}\},$$

$$i\in[1,n],\ j\in[1,n_i]$$

c)转换动态数据算法。输入转换钥 $TK=\{D_0^{'},D_2^{'},\{D_{i,1}^{'},D_{i,2}^{'}\}_{i\in[1,n],j\in[1,n_i]}\}$、密文和系统公共参数，利用公式（6）计算转换后的动态数据为 $K_{v_n}^{'}$，同时计算经过转换后的密文为 $CT^{'}=\{v_n=0,K^{'}=\hat{c},K_1=C_0,K_{v_n}^{'}\}$，其中 v_n 为云服务端计算版本号。

4 安全性分析

本方案将原始文件拆分为动态数据和静态数据分离存储，若一方发生数据泄露，可信第三方因为不能通过数据完整性验证，所以无法恢复完整原始文件，同理当静态数据发生密钥泄露时也无法获得原始文件。动态数据采用可信第三方并在用户私钥内添加全局标志的 CP-ABE 算法加密，能有效防止攻击者之间联合属性私钥解密密文的串谋攻击行为。同时通过代理重加密技术完成用户安全撤销，即在动态数据密钥泄露后保证数据的后向安全性。本文设计的数据共享方案安全性分析如下。

a）抵抗用户串谋攻击。假设两个非法用户 u_i 和 u_j 串谋，两者结合自己的属性私钥获取解密密钥，获取共享数据，通过公式（3）获得叶子节点值集合：$\{e(g,g)^{u_if_x(1)}\ldots,e(g,g)^{u_if_x(m)},e(g,g)^{u_jf_x(n)}\ldots e(g,g)^{u_jf_x(k_x)}\}$，由于叶子节点已经被 u_i 和 u_j 标志，无法通过式(4)还原非叶子节点值，因此可以防止非法用户串谋攻击。

b）后向安全性保证。发现密钥泄露或者用户注销等情况需要撤销用户时，可信第三方利用代理重加密技术对存储动态数据的云服务端进行共享数据更新。即使撤销的用户仍然可以访问解密静态数据，由于缺少动态数据无法完成文件的完整性验证，确保撤销用户不能继续访问共享数据，保证共享数据的后向安全。

c）选择明文攻击游戏[20]。方案模型将系统中的云定义为挑战者 S，将访问系统的用户定义为敌手 A，证明数据共享方案方案的安全性，具体过程如下。

①开始阶段。挑战者 S 选择安全分割文件的参数 η 和一个充分大的 CP-ABE 算法参数 λ 对密文加密，并将动态公钥和静态密钥交给敌手 A。

$$K_{v_n}^{'}=\frac{\prod_{i=1}^{n}e(C_{i,j,1},D_{i,1}^{'})e(C_1,D_0^{'})e(C_1,D_2^{'})}{\prod_{i=1}^{n}e(C_{i,j,2},D_{i,2}^{'})}=e(g,g)^{\frac{\alpha s+u_0s}{z}} \tag{6}$$

②查询阶段 1。敌手 A 提交两个挑战的明文 W_0，W_1 和访问树 ω，向挑战者查询动态数据属性集所对应的用户动态数据私钥 SK。若已查询的动态数据属性集均不满足动态数据访问树，则敌手 A 将明文 W_0，W_1 和访问树 ω 发送给挑战者 S，挑战者 S 随机进行抛硬币实验生成随机数 $\beta\in\{0,1\}$ 以及分割参数 η，对明文 M_β 加密并且将动态密文 C 发送给敌手 A。

③查询阶段 2。敌手 A 继续向挑战者进行动态数据属性集的查询，依旧不满足动态数据属性集的访问树，重复查询阶段 1。

④猜测阶段。挑战者 S 对动态数据密文 C 进行猜测，在 $\beta^{'}=0$ 或者 $\beta^{'}=1$ 中作出应答。若 $\beta^{'}=\beta$，则敌手 A 获胜，敌手 A

获胜优势定义为 $Adv(A)=\left|\Pr[\beta'=\beta]-1/2\right|$。一般情况下敌手 A 成功解密游戏的概率约为零，则本文提出的共享方案可以保证上传数据的安全性。

