云存储平台下基于属性的数据库访问控制策略

黄保华 贾丰玮 王添晶

(广西大学计算机与电子信息学院 南宁 530004)

摘 要 云存储是一种新兴的数据存储模式,具有低成本、高效、易用等特点。数据库的安全访问控制成为在云存储平台下数据库运行时不可忽视的问题。设计了一个带权重的密文策略属性加密(WCPABE)方案,并且提出了基于该加密方案的云存储平台下数据库的访问控制策略。通过引入属性权重概念,WCPABE可以动态反映数据库中各个属性的重要程度,增强数据库拥有者对数据库的访问控制;提出了3种基于WCPABE的访问控制策略;提出了WCPABE在云存储平台下的数据库加密模型,实现了云存储平台下对数据库的有效、安全的访问,增强了数据库安全性,同时解决了多用户私钥分发与管理问题。实验数据表明:WCPABE具有可行性和有效性,能使云存储平台下数据库拥有者对数据库访问控制具有更多样化的手段,增强了数据库的安全性。

关键词 数据库安全,基于属性加密,访问控制,云存储

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.3.032

Database Access Control Policy Based on Attribute in Cloud Storage Platform

HUANG Bao-hua JIA Feng-wei WANG Tian-jing

(College of Computer and Electronic Information, Guangxi University, Nanning 530004, China)

Abstract Cloud storage becomes more and more popular in large scale Database's data store recently because it has features as low-cost, high efficiency, easy-to-use. To shift database from local to cloud storage server is still facing many challenges, especially in access control of database. We designed a "Weight Cipertext-Policy Attribute-Based Encryption" (WCPABE) scheme and proposed a database access control policy based on WCPABE under the cloud storage platform. Through introducing the concept of attribute weight, WCPABE can dynamically reflect each property's important degrees in database and enhance the ability for database access control. We proposed three kinds of access control strategies based on WCPABE, and proposed WCPABE's database encryption model in cloud storage platform and achieved effective and safe access control for database, enhancing database security and solving users' private key problem in distribution and management. Experimental results show that WCPABE has feasibility and effectiveness and the database owner has more diversified means of enhancing security of the database under cloud storage platform.

Keywords Database security, Attribute-based encryption, Access control, Cloud storage

1 引言

2006年8月9日,Google首席执行官埃里克·施密特(Eric Schmidt)在搜索引擎大会(SES San Jose 2006)上首次提出"云计算"(Cloud Computing)的概念。

随着虚拟化、Grid技术、面向服务的体系结构、集群应用、分布式文件系统、网络安全传输等技术的发展,基于云计算的云存储应运而生[1,2]。通过各种云存储服务商,将数据库中的数据放到云环境下的企业也越来越多。目前已出现众多结合云存储与数据库的商业服务,国内方面有:腾讯的支持MySQL的云数据库,百度的支持MySQL、MongoDB、Redis的云数据库,阿里的云兼容MySQL、SQLServer、PostgreSQL的RDS,京东的JDS;国外方面有:在OpenStack平台上的Rackspace的MySQL托管服务,谷歌的Cloud Datastore,亚马逊关系型数据库服务(RDS)等等。将数据库与云存储相结合带来如下4点优点。

(1)海量的数据存储和易扩展性:可以实现数据库存储容量为PB(Petabyte)级甚至EB(Exabyte)级的数据的存储。

(2)抗故障性:当部分机器因不可抗拒因素发生故障时,整个数据库系统通过内部的调配机制,仍可以保证用户使用正常的数据库服务,不会明显地影响用户使用。

(3)高性能、快响应:数据库系统通过对海量的数据优化存储结构,进一步提高性能和检索效率、增大网络吞吐率、减少响应时间。分布式的数据库存储结构使得最终用户获得更快的系统响应速度,改善用户体验。

(4)绿色节能:数据库海量数据存储在数据中心系统中,并由有经验的数据库管理员统一维护,降低照明和温度控制等能源消耗,符合当前国家倡导的低碳经济与绿色计算的总体趋势。

但是,将数据库外包到云存储服务器中[3]也带来了一系

到稿日期:2015-07-12 返修日期:2015-11-29 本文受国家自然科学基金(61262072)资助。

黄保华(1973—),男,副教授,主要研究方向为信息安全等,E-mail:bhhuang66@gxu.edu.cn;贾丰玮(1989—),男,硕士生,主要研究为信息安全等;王添晶(1990—),女,硕士生,主要研究方向为信息安全等。

列的数据安全性和隐私性问题，在访问控制方面将会面临如下两点问题：

(1)第三方云存储平台环境的复杂性导致存储在云服务器上的数据库文件可能遭受到攻击者的恶意访问，对用户访问控制难度提升。

(2)数据库所有者对数据库的控制能力受到限制，本地数据库通常采取用户身份的控制方式，通过对指定的用户给予相应身份来管理数据库的访问权限。但云存储平台分布式服务器环境下，任意一处服务器被恶意攻击后，只需将其提升到管理员用户身份就可以直接获取整个数据库数据。

因此，根据数据库的功能和数据结构，使用更高效和多样化的安全机制来提升云存储平台下数据库的安全性是必要的。对此，有效的解决办法之一是用户在将数据传输到服务器之前对数据库加密。然而数据存放的物理位置与用户使用数据库的位置分置，使用户的访问控制变得更为困难，加密后访问数据库用户增多时，用户私钥的高效管理与分配成为问题。

