文章编号：2095-2163(2019)04-0240-08 中图分类号：TP309.2 文献标志码：A

云存储环境下数据安全共享模型的设计

曾德生[1,3]，骆金维[1,3]，高 静[2,3]，刘倍雄[4]，陈孟祥[4]

（1 广东创新科技职业学院 信息工程学院，广东 东莞 523960；2 广东恒电信息科技股份有限公司，广州 510630；
3 广东省教育云 PaaS 平台工程技术研究中心，广州 510630；4 广东环境保护工程职业学院 机电工程系，广东 佛山 528216）

摘 要： 随着云计算的发展，越来越多的用户将数据存储在云端，而采用传统的明文存储数据的方式不适合于开放的云存储环境，基于对称加密的方案也不适合于云端数据的分享及协同工作。针对用户对云存储中数据安全共享的需求，提出了采用层次化的身份加密技术（HIBE），规范身份标识管理，提高私钥的生成效率及密钥管理的安全性。引入私钥版本号的方法，改进 CP-ABE 算法，提高属性撤销的效率。通过相应分析，共享模型具有较好的安全性，最后采用 Samkumar 的 HIBE 和 John Bethencourt 的 cpabe 工具集进行测试，结果表明该方案有较好的性能表现。

关键词： 云存储；安全共享模型；HIBE；属性撤销

A design of data security sharing model in cloud storage environment

ZENG Desheng[1,3], LUO Jinwei[1,3], GAO Jing[2,3], LIU Beixiong[4], CHEN Mengxiang[4]

(1 School of Information Engineering, Guangdong Innovative Technical College, Dongguan Guangdong 523960, China;
2 Guangdong Hengdian Information Technology Co., Ltd., Guangzhou 510630, China;
3 Guangdong Education Cloud PaaS Platform Engineering Technology Research Center, Guangzhou 510630, China;
4 Department of Mechanical and Electrical Engineering, Guangdong Polytechnic of Environmental Protection Engineering, Foshan Guangdong 528216, China)

【Abstract】 With the development of cloud computing, more and more users store data in the cloud. The traditional plaintext storage method is not suitable for open environment, and the symmetric encryption is also not suitable for cloud data sharing and collaborative work. Aiming at the user's demand for data security sharing in cloud storage, this paper proposes the use of hierarchical identity-based encryption (HIBE), provides standardized identification management, improves private key generation efficiency and key security management. And imported version number for private key, the method improves the CP-ABE algorithm and improves the efficiency of attribute revocation. Samkumar's HIBE and John Bethencourt's cp-abe toolset is utilized, and after the test and analysis, the model has better security. The experimental results show that the scheme has better performance.

【Key words】 cloud storage; security sharing model; HIBE; attribute revocation

0 引 言

云存储是云计算中的热门应用，通过集群技术、分布式计算等技术将异构存储设备通过网络和应用软件等结合起来协同工作，构建一个大型的存储资源池，为企业及个人用户提供数据存储、备份、同步及共享等服务。云存储可以有效地解决各类用户对存储资源需求扩展的问题，已成为一种成熟的服务模式，在企业及个人市场的应用越来越广泛[1-2]。云存储中的数据安全性依赖于云存储服务供应商的管控，但由于云存储架构的开放性、共享性等特征，相较于传统的存储方式，云存储中的安全需求不仅要求保证数据的安全性，还需要包含相应的密钥的分发及更新管理，以及如何实现在密文上进行高效操作等。在多项调查报告中显示，云存储的安全性已经成为用户最关注的问题之一[2-3]。

本文提出一种方案，结合层次化身份标识加密技术（Hierarchical Identity-based Encryption，HIBE）和密文策略属性基加密技术（Ciphertext Policy Attribute-based Encryption，CP-ABE）的特点，设计云存储环境下的数据安全共享模型：CP-AHI(BE)^{2}方案。

在 CP-AHI(BE)^{2}方案中，利用 HIBE 技术构建

基金项目： 广东省教育厅重点平台及科研项目立项（2017GkQNCX130，2017GKTSCX042，2017GKTSCX112，2018GkQNCX065，2018GkQNCX111）。

作者简介： 曾德生（1983-），男，硕士，高级工程师，主要研究方向：Linux、容器、云计算等；骆金维（1980-），男，硕士，副教授，主要研究方向：分布式计算、大数据等；高 静（1975-），女，学士，工程师，主要研究方向：云计算、大数据；刘倍雄（1983-），男，硕士，高级工程师，主要研究方向：软件开发与设计、海量存储；陈孟祥（1982-），男，硕士，高级工程师，主要研究方向：物联网、软件工程。

通讯作者： 曾德生 Email：zengdesheng@ gmail.com

收稿日期： 2019-04-06

层次化的身份标识管理模块，规范身份认证及标识管理，提高属性密钥的生成效率；采用 CP-ABE 算法对云存储服务器中的数据进行加密以保证数据的机密性，实现细粒度的访问控制机制，降低合谋攻击的风险，同时改进 CP-ABE 方案，采用增加密钥版本号的方法[4-5]，提高了密钥撤销的效率[6-7]。通过相应验证，CP-AHI(BE)^{2}方案可以提高数据共享的安全性，并提高云存储系统密钥管理性能。