5　实验仿真及分析

5.1　实验环境

本节对数据共享方案进行了仿真实验。仿真环境配置如下：使用 CPU 为 Intel Core i3-3120M 2.50GHz，内存为 4.00GB，操作系统为 Win7-64 位的计算机用来模拟数据共享过程。实验中，创建 Server 为云服务器端，User 为用户端，在一台计算机上通过云服务器端 Server 与用户端 User 两者间进行信息交互来完成数据共享过程的模拟实验。

软件平台为 Eclipse4.3.0，JDK1.6，仿真通过 Java 编程实现，所使用的加密算法均建立在开源代码库 jPBC2.0.0(Java Pairing-Based Cryptography Library)上，使用 jPBC 大数库实现双线性对和密码学算法等功能。在 Eclipse 平台上，通过 Java 编程实现数据初始化、CP-ABE 加密、用户属性撤销算法以及数据解密算法等模块的仿真实验。此外，仿真的加密数据为搜狗输入法用户的常用字词数据库，该数据主要为文本形式存在，文件中包含有大量的用户常用字词并以字符串的形式存储。每个用户的常用字词文件小，但由于用户基数大使得文件量巨大。在实际云计算环境中不仅存储大文件还存储大量小文件，本文实验选择其中一种数据库进行仿真。

5.2　实验分析

本方案根据信任分散策略，不对任何一个云服务器绝对信任，将原始加密数据拆开存储，解决了数据存储时信任集中问题。在分析代理重加密算法和密文策略属性基加密的基础上，通过在用户私钥内添加全局标志以解决基于属性的访问控制方法中的串谋攻击行为，利用代理重加密技术进行属性密钥的更新以保证用户撤销时后向安全性。

1）信任集中

将上传数据分别存储在云服务端 A、B 上，根据信任分散策略将原始数据拆分存储以解决信任集中问题。采用定值抽取法将数据分离，设置用户上传数据的抽取标准为固定值，其时间复杂度为 O(1)，采用随机抽取法的时间复杂度为 O(n)，由时间复杂度比较说明，本方案采用定值抽取法分离数据可以有效减少系统开销并解决信任集中问题。表 1 为属性数量等于 10 时本方案在加密开销方面的对比，图 4 为本方案与 Jung 方案和完全 CP-ABE 加密方案三者在加密时间开销方面的变化关系。

通过实验结果可知，数据加密花费时间的多少与属性数量和加密文件大小紧密相关。图 4 中，Jung 方案采用多授权机构在利用属性基加密对称密钥后使用对称密钥加密共享数据，完全 CP-ABE 加密方案对整体数据直接采用属性基加密，本文方案只在动态数据部分存在运算量大的双线性运算。本文方案对比另外两种方案，在文件较小时分割动态和静态数据的运算对总体时间开销影响大，使算法对比其他算法花费时间稍长，但随着文件增大另外两种方案的双线性运算占比总计算开销升高，而本文方案的分割运算复杂度为 o（1），因此随着属性数量增加时间开销的优势越明显。表 1 中，当属性数量相同时，随着加密文件变大加密时间并没有大幅度增长，时间消耗变化较平稳，运算开销在可接受的范围内，满足实际云环境中数据安全共享的需求。

表 1 属性数量为 10 的文件加密测试结果

文件大小/KB	数据加密平均时间消耗/ms
10	332
20	350
30	355
40	352
50	361

2）串谋攻击

在数据共享方案中，对动态数据采用基于属性集和访问结构的 CP-ABE 算法进行加密，非法用户 u_i 和 u_j 两者可通过联合属性得到解密密钥，非法获得共享数据。本文方案在用户私钥中内嵌入用户的全局标志，使得每个用户使用自己的私钥加密数据时带有全局唯一的标志信息，从而解决串谋攻击问题。针对添加全局标志是否对数据加密产生较大额外开销，进行仿真实验，实验中属性数量均为 5。图 5~7 分别为文件大小 1KB、50KB 和 100KB 时全局标志与加密时间开销的关系图，实验次数为 50 次。