2005 年，Sahai 和 Waters 开启了一种新的加密访问控制的研究方向：基于属性的加密(Attribute Based Encryption)方案[4]。作者所提出的模糊身份(Fuzzy Identity)的概念是基于身份的加密[5-8]，在访问控制的方向则产生基于属性的加密的访问控制策略。基于属性的加密方案将身份加密中的身份化分成含有多个属性的集合，其基本思想是属性集合分别与用户分配的私钥和加密后的密文相关联，当且仅当密文的属性匹配用户私钥达到一个门限值时，用户才可以对该密文解密，否则解密失败。2006 年，Goyal 等人基于模糊的身份加密方案提出密钥策略的基于属性的加密方案 KPABE[9]，访问控制策略由一棵访问结构树控制且与用户密钥结合，将属性集加入加密过程中，使密文包含属性，仅当密文的属性满足密钥的访问控制策略时，密文才可被解密。2007 年，Bethencourt 等人提出密文策略的基于属性的访问控制策略 CPABE[10]，密文与访问结构树相关联，访问结构实现“与”、“或”和“门限(k,n)”操作。Cheung 等[11]改进访问结构，实现“与”和“非”操作，提出在标准模型下可证明安全的 CPABE。2014 年，Dalia[12]提出可搜索的 CPABE 加密结构，用户可委托搜索功能于第三方，而第三方无需解密密文。

本文引入数据库属性权重概念，将表头属性的重要程度量化，提出了一种云存储平台下数据库的安全访问控制策略 WCPABE。WCPABE 采取多叉树的访问结构，将属性的权重结合到多叉树中的属性节点，提出了 3 种可选的 WCPABE 的控制策略。通过实验证明了 WCPABE 的有效性与可行性。WCPABE 使数据库访问控制手段增加，增强了数据库的安全性。

2 数据库属性权重

2.1 属性权重定义

鉴于关系型数据库中表的特殊结构，每张表的表头都由若干属性构成，而根据各个表中储存的数据记录数目的不同，每个属性对于用户的重要程度也不同，可用属性权重量化不同属性的重要程度。

属性权重定义：可数值化的某 n 张表($n\geqslant 1$)中某一属性的重要程度。

在数据库发送到云存储平台之前，对数据库以单表或多表的细粒度进行加密，属性权重的计算如下：

当 $n=1$ 时，对一张表加密。因为该表表头中有些属性可以为空(null)。如表 1 所列，身高、体重可以是空值，对于表中每条记录并非必须存在具体数值。那么，这两个属性就不需要拥有过大的权重。此时属性基本权重计算为：

属性基本权重＝该属性下存在记录数/表中总的记录数

其中属性权重的范围为[0,1]。

如表 1 的权重计算过程为：

学号权重＝5/5＝1，学号为该表主键，不可为空

姓名权重＝5/5＝1，姓名不可以为空

身高权重＝2/5＝0.4

体重权重＝4/5＝0.8

表 1 数据库表属性可为空的示例

学号	姓名	身高	体重
01	甲	180	70
02	乙	175	80
03	丙	null	65
04	丁	null	77
05	戊	null	null

当 $n>1$ 时，对多张表合并加密。将 n 张表属性合并作为多张表的属性，属性权重为单表对应属性的属性权重。对于单表合并时可能产生属性重复的情况，将所有出现重复属性的单表中该属性权重相加，作为多表合并后的属性权重。这样属性权重大的属性意味着该属性在 n 张表中具有较高的重要程度。

图 1 为每张数据库表属性权重计算后的结果，那么 4 张表合并后属性权重的计算过程为：学号权重＝1＋1＝2，姓名权重＝1＋1＋1＋1＝4，身高权重＝0.4＋0＝0.4，年龄权重＝0.2＋0.3＝0.5，电话权重＝0，性别权重＝1。

属性	学号	姓名	身高
权重	1	1	0.4

属性	姓名	年龄	性别
权重	1	0.2	1

属性	姓名	年龄	电话
权重	1	0.3	0

属性	姓名	学号	身高
权重	1	1	0

图 1 4 张数据库表示例

2.2 基于属性权重可选的访问控制方案

前面讨论了属性增加权重的必要性和属性权重计算方法，下面给出 3 种可选的访问控制方案，可以使数据库拥有者对访问数据库的用户拥有更多的控制手段。

2.2.1 方案一：权重门限方案

在数据库表头的众多属性中，不同的属性权重反映了相应属性的重要水平不同，数据库拥有者对数据库加密后要求用户拥有多个属性联合的密钥才能解密。对于重要属性，数据库拥有者重视程度会更高一些，因此有必要提升这样的属性在加密解密时的重要程度。

权重门限方案的基本思想是通过将该表的属性与相应的属性权重返回给数据库拥有者，让数据库拥有者指定解密时属性权重的最小值 limitweight，属性权重大于等于 limitweight 的属性称为“必要属性”。在解密时，必要属性在用户私钥中需要全部匹配。只要有一个必要属性没有匹配成功，则确定该用户不具有解密权限，解密失败，解密过程终止，不需要继续判断剩余属性是否匹配，使得匹配过程中属性较多

时，减少属性匹配次数。

2.2.2 方案二：指定权重属性方案

数据库中可能会出现某些常见的属性，例如校园管理数据库系统中的教师 ID 号和学生 ID 号。这些属性会在多张表中出现，攻击者可以很容易地猜测出某些常见的属性，进而伪造私钥。

