Journal of Computer Applications
计算机应用, 2020, 40(2): 497 - 502
ISSN 1001-9081
CODEN JYIIDU
2020-02-10
http://www.joca.cn

文章编号:1001-9081(2020)02-0497-06
DOI:10.11772/j.issn.1001-9081.2019091634

基于属性加密的多用户共享ORAM方案

付　伟[1],顾晨阳[1*],高　强[2]
(1. 海军工程大学 信息安全系,武汉 430033; 2. 海军联合参谋部 指挥保障大队,北京 100841)
(*通信作者电子邮箱591483995@qq.com)

摘　要: 不经意随机访问机(ORAM)是保护用户访问行为隐私安全的关键技术之一,但现有ORAM方案主要针对单用户访问需求,不支持多用户之间的数据共享。结合Ring ORAM方案和属性加密(ABE)技术,设计并实现了一种基于属性加密的多用户共享ORAM方案ABE-M-ORAM。该方案利用属性加密实现了细粒度的访问控制,既保护了用户访问行为的安全,又实现了用户之间便捷的数据共享。理论分析和仿真实验证明该方案具有较高的安全性、实用性以及较好的访问性能。

关键词: 云存储安全;不经意随机访问机;多用户共享;属性加密;访问控制
中图分类号: TP309　　**文献标志码:** A

Multi-user sharing ORAM scheme based on attribute encryption

FU Wei[1], GU Chenyang[1*], GAO Qiang[2]
(1. *Department of Information Security, Naval University of Engineering, Wuhan Hubei* 430033, *China*;
2. *Command and Support Brigade, Naval Staff, Beijing* 100841, *China*)

Abstract: Oblivious Random Access Machine (ORAM) is one of the key technologies to protect the privacy security of the user access behaviors. However, existing ORAM schemes mainly focus on the single-user access requirements and cannot support data sharing between multiple users. Combined with Ring ORAM scheme and Attribute Based Encryption (ABE) technology, a multi-user sharing ORAM scheme was designed and implemented based on attribute encryption, namely ABE-M-ORAM. Attribute encryption was adopted to achieve the fine-grained access control, which can not only protect user access behavior security, but also realize the convenient data sharing between different users. Theoretical analysis and simulation experiments verify the high security, practicability and good access performance of the proposed scheme.

Key words: cloud storage security; Oblivious Random Access Machine (ORAM); multi-user sharing; attribute encryption; access control

0　引言

在云存储环境中,用户把数据上传至云端,由云服务提供商存储和管理数据,用户只拥有数据的所有权,服务提供商拥有数据的直接控制权。即使用户将数据加密上传,也只能保证数据内容本身不被泄露,服务提供商仍然可以通过对用户访问行为的长期记录和观察,开展行为特征分析,从中挖掘出用户的敏感信息或者对解密有用的信息。这些访问行为包括用户访问数据的频度、先后顺序、数据之间的关联关系等。

不经意随机访问机(Oblivious Random Access Machine, ORAM)[1]通过构造恰当的存储结构和访问机制,对用户访问操作进行变换,并增加一些冗余操作,使攻击者无法根据用户的行为来获取有效信息。该技术可以隐藏用户访问行为与访问目标之间的对应关系,是现阶段保护用户访问意图的主要手段之一。ORAM在传统加密保护思想上额外增加了一道安全机制,提高了云端数据安全。

现有ORAM方案[2-8]中数据只能由其拥有者访问,属于单用户操作,通常不支持用户之间的数据共享。然而在互联网时代,数据共享需求比较突出,应用场景较为普遍。目前,仅有部分ORAM方案涉及到多用户共享[9]。为实现ORAM方案内不同用户共享数据的要求,Zhang等[10]在2014年以层次ORAM方案为基础,将用户和服务器通过一系列的串联匿名器连接,设计实现了第一个具有实际应用能力的多用户ORAM方案。该方案中,用户利用自身私钥对共享数据进行加密,再通过串联匿名器依次执行加密运算,最终形成密文,并将密文提交给云服务器,由云服务器存储。基于串联匿名器的多用户共享方案假设用户之间相互信任,并且共同拥有数据访问密钥,然而在更多应用场景中,用户之间不存在完全相互信任,并且希望不同的用户对数据有不同的访问权限,上述方案均不能满足这种需求。因此,设计一个能够实现用户间数据按需共享的ORAM方案具有较大的研究意义和实际应用价值。

