基于CP-ABE的多云存储系统中访问控制模型的研究

印凯泽 汪海航
(同济大学电子与信息工程学院 上海 201804)

摘 要 针对将单个云内基于密文策略属性基加密(CP-ABE)的访问控制机制应用到多云存储系统中时遇到的策略冲突问题,设计了一个属性映射机制,通过扩展CP-ABE机制,提出了一个适用于多云存储系统的访问控制模型。这里的映射机制主要针对CP-ABE的树形访问结构以及其支持的属性值类型。最后,详细描述了该模型的框架及工作流程,通过构建一个简单的原型系统验证了该模型的有效性,同时对该原型系统进行了性能分析。该模型的提出对于多云存储系统的访问控制研究具有理论价值和实际意义。

关键词 密文策略属性基加密,访问控制,策略冲突,属性映射,多云存储系统
中图法分类号 TP311.5 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.9.032

Research on Access Control Model in Multi-clouds Storage System Based on CP-ABE

YIN Kai-ze WANG Hai-hang
(College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China)

Abstract Applying the access control system based on ciphertext-policy attributes-based encryption (CP-ABE) in single cloud to multi-clouds storage system will encounter a problem of policy conflict. Thus, an attributes mapping scheme was designed and an access control model in multi-clouds storage system based on CP-ABE was provided. The attributes mapping scheme was designed based on the access construction tree of CP-ABE and the types of attributes' value that is supported. At last, the framework of this model and its workflow were elaborated. The effectiveness of the model is verified by building a simple prototype system, and the performance of the prototype system is analyzed. The proposed model has theoretical value and actual meaning for the research of access control in multi-clouds storage system.

Keywords Ciphertext-policy attribute-based encryption, Access control, Policy conflict, Attributes mapping, Multi-clouds storage system

1 引言

云存储作为云计算概念的延伸,是一种新的服务模式,即数据存储即服务(Data Storage as a Service, DaaS)[1]。云存储最广泛的应用就是文件的存储和共享。目前,提供存储和共享服务的云存储服务提供商(Cloud Storage Service Providers, CSSPs)和应用也越来越多,国际上比较知名的有Amazon S3, Google Docs, Microsoft Windows Azure等,国内也有金山快盘、百度云盘、腾讯微云等。随着云存储不断地发展,其安全问题也越来越受到重视。在云存储环境中,用户将数据存放在云端,也就失去了对数据的控制。为了消除用户对云存储数据安全的担忧,需要有相应的安全机制来保证数据的机密性和安全共享。

目前,有很多学者提出了适用于云存储环境的基于密文策略的属性基加密(Ciphertext-Policy Attributes-Based Encryption, CP-ABE)[2]的访问控制方案。在基于CP-ABE的访问控制方案中,由数据拥有者(Data Owner, DO)对数据进行加密,其中访问控制策略由访问结构树(Access Construction Tree, $A_{C\text{-}T}$)表示,DO可以制定相应的$A_{C\text{-}T}$来执行访问控制,只有当数据使用者(Data User, DU)相应的属性满足$A_{C\text{-}T}$时,其才可以解密到共享的数据。CP-ABE机制由DU负责制定访问控制策略,因此被认为是最适合用于访问控制类应用的技术。

随着云存储的不断发展和用户需求的不断变化升级,又出现了一种新的云存储模式——多云协作的存储系统,简称为多云存储系统(Multi-Clouds Storage System, MCSS)。在MCSS环境中,不同云内的用户可以相互跨云访问对方的数据,随之产生了一些类似文献[3,4]的应用和研究,它们通过一个集中的平台或者接口来管理MCSS中的数据。这些应用只是简单地共享了多个云存储服务中的数据,却没有对这些文件实现必要的访问控制,因此还是需要类似CP-ABE的技术来保证数据的机密性和安全共享。如果将基于CP-ABE的访问控制方案直接应用于MCSS环境,会遇到一个新的问题:由于每个云可能有不同的访问控制策略,用户在跨云访问时可能引起策略冲突。因此需要一个全局的访问控制机制来进行策略冲突的检测和合成,以保证MCSS环境中的访问控