指定权重属性方案的基本思想是数据库拥有者指定解密时哪些属性为必要属性。数据库拥有者可以指定不常见属性为必要属性，使攻击者无法轻易猜测。如同方案一中，必要属性在用户私钥中需要全部匹配。

2.2.3 方案三：特征属性方案

允许数据库某张表具有可以代表该表特征、特色的与众不同的属性。譬如校园管理系统数据库中某张表具有“国籍”属性(该属性可以为空)。“国籍”属性在数据库其他表中出现次数少，且在出现过的表中属性权重都比该表中的权重小，可以将“国籍”属性作为该表的特征属性。

特征属性方案的基本思想是每次数据库拥有者对数据库进行增、删、改等操作后，都由加密系统对表重新加密，在加密系统中维护更新该数据库所有表的属性和权重信息。当数据库拥有者向加密系统提交需要加密的某 n 张表时，加密系统不但返回给数据库拥有者按照权重值从高到低排列的属性，而且通过与数据库中所有表的属性权重信息作比较，选出在本表中属性权重值较高，而在其他表很少出现且出现时属性权重值低的某几个属性，作为本表的特征属性返还给数据库拥有者。使数据库拥有者决定是否采用特征属性为解密时的必要属性。

3 CPABE 方案

基于属性的访问控制策略 CPABE(Cipertext-Policy ABE)加密方案是基于属性的加密方案，将待加密数据与访问结构直接关联，加密系统发布公钥，加密者设计访问结构，用户通过属性集合表示，用户能否解密密文的关键因素取决于密文所关联的访问结构与用户包含的属性是否匹配。

下面对 CPABE 算法中用到的属性、访问树、满足访问树进行简要概述。

假设 $S=\{A_1,A_2,\cdots,A_n\}$ 为全体属性集合，则用户分配的属性 S' 是 S 的非空子集，所以属性总个数为 n 的属性集最多将定义 2^n 个不同属性集的用户。

访问树描述一个访问结构，属性 S' 中的某一元素通过树的每个叶节点表示，而将非叶子节点定义成一个关系运算符，即与、或和门限。

满足访问树是指当用户属性集匹配访问树的访问结构即 $S'\subseteq 2^{\{A_1,A_2,\cdots,A_n\}}$ 时，用户才可解密密文。

CPABE 算法主要包含 4 个组成部分：

1)系统建立：加密者生成主密钥 MK 和公钥 PK。

2)加密明文：加密者用 PK、访问结构 T 对明文 M 加密，生成对应的密文 CT。

3)生成私钥：用主密钥 MK 和用户属性集 S 生成私钥 SK。

4)解密密文：解密者用 SK 对密文 CT 进行解密得到明文数据 M。

4 WCPABE 方案

为了方便论述，下面各个过程和改进的算法中均以“权重门限方案”作为基础进行说明，另两个方案的过程与此基本一致，不再另作说明。

4.1 算法基础

双线性型映射群：设 G_0 和 G_1 是阶为素数 p 的两个乘法循环群，g 是 G_0 的生成元，$e:G_0\times G_0\rightarrow G_1$。双线性映射 e 具有如下性质：

(1)双线性：对于任意 $u,v\in G_0$ 和任意 $a,b\in Z_p$，有 $e(u^a,v^b)=e(u,v)^{ab}$；

(2)非退化性：$e(g,g)\neq 1$。

如果 G_0 中的群操作和双线性映射 e 都是高效可计算的，则称 G_0 为双线性群。

双线性映射 e 拥有对称性 $e(g^a,g^b)=e(g,g)^{ab}=e(g^b,g^a)$。

访问策略树 T：访问策略树 T 代表一个访问结构，如图 2 所示，访问策略树 T 的每个非叶子节点为一个门结构，由一个门限 k_x 和该节点的孩子来描述；访问策略树 T 中的每个叶子节点代表了一个属性，通过属性、属性权重和门限值 $k_x=1$来描述。门限值为 $k_x(0<k_x\leqslant num_x)$表示非叶子节点 x 的孩子节点个数为 num_x：若非叶子节点描述树结构中的“OR”门，则 $k_x=1$；若非叶子节点描述树结构中的“AND”门，则 $k_x=num_x$。访问策略树 T 有如下 4 个函数：

$parent(x)$表示节点 x 的父节点；

$att(x)$表示与节点 x 相关的属性；

$weight(x)$表示节点 x 的属性权重值；

$index(x)$表示节点 x 是其父节点的第几个子节点。

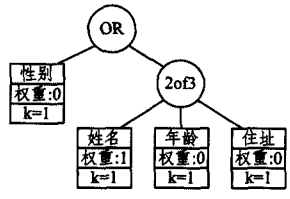

图 2 访问策略树

满足访问策略树：记 T_x 是访问策略树 T 的一棵以节点 x 为根节点的子树，访问策略树 T 以节点 R 为根节点，即 $T=T_R$。若一个属性集合 s 满足一棵子树 T_x，则记为 $T_x(s)=1$。$T_x(s)$的计算为递归过程：假如 x 是一个非叶子节点，则分别计算 x 的全部子节点 z 的 $T_z(s)$值。当且仅当至少 k_x 个子节点的 $T_z(s)=1$ 时，$T_x(s)=1$；如果 x 是一个叶子节点，将 x 的属性权重与属性权重门限 $limitweight$ 进行比较：如果 $weight(x)<limitweight$，该节点为非必须属性，若 $att(x)\in s$，则 $T_x(s)=1$，否则 $T_x(s)=0$；如果 $weight(x)\geqslant limitweight$，则节点 x 为必要属性，若 $att(x)\in s$，则 $T_x(s)=1$，否则 $T_R=0$，停止计算其他节点，不满足访问策略树 T。