1　相关工作

1.1　云存储安全现状

随着计算机技术的发展，智能手机等设备的飞速增长以及互联网应用模式的变革，用户对数据存储的容量及性能方面的要求越来越高，运维成本也随之快速增加。由于云计算具有成本低、效率高的优势，结合虚拟化、分布式计算等技术，将大量计算资源、异构存储资源、网络及软件等资源进行整合，形成一个有机整体，对外提供大规模的数据存储服务，实现按需服务等应用模式。为用户提供数据备份、多终端数据同步、用户间数据共享和协同工作等服务，为企业和个人用户的工作和生活带来了极大的便利。

从应用的角度看，云存储对用户是透明的。云存储同样具备云计算的 5 种特征[8]：按需自助、广泛网络接入、资源池化、快速弹性伸缩、可计量服务。因此云存储系统架构通常可以分为 4 个层次：数据存储层、数据管理层、数据接口层和用户访问层，系统架构如图 1 所示。

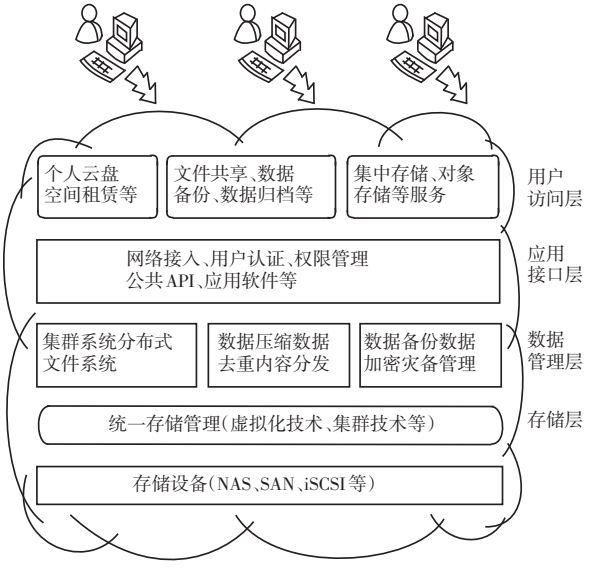

图 1　云存储系统架构

Fig. 1　Cloud storage system architecture

(1)存储层：可采用虚拟化及集群技术，将网络中的 NAS、SAN 等存储设备进行集中式管理，形成存储资源池。

(2)数据管理层：利用集群系统、分布式文件系统等文件管理系统对底层的资源池进行管理，并提供相应的数据压缩、去重和数据备份、加密等功能。

(3)应用接口层：根据用户的需求，提供数据接入的接口，为高层的用户访问层提供用户认证、权限管理等功能。

(4)用户访问层：通过应用接口层提供的标准接口，提供数据访问服务。

在云存储环境下，云存储服务供应商(Cloud Storage Service Providers，CSSP)利用虚拟化等技术手段，实现各类存储设备资源的逻辑共享，将用户的数据存储在动态共享的存储资源池中。用户间的数据可能存放在相同的物理存储设备中，同时用户数据的完全依赖于 CSSP 的保护，因此也带来了第三方依赖性问题[9]。云存储的安全风险分析，见表 1。

表 1　云存储安全风险分析

Tab. 1　Security risk analysis of cloud storage

安全风险	具体表现
一般风险	钓鱼式攻击、DOS 攻击、弱密码暴力攻击等问题
云计算环境带来的风险	数据去重等管理行为，导致用户对数据不可控，面临泄露、滥用风险等问题
	存储设备共享模式，未能提供有效的安全隔离等问题
	第三方信任依赖等问题

1.2　云计算安全模型研究现状

随着云计算应用的不断深入，国内外的研究人员都致力于云计算安全体系架构的研究。2011 年，冯登国总结了云存储环境下的数据安全问题，并提出了如图 2 所示的安全参考框架[10]。

2015 年，工业和信息化部办公厅关于印发《云计算综合标准化体系建设指南》的通知中，也明确提出了云计算综合标准化体系框架。其中安全标准，用于指导实现云计算环境下的网络安全、系统安全、服务安全和信息安全，主要包括云计算环境下的安全管理、服务安全、安全技术和产品、安全基础等方面的标准[8]，如图 3 所示。

1.3　HIBE 及 CP-ABE 算法研究

1.3.1　HIBE

基于身份标识的加密技术(Identity-based Encryption，IBE)是一种基于双线性配对和椭圆曲线的公钥密码技术。通过可信的密钥管理中心，将用户标识融入到密钥中，可以提供加密及身份认证等