到稿日期:2015-12-27 返修日期:2016-03-13
印凯泽(1989—),男,博士生,CCF学生会员,主要研究方向为云计算、访问控制,E-mail:cogito_yin@163.com;汪海航(1965—),男,博士,教授,主要研究方向为信息安全、网络与分布式计算。

制。在这里，策略的冲突主要由属性的语义引起，即语义冲突。例如，在基于 CP-ABE 的访问控制方案中，A 云中用户 UA 制定的 $A_{C\text{-}T}$ 要求访问者性别为男性（AT：*sex*＝male），当 B 云中用户 UB（拥有属性 *gender*＝man）想要访问 A 云中 UA 的数据时，就会引起语义冲突，导致 UB 无法访问 UA 的数据。

针对这个问题，本文将提出一个适用于 MCSS 环境的基于 CP-ABE 的访问控制模型。通过属性映射的方法，解决不同云中用户属性语义不同引起的策略冲突，建立相应的属性映射机制，保证基于 CP-ABE 的 MCSS 环境中访问控制策略的一致性。本文第 2 节介绍 CP-ABE 机制和云存储系统中基于 CP-ABE 的访问控制方案；第 3 节和第 4 节分别介绍属性映射机制的设计和模型；第 5 节给出实验验证和性能分析结果；最后总结全文并提出下一步的工作和未来研究的方向。

2 相关工作

2.1 CP-ABE 机制

Bethencourt 等人[2]提出了 CP-ABE 机制，同时给出了一个具体的实现[5]。其工作流程如图 1 所示。

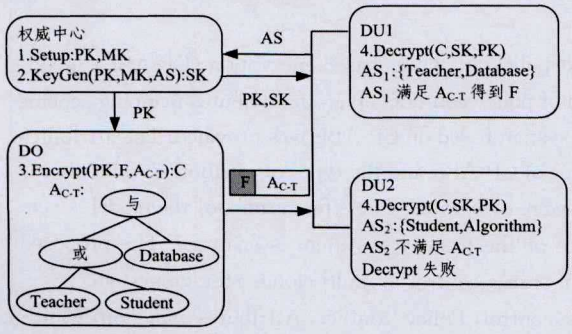

图 1 CP-ABE 机制

CP-ABE 算法主要包括如下 4 个步骤。

1）Setup：产生一个主密钥（*Master Key*，*MK*）和公开密钥（*Public Key*，*PK*）；

2）$C=Encrypt(PK,F,A_{C\text{-}T})$：将文件（*File*，*F*）用 *PK* 和 $A_{C\text{-}T}$ 加密得到密文（*Ciphertext*，*C*）；

3）$SK=KeyGen(PK,MK,S)$：输入 *PK*，*MK* 和属性集（*Attributes Set*，*AS*），输出一个私有密钥（*Secret Key*，*SK*）；

4）$Decrypt(C,SK,PK)$：只要 *SK* 中包含的 *AS* 满足 $A_{C\text{-}T}$，就可以通过 *SK* 解密 *C* 得到 *F*，反之则不行。

Bethencourt 等人[2]提出的 CP-ABE 机制采用树结构来表示访问控制策略。树中每一个非叶子节点表示一个阈值门，由它的子节点和阈值描述。假设一个节点 x 的子节点数为 num_x，阈值为 k_x，那么 $0<k_x<num_x$。当 $k_x=1$ 时，阈值门就是一个或门；当 $k_x=num_x$ 时，阈值门就是一个与门。每个叶子节点由一个属性和一个 $k_x=1$ 的阈值表示。同时该结构树还支持属性值与整数的比较操作。例如需要比较一个属性是否等于某个整数值“$a=k$”，k 是一个 n 位的整数，构建一棵包含与门和或门的子树，生成 n 个叶子节点代表 k 的每一个位。假设 k 是一个 4 位的整数 9，那么首先生成 4 个叶子节点：“a：1＊＊＊”，“a：＊0＊＊”，“a：＊＊0＊”，“a：＊＊＊1”。然后就可以采用与门和或门来实现这个整数的比较，如图 2 所示。其他比较操作符的实现也都类似，例如≤、≥、<和>都可以在最多 n 门内实现。