收稿日期: 2019-08-20;**修回日期:** 2019-09-25;**录用日期:** 2019-10-09。
基金项目: 国家自然科学基金资助项目(61672531);总装后勤科技重大项目子课题(AWS14R013)。
作者简介: 付伟(1978—),男,湖北武汉人,副教授,博士,CCF会员,主要研究方向:云计算、云安全、分布式计算、信息安全;顾晨阳(1995—),男,江苏丹阳人,硕士研究生,主要研究方向:云存储安全、信息安全; 高强(1982—),男,北京人,硕士,主要研究方向:云计算、云安全、大数据存储。

属性加密(Attribute Based Encryption, ABE)作为一种公钥密码原语,可以为云存储提供灵活细粒度的访问控制,在密文或者密钥中嵌入访问控制策略,实现对数据的灵活访问控制[11-12]。为此,本文利用属性加密对数据进行访问控制,设计实现了一种基于属性加密的新型多用户共享ORAM方案ABE-M-ORAM,在保证数据机密性和访问安全性的前提下实现了用户之间的灵活数据共享。

1 相关研究

1.1 属性加密

属性加密(ABE)[13]是公钥密码学的一种扩展形式。基于身份的密码学机制将用户身份替代为用户属性,加密者通过设定由属性构成的访问策略,指定接受者应具有的属性,只有当用户属性满足密文的访问策略要求时才能解密密文,获取明文。属性加密技术极大丰富了访问策略和用户权限的表达形式。

2005年,Sahai等[14]提出模糊身份加密方案(Fuzzy Identity-Based Encryption),将身份的概念以一组属性表示,采用门限技术实现相似匹配的访问策略,该方案被视为ABE方案的雏形。Goyal等[15]在2006年提出ABE机制,说明属性的概念和意义。ABE机制根据应用场景的不同,分为密钥策略的属性加密机制(Key Policy-Attribute Based Encryption, KP-ABE)[15]和密文策略的属性加密机制(Ciphertext Policy-Attribute Based Encryption, CP-ABE)[13],前者中密钥与访问策略关联,密文与一组属性关联,而后者相反。CP-ABE和KP-ABE在实现细粒度访问控制的同时,还保证了防串谋性。

属性加密模型主要由数据所有者、数据共享者和可信第三方构成,三者之间的关系如图1所示。

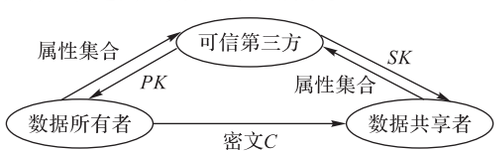

图1 属性加密模型

Fig. 1 Attribute encryption model

数据所有者 对数据拥有绝对所有权,向可信第三方提交数据属性集要求,从而获得可信第三方分发的属性公钥*PK*,利用属性公钥*PK*和访问属性要求将数据明文*M*加密成密文*C*,并将密文*C*分享给数据共享者。

数据共享者 向可信第三方提交自身属性集合,从而获得可信第三方分发的属性私钥*SK*,利用属性私钥*SK*对从数据所有者处获得的密文*C*进行解密。

可信第三方 根据数据所有者提出的属性集产生主密钥*MK*和属性公钥*PK*,利用主密钥和用户共享者属性集合产生属性私钥*SK*,分发属性公钥*PK*和属性私钥*SK*。

属性加密ABE主要有以下四种算法:

1) Setup():设计属性集,根据属性计算主密钥和属性公钥;

2) KeyGen():根据不同用户的属性集,计算用户属性私钥;

3) Encrypt():数据所有者根据访问属性集,利用属性公钥加密明文,得到密文;

4) Decrypt():数据共享者通过自身属性私钥,解密密文,得到明文。

2006年Goyal等[15]基于fuzzy IBE提出一种基于密钥的细粒度访问控制的ABE方案,该方案将访问策略嵌入私钥中,而密文与属性集合相关联,因此被称为密钥策略的属性加密机制(KP-ABE)。KP-ABE本质是一对多的公钥加密技术,该方案访问策略表示为一棵访问树,支持任意单调访问结构和细粒度的访问控制,能够实现属性间的与(and)、或(or)以及门限(threshold)操作。该方案的提出丰富了ABE的性质和适用范围,大大加快了ABE相关研究的发展。

2007年Bethencourt等[13]提出一种基于密文策略的属性加密机制(CP-ABE)。该方案将访问策略嵌入密文中,而密钥与属性集合相关联。数据所有者通过公钥加密明文,并根据密文定义访问结构。由于是将访问结构隐藏在密文之中,使方案的访问策略更加灵活。数据共享者的私钥与自身属性集相关,解密时,私钥必须满足访问策略,才能解密获取明文。

1.2 基于二叉树的Ring ORAM

Ring ORAM是Ren等[16-18]提出的新型ORAM方案。服务器以二叉树结构存储数据块,并在用户端存储一个数据块地址映射表,用于存储每个数据块的存储地址。通过层次递进遍历搜索,较好地隐藏了用户的访问模式,同时完成数据的高效访问和传输。