功能。与以往的公钥加密相比,IBE 方案可以减少对公钥的查询,提高密钥生成中心的效率[11]。

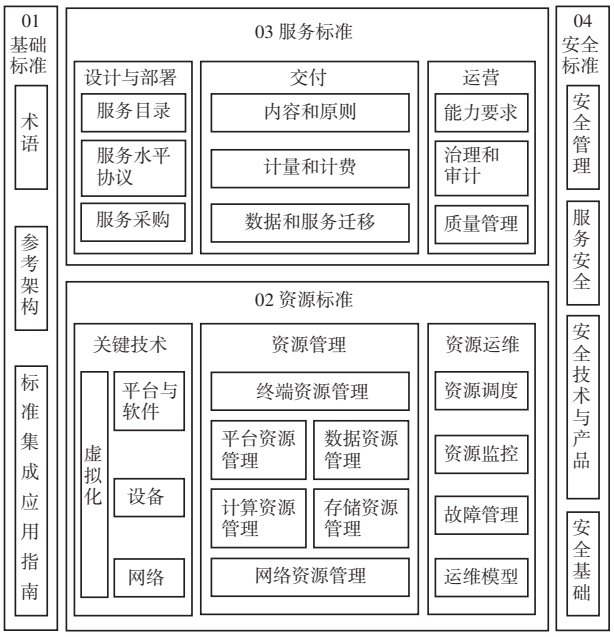

图 2 云计算安全参考框架

Fig. 2 Cloud computing security reference framework

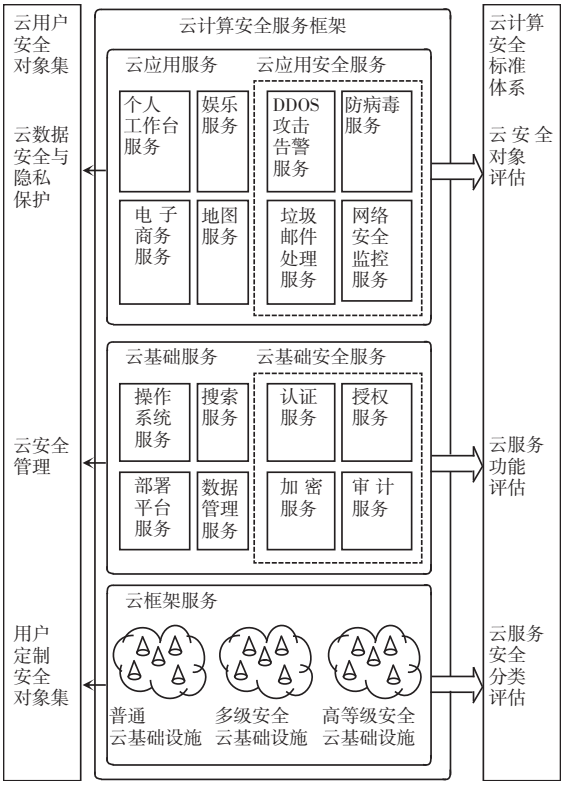

图 3 云计算综合标准化体系框架

Fig. 3 Cloud computing integrated standardization framework

传统的 IBE 管理中心只有独立的私钥生成中心(Private Key Generator,PKG),随着用户数量增加,容易导致 PKG 的负载过高,产生系统瓶颈。为解决这一问题,在基于 IBE 的基础上构建多个 PKG,并将其层次化,将多个 PKG 分层构建成一棵倒置的树,如图 4 所示。

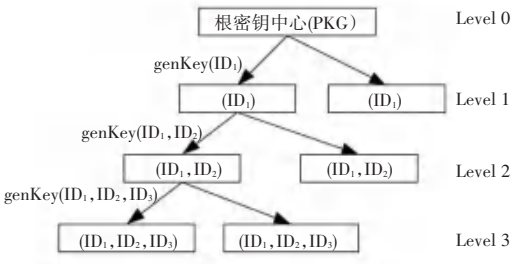

图 4 HIBE 组织结构图

Fig. 4 HIBE organization chart

HIBE 方案相对于 IBE 具有更高的安全性,可以适当缩短密文长度,减少密钥的存储空间,各层 PKG 分担密钥管理任务[12],可以减少加密解密所需的时间,提高系统运行的效率[13-16]。与传统的 PKI 方案比较,HIBE 方案在密钥管理方面具有以下优势,见表 2。

表 2 3 种加密方案风险对比

Tab. 2 Risk comparison of three encryption schemes

密钥安全威胁	PKI	IBE	HIBE
泄露风险	全部泄密	全部泄密	部分
共谋攻击风险	存在风险	存在风险	可解决
私钥风险	存在	存在	可解决

1.3.2 CP-ABE

基于属性的加密技术(Attribute - based Encryption,ABE),可以提供细粒度的非交互式访问控制机制,从而解决传统对称加密机制中一对一的加解密模式,扩展为云存储环境中一对多的多用户分享模式。在 ABE 中,引入了访问结构的概念,密文和密钥根据属性集合生成,可以提供 2 种关联方案[17]:密钥策略的属性加密(Key-policy ABE,KP-ABE)和密文策略的属性加密(Ciphertext - policy ABE,CP-ABE)。

在 KP-ABE 方案中,密钥对应于一个访问控制而密文对应于一个属性集合,解密当且仅当属性集合中的属性能够满足此访问结构。这种设计比较接近静态场景,此时密文用与其相关的属性加密存放在服务器上,当允许用户得到某些消息时,就分配一个特定的访问结构给用户。因此,KP-ABE 算法更适用于查询类的应用。