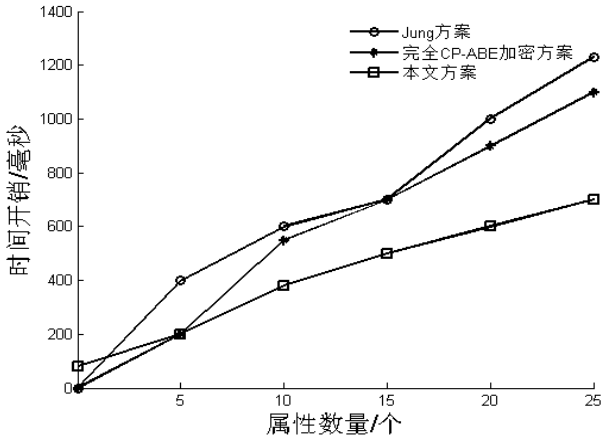

图 4 属性数量与时间开销的变化关系图

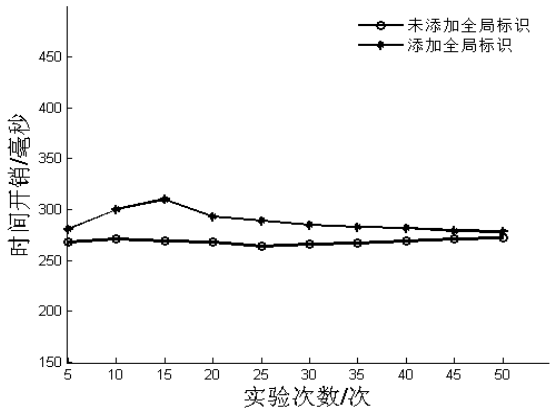

图 5 全局标志与加密时间开销关系图（1KB 文件）

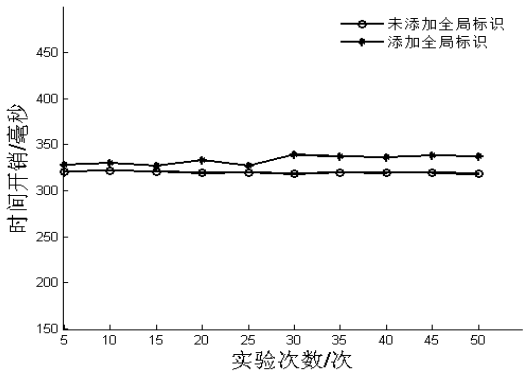

图 6 全局标志与加密时间开销关系图（50KB 文件）

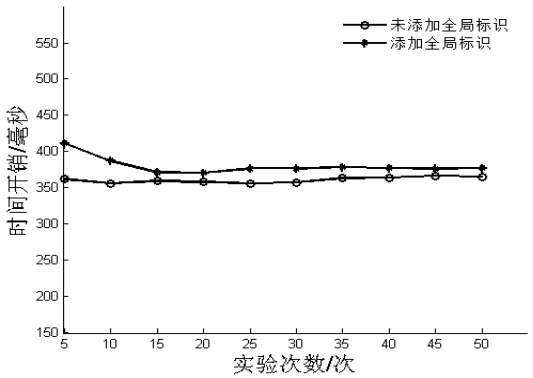

图 7 全局标志与加密时间开销关系图（100KB 文件）

实验对总体加密时间进行测试，由于每次测试时硬盘读写、IO 流输入输出等硬件因素差异，经过 50 次实验求期望值 E 得出结果，并且在文件大小为 1KB、50KB 和 100KB 不同情况下分别进行实验。通过图 5、图 6 和图 7 可知，在存有硬件差异和 IO 操作差异等误差的条件下，未加全局标志的方案由于在用户注册时不用为其分配全局变量，该环节比添加全局标志的算法计算开销小，此外本文方案在文件较小时为用户分配全局标志的部分时间开销占比总时间比例高，故对于 1KB 的数据加密时本方案与未添加全局标志的方案时间差距较大，曲线波动相对较大。但随着文件的增大分配全局变量操作的时间开销占比减少，两种方案的时间相差逐步接近。实验说明添加全局标志不会为系统加密增加过多额外开销，同时解决了串谋攻击问题。

3）后向安全性

在云计算环境下数据共享是动态变化的，为保证用户撤销时数据的后向安全性，采用代理重加密技术对动态数据进行重新加密，为数据安全提供双重保护屏障。方案针对动态数据重加密可以减轻用户撤销时密钥密文重加密的工作量，同时使撤销用户不能查看原始数据，保证后向安全性。