将数据块存储在大小为$b = O(\log N)$的*bucket*中,以*bucket*作为二叉树的节点,建立高度为$h = \log N$的二叉树,共有N个叶子节点。服务器将数据块存储在二叉树的节点中,用该节点的子叶子节点表示存储地址。在本地设置缓冲区*stash*,用于存储云服务器提交的数据块*bucket*。Ring ORAM二叉树数据存储结构如图2所示。

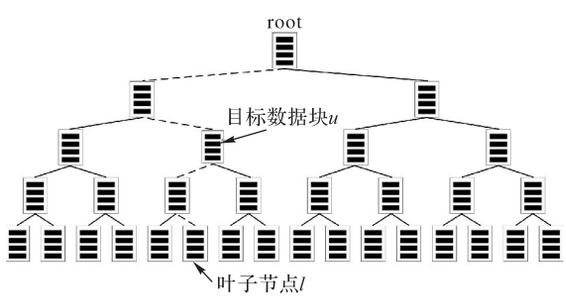

图2 Ring ORAM算法的数据结构

Fig. 2 Data structure of Ring ORAM algorithm

图2中目标数据块u的地址为叶子节点l,则说明目标数据块存储在路径$path(l)$上的某一个*bucket*中;路径$path(l)$表示从根节点*root*到叶子节点l的路径,即图中虚线路径。

Ring ORAM方案执行时,用户向服务器提交访问需求,并查询目标数据块所在路径。从*root*节点开始,沿着目标路径依次搜索每一个节点*bucket*,直至叶子节点。若仍未找到目标数据块,则遍历*stash*,查找目标数据块。用户操作结束后,为新数据块分配新的地址,并更新数据块地址映射表。最后把新数据块写回*stash*中。

Ring ORAM中的每个*bucket*中的有效数据块有X个,无效数据块有Y个。*bucket*中的有效数据块被读取至缓冲区*stash*后,服务器会将*bucket*中的原数据块删除,由于*bucket*中的有效数据块只有X个,也就说,当对一个*bucket*进行X次读取操作后,需要对该*bucket*进行重组。因此,为保证数据的茫然性,每进行$O(X)$次访问操作,就要选择对服务器的某一个二叉树存储路径进行重组操作。重组操作时,将该路径上所有数据块读取到*stash*中,然后从该路径的叶子节点开始,把

stash 中的数据块写回,写回时要保证 *bucket* 中的数据块离自身的叶子节点最近。

1.3　基于串联匿名器的ORAM方案

基于串联匿名器的ORAM方案[19-20]主要是通过在用户和云存储服务器之间引入一系列协作但相互独立的匿名器,从而实现多用户数据共享。当用户需要查询数据时,由匿名器作为中间信息传递的桥梁,用户的访问请求和云存储服务器的应答都将由匿名器转发。

当用户需要访问某些数据项时,利用匿名器来防止用户与云存储服务器进行信息交互,保护了用户的身份信息;而且用户不需要存储数据和身份密钥的相关信息避免攻击者通过用户和云存储服务器的交互信息来窃取用户的隐私信息。

由于多个串联匿名者相互独立,所以当部分匿名器不能工作时,用户的访问行为信息仍然是安全的。在体系结构中,串联匿名器整体被云存储服务器虚拟为单个用户,而且有且仅有匿名器可以和云存储服务器进行信息交互。

此方案虽然能够解决多个用户之间共享数据的问题,但访问效率很低,而且无法鉴别访问用户的身份,不能实现基于用户身份的权限访问。因此,设计一个访问效率高,并且能够实现根据用户不同身份分配访问权限的多用户共享ORAM模型具有很大的实际应用前景。

1.4　多用户ORAM模型

为解决多用户共享云存储服务器上的数据,孙晓妮等[21]在2016年提出了一种基于传统二叉树存储结构的多用户(Binary-Tree-Structed Multiple user, BTS-M) ORAM模型。该模型通过引入可信第三方作代理,作为用户和服务器之间的桥梁,用于数据传输和各类参数的生成。BTS-M ORAM模型主要由用户、代理和云存储服务器三部分组成。用户作为数据的上传者和使用者,拥有向服务器上传数据和从服务器中下载的权限;代理作为可信第三方,作为用户与服务器之间的数据传递者,同时运行参数和密钥生成算法生成各类参数和密钥,并分发给不同的用户;云存储服务器作为数据的存储者,接收并存储用户上传的数据,以及向用户提供所查找的目标数据。每个用户都需要与代理构建信息传输渠道,将代理作为信息集中和传输的渠道,不会直接与云存储服务器进行数据传递。因此,需要将原先由不同用户本地存储的位置映射表统一汇总到代理,并由代理进行位置映射表的整合,形成服务器中数据块的位置映射表。