在 CP-ABE 方案中,密文对应于一个访问结构而密钥对应于属性集合,解密当且仅当属性集合中的属性能够满足此访问结构。这种设计比较接近于

现实中的应用场景，每个用户可以根据自身条件或者属性从属性机构得到密钥，然后加密者来制定对消息的访问控制。因此，CP-ABE 算法更适用于云存储环境下的密文访问控制。方便用户在分享云存储中的数据，无需为每一目标用户分发属性密钥，只需要通过访问结构进行权限管理，大幅度地降低了权限管理的复杂度[7]，提供了更加灵活的访问控制。从功能上实现了“一对多”的加密文件访问控制，解决了云存储中多用户环境应用的瓶颈问题[17-18]。

2　安全共享需求

对于用户而言，数据安全是最重要的需求之一。通常，数据安全包含机密性、完整性、可用性 3 个方面。在云存储环境下，数据的安全包含数据存储的安全性和数据传输的安全性 2 个部分。

(1)机密性。在云存储中，数据的机密性体现在用户对数据存储和传输过程中要求任何个人或 CSSP 在未授权的情况下都无法查看到明文数据，理论上不会出现数据泄露的情形。

(2)完整性。在云存储中，数据的完整性主要体现在数据的存储、传输和使用等情形。当用户进行数据上传或下载等操作时，要求 CSSP 能够根据用户的指令，提供完整的数据读写操作，并提供相应的检测机制，确保用户数据的完整，避免云端数据被伪造或篡改。

(3)可用性。用户的数据存储在 CSSP 中，对用户而言，云端的存储硬件、网络接入都属于不可控的环境。因此，CSSP 如何为用户提高数据的可用性是实现安全共享的重要需求之一。

在云计算中，为了保护用户的数据安全和隐私，大多数方案都是采用非对称(公钥)加密(Public-key cryptography，PKE)技术来保证数据的安全性。PKE 技术经过多年的发展后，演化产生了基于身份标识的加密技术和基于属性的加密技术。

在云计算环境下，供应商采用透明化的方案，用户不需要关注云存储的软硬件系统的部署。相当于用户采用外包的方式将数据存放在 CSSP 的存储服务器中。云存储系统多处于海量用户的应用场景，须满足“M 对 N”的多对多访问模式，供应商的服务器中需要使用合理的方式保护数据加密所使用的大量密钥，用于保障数据拥有者对数据的可控性。因此，完成云存储环境下数据安全共享模型的设计，需要解决以下问题：

(1)如何解决云端存储数据的安全性和可用性，云存储服务供应商(CSSP)在获得用户信任的同时该如何保证服务的可用性。

(2)云存储中数据的机密性与算法复杂度之间存在不可调和的矛盾，CSSP 该采用哪种合适的算法，既提高用户的使用体验又降低服务器的投入。

(3)在用户“M 对 N”的访问模式下，CSSP 该如何解决密钥管理问题，每个数据拥有者都有可能面对多个不同的用户，CSSP 如何实现细粒度访问控制。

(4)当出现用户的注册、注销等，分享的增加、删除、修改等操作，密钥的分配管理都将发生变化，CSSP 该如何解决动态安全性问题。

3　算法与模型设计

3.1　共享模型设计

3.1.1　系统角色

典型云存储环境下的数据安全共享模型中，通常有 4 类实体参与云存储服务供应商(CSSP)、密钥管理中心(Key Management Center，KMC)、数据属主(Data Owner，DO)、数据用户(Data Requester，Dreq)。

(1)CSSP。云存储服务供应商，管理大量的云存储服务器，为用户提供 7 * 24 小时不间断的数据存储及访问服务。

(2)KMC。密钥管理中心，在本文的方案中，KMC 分为层次化身份认证中心和属性密钥加密中心 2 个部分。前者用于身份认证及属性的规范化管理，后者处理相应的属性加密。属性密钥加密中心，通常由一个密钥产生中心(Key Generation Center，KGC)和若干个密钥授权中心(Key Authorization Center，KAC)组成，主要完成密钥的生成、分发、更新及撤销等操作。

(3)DO。数据拥有者，通常为各类企业及个人用户，其将自己的数据存储在云端，并且依靠 CSSP 维护数据。

(4)Dreq。数据用户是 CSSP 的服务对象，可以理解为云存储服务的消费者，访问 DO 在云端共享的数据，并通过相应的密钥解密云端的密文数据。

3.1.2　模型图

在安全共享模型中，结合 HIBE 和 CP-ABE 加密技术，由 CSSP 和 KMC 完成密钥的管理；DO 制定相应的访问控制策略，与 CSSP 协商，生成对称参数密钥对，并利用相应的密钥加密数据后，将密文数据存放在云端。当 Dreq 访问云端的共享数据时，首先

使用自己的账号及密码通过 HIBE 进行身份验证，然后利用自己的私钥及相应授权的属性密钥，通过 CSSP 验证后，解密相应的密文数据，安全共享系统的模型设计如图 5 所示。