6 结束语

本文基于信任分散策略，构建了一个将原始数据进行动态和静态数据分割以解决数据存储中的信任集中问题，并且在动态数据的用户私钥中添加全局标志防止串谋攻击，采用代理重加密技术重加密动态数据以保证后向安全性的共享方案。随着物联网的发展，越来越多的传感器利用云技术实现数据收集、转换以及对相应数据实施具体操作，这些数据的重要特点是文件小但是文件数量多，本文实验选择实际应用中的一种数据库进行仿真，符合云计算环境的实际应用场景。并且针对云环境中移动端用户日益增多的实际情况，本文方案能有效减少用户端的双线性运算，降低系统整体的运算量，运算开销在可接受的范围内。下一步的工作主要包括：一方面进一步拓展云环境中基于信任分散策略的数据共享方案面向的实验对象范围，对更大的文件进行仿真实验，以满足云计算环境下多种实际应用场景；另一方面对云计算环境中用户安全撤销问题进行进一步研究，在实际场景中测试并在保证后向安全性前提下降低密钥更新的计算开销。

参考文献：

[1] Mell P, Grance T. The NIST Definition of Cloud Computing[R]. National Institute of Standards and Technology, 2009.

[2] 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83.

[3] 姚文斌, 韩司, 李小勇. 云存储环境下的密文安全共享机制[J]. 通信学报, 2015, 36(10): 1-8.

[4] 郎讯, 魏立线, 王绪安, 等. 基于代理重加密的云存储密文访问控制方案[J]. 计算机应用, 2014, 34(3): 724-727, 741.

[5] Loftus J, Smart N P. Secure outsourced computation[C] //Lecture Notes in Computer Science, vol 6737. Berlin: Springer, 2010: 1-20.

[6] Damiani E, Pagano F, Pagano D. iPrivacy: a distributed approach to privacy on the cloud[J]. International Journal on Advances in Security, 2011, 4(3): 185-197.

[7] 陈亮, 杨庚, 屠袁飞. 混合云环境下基于属性的密文策略加密方案[J]. 计算机应用, 2016, 36(7): 1822-1827.

[8] 王于丁, 杨家海, 徐聪, 等. 云计算访问控制技术研究综述[J]. 软件学报, 2015, 26(5): 1129-1150.

[9] Sahai A, Waters B. Fuzzy identity-based encryption[M] //Advances in Cryptology - EUROCRYPT. Berlin: Springer, 2005: 457-473.

[10] Brthencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C] //Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2007: 321-334.

[11] Wan Zhiguo, Liu June, Deng R H. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing[J]. Information Forensics and Security, IEEE Transactio, 2012, 7(2): 743-745.

[12] Jung T, Li Xiangyang, Wan Zhiguo, *et al*. Privacy preserving cloud data access with multi-authorities[C]// Proc of INFOCOM. 2013: 2625-2633.

[13] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Trans on Parallel and Distributed Systems, 2011, 22(7): 1214-1221.

[14] Wang Guojun, Liu Qin, Wu Jie. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services[C] //Proc of the 17th ACM Conf on Computer and Communications Security. New York: ACM, 2010: 735-737.

[15] Yu Shucheng, Wang Cong, Ren Kui, *et al*. Attribute-based data sharing with attribute revocation[C] //Proc of the 5th ACM Symp on Information,

Computer and Communications Security, 2010, New York: ACM, 2010: 261-270.

[16] Liang K, Susilo W. Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage[J]. IEEE Trans on Information Forensics & Security, 2015, 10(9): 1-1.

[17] Zhenhua L, Jinmiao W, Bo L. A ciphertext‐policy hidden vector encryption scheme supporting multiuser keyword search[J]. Security & Communication Networks, 2015, 8(6): 879-887.

[18] Shamir A. Identity-based cryptosystems and signature schemes [C] // Proc of CRYPTO. Berlin: Springer, 1985: 47-53.

[19] Beimel A. Secure schemes for secret sharing and key distribution[D]. Haifa, Israel: Israel Institute of Technology, 1996.

[20] Bellare M, Desai A, Pointcheval D. Relations among notions of security for public-key encryption schemes[C]//Lecture Notes in Computer Science, vol 1462. 1998: 22-45.