在BTS-M ORAM模型之中,执行的主要算法为以下两种:

1) $bucket.ReadAndRemove(s)$:在节点 *bucket* 中搜索访问数据块 s,访问后移除数据块 s。

用户在节点 *bucket* 中访问数据块 s 时,需要遍历访问节点 *bucket* 中的所有数据块。访问方法为,先从节点 *bucket* 中读取一个密文数据块 m,并将密文数据块 m 提交给作为数据传输桥梁的代理,由代理对密文数据块 m 进行第一次解密,得到解密数据块 m'。代理将解密数据块 m' 交给提出数据访问申请的用户,由用户对解密数据块 m' 进行第二次解密,得到最终的明文数据块 M。如果该数据块为目标数据块 s,则返回给代理一个无效数据块;如果该数据块不是目标数据块,则将该数据块直接加密后返回给代理。代理得到数据块后,先加密再交还给服务器,由服务器将数据块存储在原位置。当对节点 *bucket* 中所有数据块都进行一次访问后,算法运行结束。如果 $bucket.ReadAndRemove(s)$ 算法执行的结果为数据块 s,那么表明用户从该节点成功访问到数据块 s;如果 $bucket.ReadAndRemove(s)$ 算法执行的结果为无效数据块,那么表明该节点不存在数据块 s,用户访问失败。

2) $bucket.Add(s, d)$:将数据块 s 写入节点 *bucket* 中。

用户在节点 *bucket* 中写入数据块 s 时,需要遍历访问节点 *bucket* 中的所有数据块。访问方法为,先从节点中读取一个密文数据块 m,并将密文数据块 m 提交给作为数据传输桥梁的代理,由代理对密文数据块进行第一次解密,得到解密数据块 m'。代理将解密数据块 m' 交给提出数据访问申请的用户,由用户对解密数据块 m' 进行第二次解密,得到最终的明文数据块 M。当用户得到的数据块为有效数据块,则直接将该数据块返回给代理;当用户第一次从代理得到无效数据块时,将数据块 (s, d) 作为新数据块加密后发送给代理,之后得到的无效数据块的处理方法与有效数据块相同。代理得到数据块后,先加密再交还给服务器,由服务器将数据块存储在原位置。当对节点 *bucket* 中所有数据块都进行一次访问后,算法运行结束。如果 $bucket.Add(s, d)$ 算法执行的结果为数据内容 d,则表明已经将数据块 s 成功存储在该节点 *bucket* 之中;如果 $bucket.Add(s, d)$ 算法执行的结果为空,则表明没有成功将数据块 s 存储在该节点 *bucket* 之中。

2　基于属性加密的多用户共享ORAM方案

基于属性加密的多用户共享ORAM方案ABE-M-ORAM的是在BTS-M ORAM模型的基础上,结合属性加密技术而设计实现的新型ORAM模型,它可以有效解决当下多用户差别数据共享问题,同时能够为数据提供有效的保护。

2.1　方案介绍

ABE-M-ORAM的主体包括用户(数据所有者和数据共享者)、可信第三方和云端服务器[22]。用户和服务器不直接通信,而是由可信第三方负责两者之间的数据传递。可信第三方除了进行数据传递,还需要根据每一个接入的用户的属性,完成具有属性特性的密钥生成和分发工作;同时,还建立本地缓冲区 *stash* 和存储一张数据块地址映射表,记录每个数据块所在路径信息。数据在云端服务器以二叉树的存储结构存储,以 *bucket* 为基本存储单元。

2.1.1　用户接入阶段

用户0(数据所有者)将自身属性集合提交至可信第三方,可信第三方则根据用户0提交的属性集合生成主密钥 MK 和属性公钥 PK,保存主密钥,并将属性公钥发布在公开网络。

用户 i(数据共享者)将自身属性集合同样提交给可信第三方,可信第三方则根据用户 i 提交的属性集合生成包含个人属性集合信息的用户属性私钥 SK_i,并通过保密通信渠道将 SK_i 发送给用户 i。

2.1.2　数据上传阶段

用户0从公开渠道获取属性公钥 PK,利用属性公钥 PK 加密明文数据块 M,生成密文数据块 C;然后将密文数据块 C 提交给可信第三方和云存储服务器。

可信第三方获取密文数据块 C,为其随机分配路径地址,并记录在数据块地址映射表中;随后将密文数据块 C 存放在 *stash* 中。

2.1.3　数据访问阶段

1) 用户 i 向可信第三方提出访问请求。

2) 可信第三方查询留存的属性密钥 SK_i,判断用户 i 是否具有访问权限,验证不通过则驳回访问请求,通过则搜索数据

块地址映射表，确定数据所在的目标块路径地址。

3）从*root*节点开始，沿着目标路径依次搜索每一个节点，找到目标数据块，则将目标数据块提交给可信第三方；若未找到或者在之前节点已经找到目标数据块，则提交一个无效数据块。