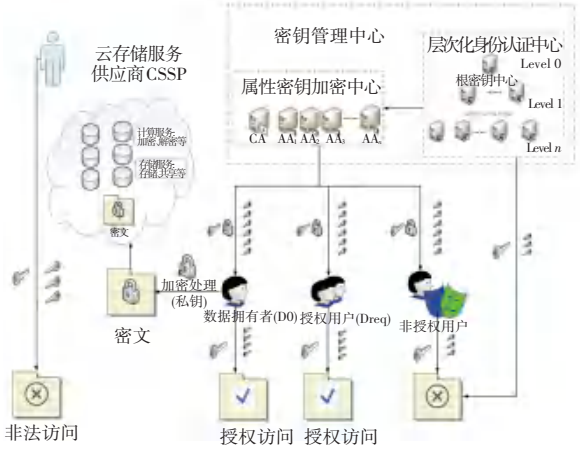

图 5 云存储安全共享模型图

Fig. 5 Cloud storage security sharing model diagram

3.2 CP-AHI(BE)^{2}算法设计

在算法设计过程中，首先利用 HIBE 算法的优势，实现统一规范的身份标识管理，其次根据规范化处理后的细粒度属性，采用改进的 CP-ABE 方案，应用于云存储环境中。

3.2.1 HIBE

在共享模型中，HIBE 模块用于实现身份的认证及相应属性私钥的管理。进行相应的形式化定义后，HIBE 算法加密的流程可以分解为 5 个步骤：

(1)根密钥中心初始化(initSetup)。根密钥中心选取安全参数 k，产生主密钥 s 和系统参数 $params$。其中，系统参数 $params$ 是公开使用的参数，包含明文空间描述 M 和密文空间描述 C，初始根结点的私钥 s（即主密钥）是秘密信息，$M = \{0,1\}^n$，$C = G_1^t \times \{0,1\}^n$，在公开 $params$ 的情况下 s 可以实现保密。

(2)分层密钥中心初始化(levelSetup)。每个用户设置自己的低层密钥，为下一层用户的私钥生成做准备。

(3)生成密钥(keyGen)。根据用户的 ID 首先为用户产生公钥 Q，然后根据公钥等信息计算出私钥 S_t。如果用户是在根密钥中心的下一层，则直接由根密钥中心为用户产生私钥 $genKey(ID_1)$；如果用户在其它层，则由用户的上一层密钥生成中心为用户产生。如 $genKey(ID_1, ID_2)$ 由 ID_1 所在的密钥生成中心产生。

(4)加密(Encryption)。输入系统参数 $params$、接收方(Receiver)用户的身份信息 ID，明文 m、输出相应的密文 c。当发送方(Sender)经秘密安全通道从根密钥中心接收 $params$，使用接收方的公钥 Q_{Rec} 和 $params$ 对明文数据 m 加密，并把密文 c 发送给接收方，加密公式为 $c = EncData(params, Q_{Rec}, m)$。

(5)解密(Decryption)。输入系统参数 $params$、接收方(Receiver)用户的私钥 s_{Rec}、密文 c，输出相应的明文 m。接收方依据(3)的方法从本层 PKG 处得到私钥 S_{Rec} 并从根密钥中心得到 $params$，使用算法对密文 c 解密得到明文 m，$m = DecData(params, S_{Rec}, C)$。

在共享模型中，通过 HIBE 的规范管理规则包含标识管理、命名和访问 3 个方面进行身份认证及属性粒度管理：

(1)规范标识管理规则。规范用户注册、登录、信息维护及注销 4 种规则。

(2)规范标识命名规则。将用户的用户名(ID)、电子邮箱等各种属性按照身份标识命名规则进行标识。

(3)规范标识访问规则。建立标识管理模块，制定相应访问规则及限制策略。当系统接收到用户登录请求时，首先验证接入端是否符合相应规则，然后验证用户登录标识是否合法，最后验证用户的身份。通过用户身份验证后，采用会话模式(Session)将用户的相应密钥分发至其它功能模块。此后标识管理模块采用周期性的检测机制，检查用户标识当前是否有效，如果无效，则强制退出。

3.2.2 改进的 CP-ABE 算法

用户在 CSSP 中进行注册时，在 IBE 体系中，完成身份标识管理，根据规则生成细粒度的属性集合，进行相应用户属性私钥(Attribute Private Key，APK)分发，DO 可以根据属性集合设定合适的访问控制策略。User 通过 CSSP 进行身份验证登录后，KMC 验证用户属性，KGC 根据用户属性集，计算生成用户的私钥(Private Key，Prik)，User 合并 $Prik$ 和 DO 分享的 APk 后解密共享的密文数据。

(1)初始化算法。初始化算法由 CSSP 和 KMC 完成。KMC 为数据共享模型中的属性密钥生成公开参数 $Prik$ 和主密钥 mk，CSSP 为共享模型生成对称参数 csk 和系统属性集合 A，为模型中的每个属性设置一个唯一标识 a_k，并且向 KMC 发送系统属性集合 A。

KMC：setup1$\rightarrow \{Prik, mk\}$，

CSSP：setup2$\rightarrow \{csk, A = \{a_1, a_2, a_3, \cdots, a_k, \cdots..\}\}$.