4.2 算法描述

本文提出的带权重的基于密文策略的属性加密方案(Weight Ciphertext-Policy Attribute-Based Encryption，WCPABE)由 5 个阶段组成：系统建立(Setup)、加密(Encrypt)、密钥提取(KeyGen)、子密钥分配(Delegate)、解密(Decrypt)。

Setup：系统输出公钥 PK 和主密钥 MK。运行双线性

Diffie-Hellman（Bilinear Diffie-Hellman，BDH）参数生成器，产生两个阶为素数 q 的群 G_0 和 G_1，g 为 G_0 的生成元，双线性映射对 $e:G_0\times G_0\rightarrow G_1$，随机数 $\alpha,\beta\in\mathbb{Z}_p$。生成公钥和主密钥如下：

$PK=G_0,g,h=g^{\beta},f=g^{1/\beta},e(g,g)^{\alpha}$

$MK=(\beta,g^{\alpha})$

Encrypt$(PK,M,T,limitweight)$：系统输入公钥 PK，明文 M，访问策略树 T，属性权重门限 *limitweight*；系统输出密文 CT。根据访问策略树 T 加密消息 M。访问策略树 T 中用二进制串描述的属性通过哈希函数 $H:\{0,1\}^*\rightarrow G_0$ 映射为随机群上的一个元素。

为 T 中每个节点 x（包含叶子节点）选择一个多项式 q_x。从树的根节点 R 开始，自上而下选择多项式。节点 x 的多项式 q_x 的度 d_x 比它的门限值 k_x 小 1，即 $d_x=k_x-1$。

首先，算法从根节点 R 起始选择随机数 $s\in\mathbb{Z}_p$，并设置 $q_R(0)=s$。然后，算法随机选择多项式 q_R 上的 d_R 个点来完全定义 q_R。最后，对于其他的顶点 x，令 $q_R(0)=q_{parents(x)}(index(x))$，随机选择其他 d_x 各顶点来完全定义 q_x。

设 T 中所有叶子节点的集合为 Y，那么根据给定的访问策略树 T 计算密文：

$$CT=(T,C'=Me(g,g)^{\alpha s},C=h^s,limitweight$$
$$\forall y\in Y:C_y=g^{q_y(0)},C_y'=H(att(y))^{q_y(0)})$$

KeyGen(MK,S)：系统输入属性集合 S；系统输出被 S 标记的密钥。首先选择随机数 $r\in\mathbb{Z}_p$，然后对每一个 $j\in S$ 选择随机数 $r_j\in\mathbb{Z}_p$。最后，计算出私钥：

$$SK=(D=g^{(\alpha+r)/\beta},\forall j\in S:D_j=g^r\cdot H(j)^{r_j},D_j'=g^{r_j})$$

Delegate(SK,S')：系统输入私钥 SK 和用户属性集 S'；系统输出用户密钥 SK'。根据已有属性集 S 的密钥 SK 生成另一个集合 $S'(S'\in S)$ 的密钥。算法为 S' 中的每一个元素 K 随机选择一个值 $r'(r'\in\mathbb{Z}_p)$，子密钥 SK' 生成过程如下：

$$SK'=(D'=Df^{r'},\forall k\in S':D_k'=D_kg^{r'}H(k)^{r_k'},D_k'=D_k'g^{r_k'})$$

Decrypt(CT,SK)：系统输入密文 CT 和用户私钥 SK；系统输出明文消息 M。解密过程同样也为递归过程。定义中间函数 $F_x=DecryptNode(CT,SK,x)$。

若 $weight(x)\geqslant limitweight$，该节点属性为必要属性。设 $i=att(x)$，若 $i\in S$（S 是密钥 SK 对应的属性集合），那么计算过程如下：

$$F_x=\frac{E(D_i,C_x)}{E(D_i',C_x')}=\frac{e(g^r\cdot H(i)^{r_i},g^{q_x(0)})}{e(g^{r_i},H(i)\cdot g^{q_x(0)})}=e(g,g)^{rq_x(0)}$$

如果 $i\notin S$，则不再继续解密，解密失败。

若 $weight(x)\leqslant limitweight$，该节点属性为非必要属性。如果 $i\in S'$，F_x 计算过程不变；反之，如果 $i\notin S$，定义 $F_x=\perp$。

对于非叶子节点的情况，定义拉格朗日系数 $\Delta_{i,S},i\in\mathbb{Z}_p$，$S$ 是集合 $\mathbb{Z}_p$ 中的元素：$\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$。中间函数 F_x 计算如下：对于节点 x 的所有子节点 z，计算 $F_z=DecryptNode(CT,SK,z)$。选择 k_x 个 $F_z\neq\perp$ 的节点组成集合 S_x。如果找不到这样的集合 S_x，则 $F_z=\perp$，否则计算过程如下：

$$\begin{aligned}F_x&=\prod_{z\in S(x)}F_z^{\Delta_{i,S_x'(0)}}\\&=\prod_{z\in S(x)}(e(g,g)^{r\cdot g_z(0)})^{\Delta_{i,S_x'(0)}}\\&=\prod_{z\in S(x)}(e(g,g)^{r\cdot q_{parent(z)}(index(z))})^{\Delta_{i,S_x'(0)}}\\&=\prod_{z\in S(x)}e(g,g)^{r\cdot q_x(i)\cdot\Delta_{i,S_x'(0)}}\\&=e(g,g)^{r\cdot q_x(0)}\end{aligned}$$