4）若仍未找到目标数据块，则可信第三方遍历本地缓冲区*stash*，查找目标数据块。

5）可信第三方将目标数据块发送给用户i。

6）用户i利用属性私钥SK_i对目标数据块解密获得明文数据块M，进行相应的操作，更新为新的明文数据块M'。

7）用户i同样利用公开渠道获得的属性公钥PK将新的明文数据块M加密变成新的密文数据块C'，并提交给可信第三方。

8）可信第三方为新的密文数据块C'分配新的地址，并更新数据块地址映射表，然后将新的密文数据块C'写回*stash*中。

2.2 系统模型

ABE-M-ORAM系统模型主要有三部分：用户群、可信第三方和云存储服务器，如图3所示。用户群又分为数据所有者和数据共享者。模型构建三部分之间的相互关系，并建立通信，从而实现具有安全性的ABE-M-ORAM系统。

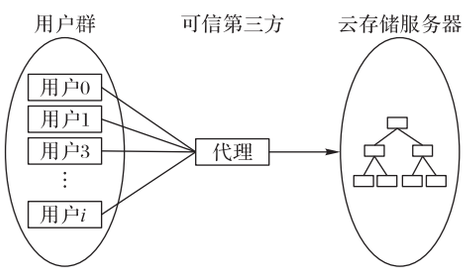

图3 ABE-M-ORAM系统模型

Fig. 3 ABE-M-ORAM system model

2.2.1 构建方法

根据系统模型，设计模型构成，构建多用户访问环境。由多个用户组成的用户群构成数据提交和数据访问端，云存储服务器提供数据存储服务功能。将可信第三方作为二者的连接枢纽，进行信息交换。用户群、代理和云存储服务器三部分共同组成了ABE-M-ORAM系统模型。

2.2.2 模型描述

用户i：用户群中的用户，既可以担任数据所有者的身份，也可以担任数据共享者的身份，二者并不冲突。但在某一次访问行为中，只能拥有一种身份，担任数据所有者或者是数据共享者。

代理：由可信第三方担任，主要需要承担用户群和云存储服务器之间信息传递，负责二者的沟通。为了保证访问的安全，代理还需要具有用户身份认证等功能；与此同时，系统初始化时，代理还需要产生密钥和根据不同用户的属性分配密钥。

云存储服务器：作为云端的数据存储端，主要负责对数据进行存储。服务器采用二叉树存储结构，内置ORAM方案，极大地提高了数据的安全性，保护了用户的访问行为。

2.2.3 系统特点

ABE-M-ORAM方案结合属性加密，能较好地实现多用户共享的功能。该方案主要具有以下三个优点：第一，实现用户细粒度划分，利用属性加密，实现访问控制，对用户数据进行更好的保护，具有较好的实用性；第二，基于属性加密的数据共享根据用户属性进行访问控制，能够便捷地增加和删除用户，而不影响整体，具有良好的适用性；第三，属性加密和ORAM方案都能较好地保护用户数据，二者结合，能够更好地对用户数据进行保护，具有强安全性。

2.3 算法设计

1）Initalize()：可信第三方初始化生成主密钥，并根据用户属性产生和分发属性公钥和属性密钥。

2）Enc()：数据拥有者用户0根据属性公钥加密数据。

3）DataAdd()：可信第三方向云存储服务器添加数据。

4）IdVer()：验证数据共享者用户i属性是否满足数据所有者对其搜索数据的属性要求。

5）DataSearch()：可信第三方从云存储服务器搜索数据。

6）Dec()：数据共享者用户i根据属性私钥解密数据。

7）Recombine()：云存储服务器重排数据。

3 方案分析

3.1 安全性分析

属性加密是根据身份加密创新提出的，但属性加密仍然属于公钥加密。公钥加密主要由四个算法构成，其中系统初始化Setup()、密钥生成KeyGen()和信息加密Encrypt()三个算法是概率算法，而解密算法Decrypt()是确定性算法。常见的安全模型有选择明文攻击安全和选择密文攻击安全模型。

选择明文攻击的定义是攻击者选择任意确定明文，通过掌握的加密方法获取密文，通过明密文对比，获取解密信息。CP-ABE机制是选择明文攻击安全（INDistinguishability under Chosen-Plaintext Attack，IND-CPA），即攻击者无法通过选择明文攻击获取任何有用信息。CP-ABE的密文与访问策略有关，如果任何具有下面优势的攻击者都能忽略那么就是IND-CPA。攻击模型如下：