(2)属性密钥分发算法。属性密钥生成算法主要完成注册用户属性私钥的生成与分发。在执行过程中,首先由 CSSP 为注册用户分配属性集合,然后 KCA 根据用户所持有的属性集生成属性参数,最后用户使用属性参数计算得到最终的属性私钥。属性密钥的生成算法主要包括如下几个步骤。

①由 CSSP 为注册用户分配用户标识 ID = i,用户属性组 $A_i \in A$ 并为其分发对称参数 CSK。

CSSP:KeyGen1→ $\{i, A_i, CSK\}$

②在 KMC 中,可以设置 m 个 KAC,管理中心根据细化后的属性粒度情况,向其中 j 个 KAC 发起请求,并生成 j 个私钥参数,其中 $1 \leqslant j \leqslant m$。用户向 KAC 发送密钥授权请求,在请求信息中包含用户从 CSSP 中获取的用户标识和用户自身的属性集合 $\{i, A_i\}$。

③KAC 执行相应的生成算法产生属性私钥参数并将其返回给请求用户。

KACi:KeyGen2$(i, A_i) \rightarrow (SK_j^1, SK_j^2, SK_j^3)$

④注册用户 $User_i$ 接收到 j 个 KGC 的属性私钥参数集合后,执行 KeyGen3 算法,生成自己的属性私钥。

User: KeyGen3$(\{(SK_1^1, SK_1^2, SK_1^3), \cdots, (SK_j^1, SK_j^2, SK_j^3)\}) \rightarrow SK_i$

经过上述 4 个步骤后,注册用户取得了数据安全共享模型中的私钥属性 SK 以及对应的 CSK。

(3)加密算法。在共享模型中,加密通常由数据属主(DO)完成。加密过程分 2 个步骤,首先执行 Enc.Arch 算法,生成由属性和逻辑运算符组成的访问控制结构 τ,然后使用公共属性密钥 $Prik$ 和对称参数 CSK 执行 Enc.Crypt 算法对明文 M 执行加密运算,生成密文 CT。

DO:Enc.Arch→ (τ)

DO:Enc.Crypt $(PriK, M, CSK) \rightarrow CT$

(4)解密算法。在共享模型中,需要访问加密数据的用户,在合法获取云存储环境中的加密数据 CT,结合用户的私有属性密钥 SK_i 和 CSK,执行 Decrypt 解密算法,完成数据还原操作,得到明文 m。

$User_i$:Decrypt $(SK_i, CSK, CT) \rightarrow M$

(5)改进的密钥更新算法。在共享模型中,当某个用户注销或者撤销分享操作时,直接作废该用户的所有权限;撤销分享操作时,应保证该用户失去该属性相对应的权限,而具有该属性的其它用户仍保留此相应的权限。

属性撤销即撤销用户属性集合中的部分或者全部属性,被撤销某些属性的用户失去该属性对应的权限,不影响其它属性的权限,同时不影响其它仍然具备该属性的用户的访问权限。如果 DO 需要撤销某个 u_{uid} 的部分或全部属性时,不仅仅需要对 CSSP 中使用该属性的密文进行更新,而且还要对拥有该属性且未撤销的用户私钥进行更新。属性撤销的过程包含以下 4 个步骤:

(1)更新授权用户列表(Authorized user list, AUL)。由 DO 发起请求,向用户中心提出更新请求,将需要取消权限的用户 u_{uid} 从授权列表 AUL 中删除,即:$u_{uid} \notin AUL$。

(2)更新密钥版本号。由 DO 发起更新请求,当 CA 收到更新操作指令时,向属性密钥授权中心发送更新密钥版本的请求,请求信息中包含更新属性的唯一标识 a_k 和相应的版本信息 ver。属性密钥授权中心根据请求生成新版本的主密钥 mk_{ver+1} 与公开参数 $prik_{ver+1}$。

(3)更新密钥。利用更新的主密钥 mk_{ver+1} 与公开参数 $prik_{ver+1}$,DO 将被撤销用户时一并撤销的属性 $(a_k)_{ver}$ 进行更新,CA 重新生成新的 $(a_k)_{ver+1}$。未被撤销并拥有该属性的用户,可以通过广播的方式接收新的密钥,或者采用懒惰更新算法,有需要时访问 AUL,经过 AUL 后,更新。

(4)重加密。CSSP 中,根据原属性 a_k 和新生成的属性 $(a_k)_{ver+1}$ 将撤销前的密文执行解密后重新加密,生成新的密文 CT_{ver+1}。

3.3　安全性分析

安全性分析侧重于 2.1 节中所定义的系统安全需求。在 CP-AHI(BE)^{2}模型中,使用 HIBE 提高系统中用户的安全性验证,降低了系统中恶意用户通过分享密钥访问为授权的数据时带来的风险,提高系统的抗合谋攻击,改进的 CP-ABE 算法,实现了用户的细粒度访问控制,同时也解决了属性撤销等动态分享带来的风险,提高系统的前后向安全性。

(1)机密性。云存储环境下数据安全共享面临的数据机密性问题。主要包括以下 3 种情形:

①密钥的产生。通过 CSSP 与用户协商对称参数,因此 CSSP 可以通过还原用户的属性私钥解密数据。

②用户的属性私钥由 KMC 管理,因此 KMC 可以轻松获取用户的属性私钥,可以尝试还原用户与 CSSP 协商的对称参数,进而解密数据。

③由于云存储的分享特性,可以提供多重接入的方式,恶意用户可以通过伪装攻击等多种获取加

密后的数据,然后实施暴力破解等方式进行解密。

数据安全共享模型中,使用了对称和非对称 2 种方式对数据进行加密,假设密钥的长度为 len ,访问控制结构中所用的属性数量为 n, 对称加密算法的数量为 m。 则上述 3 种情形被暴力破解的次数如下:

①CSSP 持有对称参数,则 CSSP 需要破解的属性密钥的空间大小为:

$$\sum_{i=1}^{len} len \times 2^i \times C_{len}^n.$$

②KMC 管理用户的所有属性私钥,当所有关联的属性机构合谋解密时,则 KMC 需要破解的密钥空间大小为: $\sum_{i=1}^{len} m \times 2^i.$

③恶意用户尝试暴力破解,则需要同时破解对称参数和所有的属性私钥,其需要破解的密钥空间大小为: $\sum_{i=1}^{len} len \times m \times 2^i.$

因此,当 len、n 和 m 都达到一定长度时,CSSP、KMC 及恶意用户都无法通过暴力破解的方式还原共享数据。

(2)抗合谋攻击。在模型中,密钥生成算法中属性私钥由多个密钥授权中心共同生成,用户的 ID 与用户的属性捆绑在一起。在加密算法中数据属主(DO)生成的访问控制结构由多个属性组合成逻辑运算结构,因此方案可以避免来自用户合谋及 KAC 合谋 2 类攻击。

(3)前向安全性。当 DO 的某个属性在某个时间点从某个用户 Dreq 中撤销后,相应的属性 $(a_k)_{ver}$ 会被更新为 $(a_k)_{ver+1}$。 新的属性只有具备相应权限的用户才能访问,同时密文也被重新加密后更新,因此新生成的密文不会被旧的属性密钥解密,从而保证了前向安全性。

(4)后向安全性。当一个用户获得新的 $(a_k)_{ver+1}$ 后,相关的密文已经被更新,只能对新的密文 CT_{ver+1} 进行解密,而无法对旧的密文解密,从而保证了数据共享的后向安全性。

4 共享模型测试

4.1 测试环境

为验证上述的算法和共享模型,基于 3.1.2 节的模型图,采用 samkumar 的 HIBE 和 John Bethencourt 的 cpabe 工具集在 CentOS7.5 中实现一个验证模型,使用 1 台 DELL PowerEdge R720xd 服务器,安装 VMware ESXi6.0U3 软件构建虚拟化平台。实验环境及参数见表 3 和表 4。

使用虚拟机模板,创建多个虚拟机后,使用其中 5 个虚拟机搭建 5 层深度的层次化身份认证中心,使用 10 个虚拟机构建属性密钥管理中心,每台虚拟机独立处理单个属性。测试环境所使用的虚拟机,部署在一台物理服务器中,处于同一内网,测试中所使用的文件 size 较小,由 SSD 组成的磁盘阵列,可以提供较高的读写性能,可以忽略网络传输速率及 I/O 读写对模型的影响。

表 3 物理服务器参数

Tab. 3 Physical server parameters

选项	参数/型号	备注信息
服务器	DELL R720xd	--
CPU	E5-2680v2 * 2 颗	2.80GHz,10Core 支持超线程技术
内存	128G	--
硬盘	128G * 12 块	固态硬盘,组建 RAID-0 提高读写性能
磁盘整列卡	PERC H710P mini	1G 缓存

表 4 虚拟机模板

Tab. 4 Virtual machine template

选项	参数/名称
CPU	2 * vCPU Core
内存	8G
硬盘	60G

4.2 密钥生成

通过模拟不同数量的用户,在深度为 5 层的 HIBE 模块中进行处理,生成属性私钥。相应私钥信息通过 SSH 通道,导入到 cpabe 工具集中进行后续处理。执行过程中,编写相应脚本,使用“date +%s.%N”获取相应时间记录,累积密钥处理过程的时间,如图 6 所示。

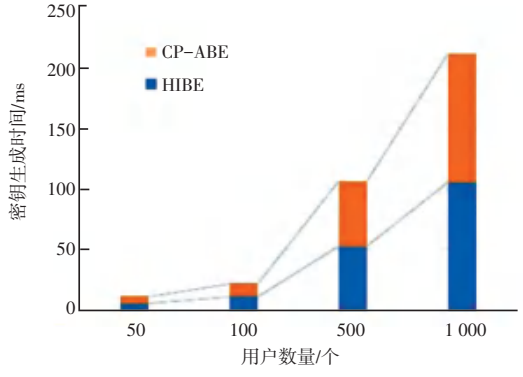

图 6 密钥生成时间

Fig. 6 Key generation time

4.3　加密与解密

生成属性密钥后，根据相应的参数和密钥执行加解密过程。由于在属性分解的数量及文件大小不同，所消耗的时间也不相同，详情如图 7 所示。

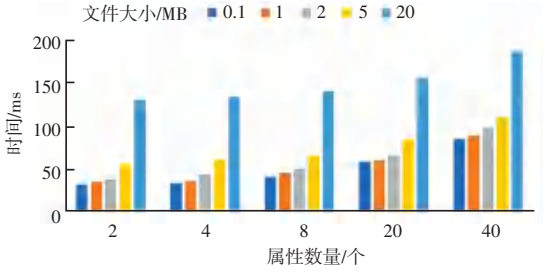

图 7　加解密处理时间

Fig. 7　Encryption and decryption processing time

4.4　密钥更新

在共享模型中，使用改进的密钥更新算法，当发生权限撤销或用户注销等操作时，系统所消耗的时间与云存储共享所关联的用户数量及属性数量相关，测试时用户数量与属性数量及时间消耗情况如图 8 所示。