其中，$i=index(z),S_x'=\{index(z):z\in S_x\}$

在定义了 *DecryptNode* 函数之后，定义解密算法。算法首先计算 F_R，R 是访问策略树 T 的根节点，如果 S' 满足访问策略树 T，解密出消息 M：

$$\begin{aligned}&C'/(\frac{e(C,D)}{DecryptNode(CT,SK,r)})\\&=C'/(\frac{e(h^s,g^{(\alpha+r)/\beta})}{e(g,g)^{r\cdot q_R(0)}})\\&=C'/(\frac{e(h^s,g^{(\alpha+r)/\beta})}{e(g,g)^{rs}})\\&=M\end{aligned}$$

5 云存储平台下数据库访问控制策略模型

5.1 控制策略模型

在云存储平台下，数据库存储服务通过互联网实现数据库上传、访问、备份、共享等功能。云存储平台下基于WCPABE的数据库访问控制模型由数据库拥有者、云存储平台、加密系统、用户组成，如图 3 所示。

数据库拥有者：数据拥有者使用公钥 PK、访问策略树和属性权重门限 *limitweight* 加密数据，上传密文到云存储平台。

云存储平台：云存储平台通过网络提供数据存储和访问服务。云存储平台是半可信的第三方，存储加密的数据库，但也有可能想要获取数据明文。

加密系统：加密系统负责整个加密算法的计算和密钥的分配，为用户分发属性，获取数据库属性及属性权重。本方案中假设加密系统为完全可信的第三方。

用户：用户为数据库的最终使用者，从云存储平台下载密文数据，解密得到数据库数据明文。

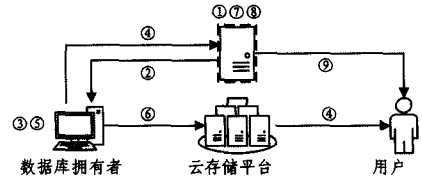

图 3 云存储平台下基于 WCPABE 的数据库访问控制模型

云存储平台下基于 WCPABE 的数据库访问控制模型包括以下 5 个过程。

（1）准备阶段：①加密系统生成公钥 PK 和主密钥 MK，②将公钥 PK 发送给数据库拥有者 *Owner*。

（2）加密过程：③数据库拥有者对需加密表计算属性权重，④将表的属性集 S 和属性权重集 W 发给加密系统，⑤数据库所有者根据属性集 S 和属性权重集 W，决定访问策略树 T、权重门限值 *limitweight*，⑥用公钥参数 PK、访问结构树 T、权重门限值 *limitweight* 加密该表，生成密文 CT，传输到云存储平台。

（3）密钥生成：⑦加密系统用主密钥 MK、表属性集 S 生成私钥 SK。

(4)用户私钥分配:⑧根据用户分配的属性 S' 生成用户私钥 SK',⑨将用户私钥 SK' 发送给用户 *User*。

(5)解密过程:⑩当接收者接收到密文 *CT* 后,使用用户私钥 SK' 解密密文。当用户私钥 SK' 中包含的属性满足了密文的访问策略树 T,且权重大于权重门限 *limitweight* 的必要属性都存在时,解出明文,恢复出被加密的表 *Table*。

为了保证加密系统中属性分配过程的安全,Chase 等[13]提出多属性机构方案,每个属性机构仅生成一部分属性对应的属性私钥,用户私钥需要多个属性机构联合产生,解决了密钥托管问题。

5.2 策略分析

本文将 WCPABE 算法实施于云存储平台下数据库加密模型。数据库拥有者使用 WCPABE 加密数据库得到密文并传输到云存储平台,用户使用用户密钥对云存储平台中加密存储的数据库进行相应的访问操作。对该控制策略分析如下。

(1)通信安全:数据库的数据以密文的方式传输,防止在传输过程中被窃取、第三方不可信云存储服务提供商对数据库的访问篡改。

(2)访问权限:采用加密算法和数据库表头属性结合的方式,可以有效防止用户越权访问。加密系统为不同用户分派不同权重属性的属性集,指定用户的访问范围。

(3)密钥分配:加密系统使用主密钥生成不同属性集的用户私钥,使得数据库拥有者加密数据库后可以离线,由加密系统负责给用户分配私钥,解决了用户私钥分发的问题。

(4)算法效率:使用原 CPABE 方案解密时要递归匹配所有的访问策略树节点,而使用 WCPABE 方案时,在用户密钥的属性匹配访问策略树过程中,若必要属性未在用户密钥中出现,则不用继续匹配访问策略树的其他节点,从而迅速被系统认定解密失败,提高解密失败情况下算法效率。

(5)抗合谋攻击:加密系统集中管理用户密钥,在密钥更新时,加密系统只需重新为用户指定一组属性并且分配一个新的属性密钥。用户被撤销时,加密系统更新访问策略树,致使撤销用户无法继续访问,用户之间的合谋攻击无效。方便了用户密钥的更新与撤销。