1）初始阶段：攻击者选择要挑战的访问结构τ，然后传给挑战者。

2）Setup阶段：挑战者运行Setup()算法，得到公钥PK并交给攻击者。

3）查询阶段1：挑战者随机选择不满足τ的属性集，运行密钥生成算法，将生成的用户私钥交给攻击者。

4）挑战阶段：攻击者给挑战者一个挑战属性集及两个等长的明文M_1、M_2，而且攻击者不知道挑战属性集的密钥。挑战者从两个明文中随机选取一个$a \in \{0, 1\}$，然后利用τ进行加密，获得密文C并交给挑战者。

5）查询阶段2：重复选择阶段1。

6）猜测阶段：攻击者输出猜测值$a' \in \{0, 1\}$，如果$a' = a$，则获得攻击成功。

在模型中，攻击者的优势定义为$Adv = |\Pr[a = a'] - 1/2|$。在多项式时间内，攻击者的优势是可以忽略的，故此方案在IND-CPA下是安全的，即为选择明文攻击安全。

3.2 性能分析

计算机：Lenovo ideaiPad 410P，操作系统：Windows 7旗舰版64 bit，CPU：Intel Core i5-4200M CPU 2.50 GHz，运行内存：8 GB。运行Matlab R2017a版本，进行仿真实验。

3.2.1 实验方法

本实验主要进行多用户访问测试，但Ring ORAM方案是单用户方案，因此对Ring ORAM方案进行调整，得到改进

Ring ORAM方案。因为数据共享者访问数据时需要获得数据块地址,以及搜索数据时需要涉及数据缓冲区,而数据块地址表和数据缓冲区都是数据所有者本地存储;因此,对单用户的Ring ORAM方案进行改进,将数据所有者作为数据共享者与云存储服务器的第三方,负责数据块地址查询工作和担任数据缓冲区的角色。数据共享者访问数据时,首先需要与数据所有者建立通信,通过数据所有者获取数据块地址,并在云存储服务器和数据所有者的缓冲区中搜索数据。

ABE-M-ORAM方案和传统的基于串联匿名器的ORAM方案以多用户共享为设计目标,根据方案的设计原理和方法,在Matlab上分别编写算法,仿真多用户访问共享云存储数据。

3.2.2　ABE-M-ORAM方案与改进Ring ORAM方案对比

ABE-M-ORAM方案是在Ring ORAM方案的基础上集合属性加密而形成的多用户共享方案。本次实验在Matlab上仿真,针对ABE-M-ORAM方案和改进Ring ORAM方案,模拟不同用户数量同时访问100次共享数据。实验获取每个用户的访问总时间,计算平均每个用户100次访问的总时间。通过分析平均用户访问时间,研究同时访问的用户数量在不同方案中对访问效率的影响。

表1　ABE-M-ORAM方案和改进Ring ORAM方案的平均用户访问时间对比　　单位:s

Tab. 1　Average user access time comparison of ABE-M-ORAM scheme and improved Ring ORAM scheme　　unit: s

访问用户数	ABE-M-ORAM方案	改进Ring ORAM方案
2	0.268 9	0.381 7
4	0.271 2	0.514 7
6	0.270 5	0.843 8
8	0.267 9	1.116 5
10	0.275 8	1.354 2

在改进Ring ORAM方案中,数据共享者访问数据时,首先与数据所有者建立信息交互渠道,将数据访问请求发送给数据所有者。数据所有者根据数据共享者的访问请求,从云存储服务器获取数据,并传递给数据共享者。因为数据块地址表和数据缓冲区都建立在数据所有者本地,从云服务器端看,还是与数据所有者的双向访问,仍然属于单用户进行操作。所有的数据的访问操作都是由数据所有者进行,当访问的用户较多时,访问请求需要进行排队。同时访问的用户越多,平均访问时间越长,访问效率越低。

在ABE-M-ORAM方案中,数据所有者不需要参加任何工作,身份认证和信息传递的工作由代理负责。不同的用户访问时通过代理传输数据,而代理可以同时处理多个用户的访问请求,因此,多个用户可以并行访问,减少了用户大量的等待时间,极大地缩短了用户的访问时间,提高了用户的访问效率。而且,用户的平均访问时间几乎不受同时访问用户数的影响。另外,每个用户在访问代理时,互不影响。当一个用户访问出现错误时,其他用户仍然可以正常访问。