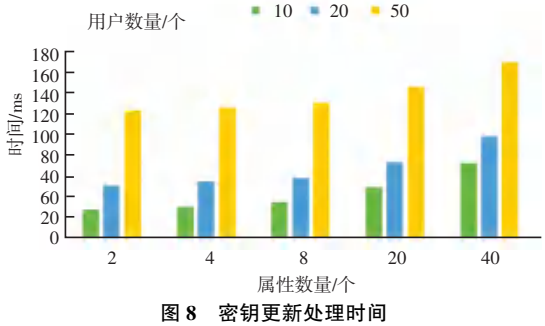

图 8　密钥更新处理时间

Fig. 8　Key update processing time

经过上述的测试，证明 CP-AHI(BE)^{2}模型，有较好的性能表现，该方案能够解决云存储中的信任依赖等问题。

5　结束语

目前，云计算因其成本低、可定制性高等特点，发展势态良好，具有广阔的发展前景，但安全性方面仍面临着严峻的挑战。本文针对云计算中的云存储服务，研究了 IBE、ABE 等算法，构建 CP-AHI(BE)^2 共享模型，针对属性密钥的生成问题，采用构建层次化的 HIBE 模块，针对属性撤销的问题，改进 CP-ABE方案，采用增加密钥版本号的方法，提高了密钥撤销的效率。通过测试，基于 CP-AHI(BE)^{2}的云存储共享模型，具有较好的性能表现，适合部署于云存储共享环境中。

参考文献

[1] Clutch. 企业数据存储偏爱云[EB/OL]. [2017-08-02]. http://cloud.yesky.com/407/285947907.shtml.

[2] 问卷星. 云存储相关使用情况及安全性调查[EB/OL]. https://www.wjx.cn/report/4010291.aspx.

[3] 孙会峰. 2018 网络安全产业发展报告[J]. 信息安全研究，2019,5(2):98-104.

[4] SHI Jiaoli, HUANG Chuanbe, WANG Jing, et al. An access control scheme with direct cloud-aided attribute revocation using version key SUN X H, et al. ICA3PP 2014, Part I, LNCS 8630. SwitzerLand: Springer International Publishing, 2014:429-442.

[5] LIANG Xiaohui, LU Rongxin, LIN Xiaodong, et al. Ciphertext policy attribute based encryption with efficient revocation[R]. Ontario, Canada: University of Waterloo, 2011.

[6] CHEN Genlang, XU Zhiqian, JIANG Hai, et al. Generic user revocation systems for attribute-based encryption in cloud storage [J]. Frontiers of Information Technology & Electronic Engineering, 2018,19(11):1362-1384.

[7] 王鹏翩，冯登国，张立武. 一种支持完全细粒度属性撤销的 CP-ABE 方案[J]. 软件学报，2012,23(10):2805-2816.

[8] 工业和信息化部. 云计算综合标准化体系建设指南[EB/OL]. [2015-11-09]. http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757022/c4414407/content.html.

[9] 傅颖勋，罗圣美，舒继武. 一种云存储环境下的安全网盘系统[J]. 软件学报，2014,25(8):1831-1843.

[10] 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.

[11] 胡亮，初剑峰，林海群，等. IBE 体系的密钥管理机制[J]. 计算机学报，2009,32(3):543-551.

[12] BONEH D, BOYEN X, GOH E J. Hierarchical identity based encryption with constant size ciphertext[M]. CRAMER R. Advances incryptology—Eurocrypt 2005. Lecture notes in Computer Science. Berlin/Heidelberg: Springer, 2005, 3494: 440-456.

[13] 梁潘，冯朝胜. 基于 HIBE 的电子政务系统安全解决方案[J]. 计算机工程与设计，2011,32(3):842-845.

[14] 唐鑫，齐芳. 免密钥托管的基于身份的分层加密机制研究[J]. 计算机工程与科学，2017,39(5):870-876.

[15] 杨海滨. 一种新的格上基于身份的分层加密方案[J]. 武汉大学学报(理学版)，2016,62(2):155-160.

[16] 计海萍，徐磊，蔚晓玲，等. 云计算环境下基于身份的分层加密管理系统研究[J]. 信息网络安全，2016(5):30-36.

[17] 冯登国，陈成. 属性密码学研究[J]. 密码学报，2014,1(1):1-12.

[18] 熊安萍，许春香，冯浩. 云存储环境下支持策略变更的 CP-ABE 方案[J]. 计算机科学，2016,43(1):191-194.

(上接第 239 页)

[10] KABISCH N, SELSAM P, KIRSTEN T, et al. A multi-sensor and multi-temporal remote sensing approach to detect land cover change dynamics in heterogeneous urban landscapes [J]. Ecological Indicators, 2019, 99(10): 273-282.

[11] 孙成功，肖本贤. 电动叉车稳定性控制系统传感器故障重构[J]. 电子测量与仪器学报，2019,33(1):120-127.