(6)空间存储:在物理存储上,由于增加了权重数值,使得密文的长度增加,但对于正常情况下的数据库表中数据的数量级影响微乎其微,用户私钥的长度并没有改变。

6 WCPABE 分析与仿真

6.1 WCPABE 特点与优势

对比原 CPABE 方案,本文提出的 WCPABE 的优势特点总结如下。

(1)有效区分加密时不同属性的地位

在多数据库表加密时,因为表头属性数目将到达很大的数量,部分属性的有无在数据库使用者看来将非常重要,相反,一些属性在数据库中是可有可无的,因此区分加密时所采用的数据库表头众多属性的主次地位是有必要的。本文的 WCPABE 方案将属性权重的概念引入到访问策略树的设计中,通过权重的计算,使得属性的地位与数据库表头属性和表记录数目相关联,权重门限方案中属性权重超过权重门限的为必要属性,必要属性在解密时起到了决定性的作用,突出了不同属性的主次地位。解决了 CPABE 方案中所有属性节点在访问策略树中地位相同的问题。

(2)提高解密失败时算法效率

针对用户私钥解密时需要递归匹配访问策略树中的所有属性节点的情况,WCPABE 的权重门限方案在匹配访问策略树时,一旦出现必要属性匹配失败的情况,则立即停止后续所有属性节点的匹配计算过程,直接认定解密失败,从而加快解密失败时的计算速度,提高算法效率。

(3)加强控制手段,有效区分用户

WCPABE 方案为用户分配带有权重的属性集,较高级别的用户将分配到权重较大的属性集合,相反,低级别用户分配到权重小的属性集,从而通过不同级别的用户获得的不同权重属性集,影响解密时的访问策略树匹配,有效区分了用户级别,增强了用户控制方式。

6.2 WCPABE 性能仿真

实验环境:处理器为 Intel i5-4200U,内存为 4GB,操作系统为 Windows 7,数据库版本 MySQL Server 5.6,开发语言 Java,使用 jPBC1.2.0 库[14]。

实验采取本地方式测试,忽略数据在分布式网络中存在的传输延迟,对本文 5.1 节提出的云存储平台下基于 WCPABE 的数据库访问控制模型进行部分修改,采用属性权重门限方案,实验由下列 5 个阶段组成。

(1)预准备阶段 setup:加密系统连接数据库;生成公钥和主密钥。

(2)密钥生成阶段 keygen:获取待加密表的表头属性集,计算每个属性的权重;生成主密钥。

(3)数据加密阶段 enc:通过数据库的备份操作获取待加密表备份文件,确定权重门限和访问策略树;加密文件获得密文。

(4)密钥分配阶段 delegate:确定子属性集;生成被子属性集标记的用户私钥。

(5)用户解密阶段 dec:解密密文,获取明文。

实验结果如下:图 4—图 6 为 WCPABE 随数据库中可变因子变化的各个加密阶段的耗时情况,图 7—图 9 为原 CPABE 与本文 WCPABE 的耗时对比情况。

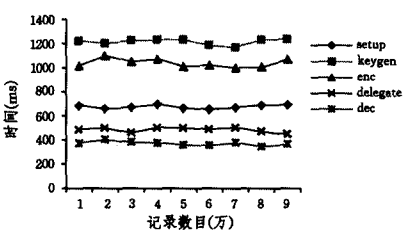

图 4 十万条记录以下各阶段耗时随记录数目变化的情况

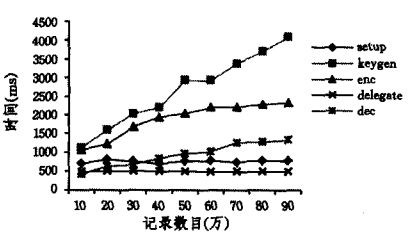

图 5 百万条记录以下各个阶段耗时随记录数目变化的情况

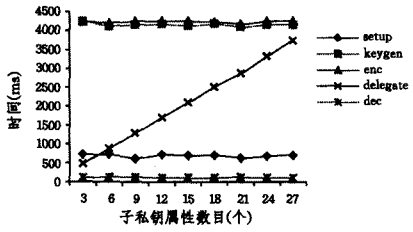

图 6 各个阶段耗时随用户私钥属性数目变化的情况

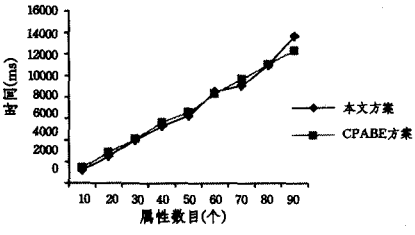

图 7 本文方案与原 CPABE 总耗时随表属性数目变化的情况

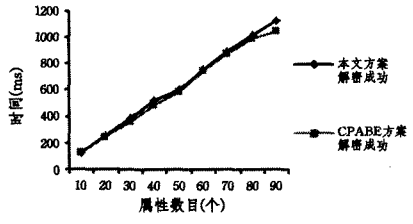

图 8 本文方案与原 CPABE 解密阶段耗时随表属性数目变化的情况

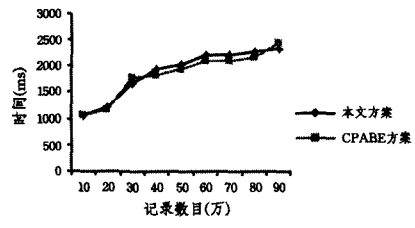

图 9 本文方案与原 CPABE 加密阶段耗时随表属性数目变化的情况

图 4、图 5 示出随着数据库待加密表中记录数目的增加，各个阶段的耗时变化情况(实验时数据库待加密表表头的属性数目设定为 5)。实验结果说明：WCPABE 的加密过程中，数据库中记录数递增单位为万，耗时无明显变化；当数据库中数据记录数递增单位为十万时，耗时变化比较明显，主要原因是 keygen 过程中计算属性权重时对数据库总记录数的查询和每个属性的记录值的查询，因此记录查询导致 keygen 耗时与记录数呈线性关系。