3.2.3　ABE-M-ORAM方案与基于串联匿名器的ORAM方案对比

在Matlab上,模拟仿真基于串联匿名器的ORAM方案和ABE-M-ORAM方案。实验设定有2个用户在访问云存储服务器内的数据,获取不同访问数据量,即不同访问次数情况下,计算平均每个用户单次访问时间,分析研究不同方案中访问次数对访问效率的影响。

在基于串联匿名器的ORAM方案中,用户每次访问数据前,都需要进行严格的身份认证,多用户同时访问时,需要进行多次身份认证。随着访问数据量增加、访问次数的增多,用户的平均单次访问时间在逐渐变长。ABE-M-ORAM方案通过用户属性来对访问进行细粒度控制,利用可信第三方作为代理来进行身份认证,减少了身份认证时间,提高了身份认证的效率。访问数据的增加,对用户的平均单次访问时间影响较小,方案的稳定性更好。同时,可信第三方作为代理,还能够有效提高数据通信的效率,加快数据传递,提高用户访问数据的效率。

表2　ABE-M-ORAM方案与基于串联匿名器的ORAM方案的平均用户单次访问时间对比　　单位:ms

Tab. 2　Average user single access time comparison of ABE-M-ORAM scheme and serial anonymous device based ORAM scheme　　unit: ms

访问次数	ABE-M-ORAM方案	基于串联匿名器的ORAM方案
100	2.689	2.738
200	2.702	2.954
300	2.699	3.319
400	2.717	3.966
500	2.721	4.704

3.2.4　ABE-M-ORAM方案与BTS-M-ORAM方案对比

在Matlab上,模拟仿真BTS-M-ORAM方案和ABE-M-ORAM方案。实验中,模拟不同数量用户向云服务器同时提出对数据的100次访问请求,即获取不同方案完成多用户访问所消耗的时间,计算平均完成每个用户所有访问所需要的时间,分析不同方案中多用户访问的时间效率。

表3　ABE-M-ORAM方案与BTS-M-ORAM方案的平均用户访问时间对比　　单位:s

Tab. 3　Average user access time comparison of ARE-M-ORAM scheme and BTS-M-ORAM scheme　　unit: s

访问用户数	ABE-M-ORAM方案	BTS-M-ORAM方案
2	0.268 9	0.401 2
4	0.271 2	0.524 5
6	0.270 5	0.660 2
8	0.267 9	0.814 7
10	0.275 8	0.974 4

在BTS-M-ORAM方案中,用户提出对云存储服务器中存储数据的访问请求后,代理首先需要对用户进行身份验证,明确用户对该数据是否具有访问权限,具有权限则代理向云存储服务器提取数据,否则直接拒绝用户的访问请求。而且用户的访问权限不是永久授权的,在访问期间,代理需要对用户进行多次身份验证,影响访问效率。在ABE-M-ORAM方案中,采用了属性加密,保证了用户只能对具有访问权限的数据进行解密,无法获取权限之外的数据,因此,不需要对用户进行身份验证,能大大提高用户的访问效率,节约代理的运行资源,保证数据访问的高效性。

4　结语

基于属性加密作为一种新型的密码方案,能够实现对数据的灵活细粒度访问控制,使得它可以广泛地应用于政治、军事、商业等诸多领域,尤其是属性基加密为解决云存储环境下数据的多用户安全共享提供了一种解决方案。现阶段,对基

于属性加密机制的研究虽然成果显著,但是由于实际运用中还出现了很多问题,所以还有许多地方有待改进。下一步的研究重点主要涉及到以下两个方面:第一,为了保证安全,增加了可信第三方和存储了大量无效数据块,对用户的访问效率产生了很大的影响。同时,为确保安全性,可信第三方要对密钥进行维护和更新,占用了更多的计算资源和存储空间,一定程度上影响了系统的工作效率。所以,如何在保证安全的基础上提高效率是主要的研究方向之一。第二,在属性修正机制方面,效率和安全依然是重中之重。可信第三方需要根据数据共享者属性产生对应的私钥,而数据共享者的属性并不是保持不变的。数据共享者属性的不断变化将占用可信第三方大量的计算资源,因此如何解决数据共享者属性变化带来的效率降低问题,也是现阶段主要的研究方向之一。

参考文献(References)

[1] 李树凤. 抗访问模式泄露的ORAM技术研究[D]. 济南:山东大学, 2016: 9-22. (LI S F. Research on ORAM technique to protect data acess pattern[D]. Jinan: Shandong University, 2016: 9-22.)

[2] STEFANOV E, SHI E, SONG D. Towards practical oblivious RAM [EB/OL]. [2019-02-12]. http://www. dhosa. org/wp-content/uploads/2012/08/towards-oram. pdf.