图 6 显示随着分配用户私钥属性的个数增加，各个阶段的耗时情况(实验时数据库待加密表表头的属性数目设定为 30，此时子私钥属性个数的范围为 0～30)。实验结果说明：分配用户私钥属性数目逐渐增加时，分配处理时间逐步趋向于主密钥的生成时间。这与预期相符，因为当用户子密钥分配全部的属性时，相当于把主密钥分配给用户，主密钥具有全部属性和权重的信息。

对比原 CPABE 方案[10] 的总耗时，结果如图 7 所示，WCPABE 增加了更多的访问控制手段，但并未增加系统负担，总耗时基本与原方案一致。

对于解密阶段，结果如图 8 所示(实验时数据库待加密表表头的属性数目变化范围为 10～90，设置子私钥中属性数目和表头的属性数目相同，即每次都将所有属性全部分配给用户子私钥，这样可以使得该阶段耗时变化明显，利于观察分析)，因为用户密钥中的属性需递归匹配访问策略树，所以当用户私钥解密成功时，随访问策略树的属性数目增加，匹配耗时增加，且 WCPABE 与原方案解密耗时基本一致；当用户私钥不满足访问策略树时，WCPABE 方案由于增加了属性权重，当且仅当有一个属性不满足访问策略树的必要属性则立即停止后续匹配，判定为解密失败，因此它比原 CPABE 方案更快地完成访问策略树匹配，减少了解密时间和系统性能消耗，具体解密时间根据用户未匹配私钥属性在访问策略树中的位置而定。

对比原 CPABE 方案[10] 的数据加密阶段，结果如图 9 所示，由于数据读取过程是将 MySQL 表与权重门限进行加密运算，因此数据表中的记录数目是影响数据读取耗时的主要因素。实验结果说明：本文方案增加属性权重后与原 CPABE 耗时基本一致。

结束语 本文分析云存储与数据库的现状，基于密文策略的属性加密方案，提出了一种云存储平台下对数据库具有灵活访问策略的带权重的密文策略的属性加密方案 WCPABE；提出了云存储平台下数据库加密模型；在 WCPABE 方案的基础上提出 3 种可选的控制方案。针对原 CPABE 方案解密需要递归匹配所有的访问策略树节点、每个节点属性均有同等地位、用户访问控制手段单一等问题，本文将属性权重与数据库表头的属性和记录数相关联，动态反映数据库中每个属性的重要程度，使得云存储平台下数据库拥有者对数据库具有多样化的访问控制手段，更加适合在云存储平台下多用户访问时保证数据库数据的安全。改进算法的安全性与原 CPABE 相同，能确保数据库的数据安全。

参 考 文 献

[1] Krutz R L, Vines R D. Cloud security: a comprehensive guide to secure cloud computing[M]. Indianapolis, IN: Wiley Publishing, 2010: 358

[2] Toosi A N, Calheiros R N, Rajkumar B. Interconnected cloud computing environments: challenges, taxonomy, and survey[J]. ACM Computing Surveys, 2014, 47(1): 1-47

[3] Zhu Qin, Yu Shou-jian, Le Jia-jin, et al. Research on Security Mechanisms of Outsourced Database[J]. Computer Science, 2007, 34(2): 152-156(in Chinese)
朱勤，于守健，乐嘉锦，等. 外包数据库系统安全机制研究[J]. 计算机科学，2007，34(2)：152-156

[4] Sahai A, Waters B. Fuzzy Identity-Based encryption [M]// Advance in Cryptology-EUROCRYPT 2005. Berlin, Germany: Springer-Verlag, 2005: 557-557

[5] Boneh D, Boyen X. Efficient selective Identity-Based encryption without random oracles[J]. J. Cryptology, 2011, 24(4): 659-693

[6] Boneh D, Boyen X. Efficient Selective-ID secure Identity-Based encryption without random oracles[M]// Advances in Cryptology-EUROCRYTP 2004. Switzerland: Springer Berlin Heidelberg, 2004: 223-238

[7] Boneh D, Franklin M. Identity-Based encryption from the weil pairing[J]. SIAM Journal on Computing, 2003, 32(3): 586-615

[8] Backes M, Gagn M, Thyagarajan S A K. Fully secure Inner-

Product proxy Re-Encryption with constant size ciphertext[C]// SCC'15. Singapore: ACM, 2015: 31-40

[9] Goyal V, Pandey O, Amit S, et al. Attribute-Based encryption for fine-grained access control of encrypted data [C] // 13th ACM Conference on Computer and Communications Security. Alexandria, VA, United states: ACM, 2006: 89-98

[10] Bethencourt J, Amit S, Brent W. Ciphertext-policy attribute-based encryption[C]// IEEE Symposium on Security and Privacy, 2007(SP '07). Berkeley, CA, United states, 2007: 321-334

[11] Cheung L, Newport C. Provably secure ciphertext policy ABE [C]//14th ACM Conference on Computer and Communications Security. Alexandria, Virginia, USA: ACM, 2007: 456-465

[12] Khader D. Attribute based search in encrypted data[C]// 2014 ACM Workshop on Information Sharing and Colla. Scottsdale, AZ, United States: ACM, 2014: 31-40

[13] Chase M, Chow S M. Improving privacy and security in multi-authority attribute-based encryption [C] // 16th ACM Conference on Computer and Communications. Chicago, IL, United States: ACM, 2009: 121-130

[14] De Caro A, Vincenzo I. Jpbc: Java pairing based cryptography [C] // 2011 IEEE Symposium on Computer and Communications. Kerkyra, Corfu, Greece, 2011: 850-855

(上接第 166 页)

参 考 文 献

[1] Zang Tian-ning, Yun Xiao-chun, Zhang Yong-zheng. A Model of Network Device Corrdinative Run[J]. Chinese Journal of Computers, 2011, 34(2), 216-228(in Chinese)
臧天宁,云晓春,张永铮. 网络设备协同联动模型[J]. 计算机学报,2011,34(2):216-228

[2] Wang B Y, Yang H P, Zhang S M. Research on application of interaction firewall with IDS in distribution automation system [M]// Advances in Electronic Engineering, Connumication and management Vol 1. Springer, 2012: 527-532

[3] Zheng Li-ming, Zou Peng, Jia Yan. How to Extract and Train the Classifier in Traffic Anomaly Detection System[J]. Chinese Journal of Computers, 2012, 35(4): 719-729(in Chinese)
郑黎明,邹鹏,贾焰. 网络流量异常检测中分类器的提取与训练方法研究[J]. 计算机学报,2012,35(4):719-729

[4] Ahmed M, Mahmood A N. Novel Approach for Network Traffic Pattern Analysis using Clustering-based Collective Anomaly Detection[J]. Annals of Data Science, Springer, 2015, 2(1): 111-130

[5] Zhang Bin, Yang Jia-hai, Wu Jian-ping. Survey and Analysis on the Internet Traffic Model[J]. Journal of Software, 2011, 22(1): 115-131(in Chinese)
张宾,杨家海,吴建平. Internet 流量模型分析与评述[J]. 软件学报,2011,22(1):115-131

[6] Alotibi G, Li F, Clarke N. Behavioral-Based Feature Abstraction from Network Traffic[C]// ICCWS 2015. 2015: 176-188

[7] Yang Xin-yu, Yang Shu-sen, Li Juan. A Flooding-Based DDoS Detection Algorithm Based on Non-Linear Preprocessing Network Traffic Predicted Method[J]. Chinese Journal of Computers, 2011, 34(2): 395-405(in Chinese)
杨新宇,杨树森,李娟. 基于非线性预处理网络流量预测方法的泛洪型 DDoS 攻击检测算法[J]. 计算机学报,2011,34(2):395-405

[8] Hofleitner A, Herring R, Abbeel P. Learning the dynamics of arterial traffic from probe data using a dynamic Bayesian network[J]. IEEE Transactions on Intelligent Transportation System, 2012, 13(4): 1679-1693

[9] Wei Xiong, Hu Han-ping, Laurence T. Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications[J]. Information Sciences, 2014 (258): 403-415

[10] Yang Yue. Network Traffic Anomaly Detection Method Based on a Feature of Catastrophe Theory[J]. CHIN. PHYS. LETT., 2010, 27(6): 116-124

[11] Lin Jian-ren, Yang Xiao-long, Long Ke-ping, et al. Catastrophe Model Construction and Verification for Network Anomaly Detection[C]// SPIE Proceedings. Vol. 7137, 2008: 70-81

[12] Wei Xiong, Nai Xue-xiong, Laurence T. Yang. Network Traffic Anomaly Detection based on Catastrophe Theory [C] // 2010 IEEE GLOBECOM Workshops. 2010: 2070-2074

[13] Gu J, Chen S. Nonlinear Analysis on Traffic Flow Based on Catastrophe and Chaos Theory[J]. Discrete Dynamics in Nature and Society, 2014, 23(3): 253-264

[14] Yang Xiao-long, Zhang Min, Hu Wu-sheng. IP Network Anomalous Behaviors Detection Mechanism[J]. Journal of University of Electronic Science and Technology of China, 2011, 40(6): 892-897(in Chinese)
阳小龙,张敏,胡武生. 基于尖点突变模型的 IP 网络异常行为检测方法[J]. 电子科技大学学报,2011,40(6):892-897

[15] Zhang Xian-jiang, Liu Xiao-qiang. Nonlinear Network Traffic Prediction Model Based on Parameters Joint Optimization[J]. Computer Engineering and Application, 2014, 50(6): 64-67(in Chinese)
张显江,刘小强. 一种参数联合优化的网络流量非线性预测模型[J]. 计算机工程与应用,2014,50(6):64-67

[16] Wen Xiang-xi, Meng Xiang-ru, Ma Zhi-qiang. The Chaotic Analysis and Trend Prediction on Small-Time Scale Network Traffic [J]. ACTA Electronica Sinica, 2012, 40(8): 1609-1616(in Chinese)
温祥西,孟相如,马志强. 小时间尺度网络流量混沌性分析及趋势预测[J]. 电子学报,2012,40(8):1609-1616

[17] Kane J, Lawrence J, Farnon M. Analysis of network traffic: 883870[P].

[18] 胡晓洁. 正态分布及其扩展综述[J]. 数学学习与研究,2014(3): 92-94

[19] Kolbusz J, Rozycki P, Korniak J. The Simulation of Malicious Traffic Using Self-similar Traffic Model[M]// Human-Computer Systems Interaction: Background and Applications 2. Springer, 2012: 327-341