[3] SHI E, CHAN T H H, STEFANOV E, et al. Oblivious RAM with $O((\log N)^3)$ worst-case cost[C]// Proceedings of the 2011 International Conference on the Theory and Application of Cryptology and Information Security, LNCS 7073. Berlin: Springer, 2011: 197-214. .

[4] ZAHUR S, WANG X, RAYKOVA M, et al. Revisiting square-root ORAM: efficient random access in multi-party computation [C]// Proceedings of the 2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2016:218-234.

[5] ZHANG J, MA Q, ZHANG W, et al. TSKT-ORAM: a two-server *k*-ary tree ORAM for access pattern protection in cloud storage[C]// Proceedings of the 2016 IEEE Military Communications Conference. Piscataway: IEEE, 2016:527-532.

[6] BINDSCHAEDLER V, NAVEED M, PAN X, et al. Practicing oblivious access on cloud storage: the gap, the fallacy, and the new way forward[C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2015:837-849.

[7] LIU Z, HUANG Y, LI J, et al. DivORAM: towards a practical oblivious RAM with variable block size[J]. Information Sciences, 2018, 447:1-11.

[8] 苑丹丹. 基于ORAM的隐私保护数据共享方案研究[D]. 济南:山东大学, 2018: 12-32. (YUAN D D. Research on data sharing scheme of privacy protection based on ORAM[D]. Jinan: Shandong University, 2018: 12-32.)

[9] 熊露. 基于属性加密的访问结构隐藏技术研究[D]. 成都:西南交通大学, 2018: 15-19. (XIONG L. Research of the access structure hiding technology based on attribute encryption[D]. Chengdu: Southwest Jiaotong University, 2018: 15-19.)

[10] ZHANG J, ZHANG W, QIAO D. A multi-user oblivious RAM for outsourced data[R]. Iowa State University, 2014.

[11] 史慧丽. 基于属性的云存储访问控制机制研究[D]. 重庆:重庆邮电大学, 2016: 22-26. (SHI H L. Research on access control mechanism of cloud storage based on attribute [D]. Chongqing: Chongqing University of Posts and Telecommunications, 2016: 22-26.)

[12] 刘秀彬. 基于云计算的属性加密访问控制研究[J]. 无线互联科技, 2017(12):30-31. (LIU X B. Research on attribute encryption access control based on cloud computing[J]. Wireless Internet Technology, 2017(12):30-31.)

[13] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]// Proceedings of the 2007 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2007: 321-334.

[14] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// Proceedings of the 2005 Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 3494. Berlin: Springer, 2005: 457-473.

[15] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006:89-98.

[16] REN L, FLETCHER C, KWON A, et al. Constants count: practical improvements to oblivious RAM[C]// Proceedings of the 24th USENIX Security Symposium. Berkeley, CA: USENIX Association, 2015:415-430.

[17] DAUTRICH J, STEFANOV E, SHI E. Burst ORAM: minimizing ORAM response times for bursty access patterns[C]// Proceedings of the 23rd USENIX Security Symposium. Berkeley: USENIX Association, 2014: 749-764.

[18] MAAS M, LOVE E, STEFANOV E, et al. PHANTOM: practical oblivious computation in a secure processor[C]// Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013:311-324.

[19] 张少波,王国军,刘琴,等. 基于多匿名器的轨迹隐私保护方法[J]. 计算机研究与发展, 2019, 56(3):576-584. (ZHANG S B, WANG G J, LIU Q, et al. Trajectory privacy protection method based on multi-anonymizer[J]. Journal of Computer Research and Development, 2019, 56(3): 576-584.)

[20] NAKAMURA Y, SAWAGUCHI S, NISHI H. Implementation and evaluation of an FPGA-based network data anonymizer[J]. IEEJ Transactions on Electrical and Electronic Engineering, 2017, 12 (S1): S134-S140.

[21] 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. (SUN X N, JIANG H, XU Q L. Multi-user binary tree based ORAM scheme[J]. Journal of Software, 2016, 27(6): 1475-1486.)

[22] 吴杰铭. 基于属性加密算法的云存储研究[D]. 深圳:深圳大学, 2017: 14-22. (WU J M. Research on cloud storage based on attribute encryption algorithm[D]. Shenzhen: Shenzhen University, 2017: 14-22.)

This work is partially supported by the National Natural Science Foundation of China (61672531), the Sub-project for Major Logistics Technology Project (AWS14R013).

FU Wei, born in 1978, Ph. D., associate professor. His research interests include cloud computing, cloud security, distributed computing, information security.

GU Chenyang, born in 1995, M. S. candidate. His research interests include cloud storage security, information security.

GAO Qiang, born in 1982, M. S. His research interests include Cloud computing, cloud security, big data storage.