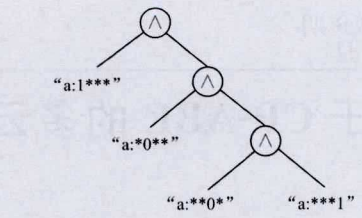

图 2 实现属性与整数的比较“$a=9$”

2.2 云存储中基于 CP-ABE 的访问控制研究

目前，已经有很多学者提出了基于 CP-ABE 的云存储访问控制模型及应用，这里将给出这些模型的一般框架示意图，如图 3 所示。在这个框架中，主要有 DO，DU 和 CSSP 3 个实体。这些框架主要扩展了基本的 CP-ABE 机制，不是直接将 CP-ABE 用于加密存储数据，而是选取另外一个密钥 k 用于加密存储数据，然后再用 CP-ABE 算法加密这个密钥 k，如图 3 步骤 3 所示。DO 负责 CP-ABE 算法中的前 3 个步骤，并且制定 $A_{C\text{-}T}$，将加密得到的 C 和 $E_{A_{C\text{-}T}}(k)$ 发送到云端存储。如果 DU 的 *AS* 满足 $A_{C\text{-}T}$，则可以解密得到 k，最后再解密得到 F，反之则不然。

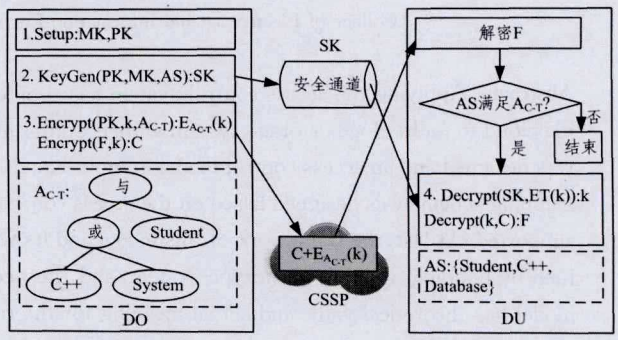

图 3 基于 CP-ABE 的云存储访问控制框架

Wang 等人[6]和 Wan 等人[7]都提出了一个基于分层的身份基加密（Hierarchical Identity-based Encryption，HIBE）和 CP-ABE 的具有细粒度访问控制的云存储系统。Li 等人[8]和 Barua 等人[9]将 CP-ABE 应用于基于云的电子健康系统中，以保证电子档案安全的存储。我们之前的研究[10]也提出了一个基于 CP-ABE 的具有细粒度访问控制和低存储空间开销的云存储系统，该系统不仅能够降低用户的计算量，还可以减轻 CSSPs 的存储负担。

3 属性映射机制

3.1 属性映射

根据第 1 节中的分析，在 MCSS 环境中应用基于 CP-ABE 的方案引起的策略冲突主要来自于属性的语义冲突。因此，需要相应的属性映射机制对其进行消除。这里为了简化系统，语义的冲突检测先简单地转化为判断两个字符串是否相等。一个属性包括属性名和属性值，因此这里的映射包括属性名的映射和属性值的映射。其中对于属性名的映射，已经有很多基于本体的方法[11,12]被提出来用于建立映射关系，因此本文将不再进行赘述，而是将研究的重点放在属性值的映射上。

根据 2.1 节中对访问结构树的分析，可以得出该类型的访问结构树支持的属性值的类型和取值范围，如表 1 所列。可取的属性值类型包括字符型、日期型和整数型。其中字符型的映射依旧可以采用属性名映射的方法；日期型的属性值

可以转换成整数型再进行映射，例如 2015-11-11 根据距离 1970-01-01 的天数转换成 16750；对于整数型属性值的映射，如果要将云 A 的某个属性值 k_A 映射成云 B 中属性值 k_B，则一共有 $[(-\infty,+\infty),(-\infty,k_A)$ 或 $(k_A,+\infty),(k_{\min A},k_{\max A})]\times[(-\infty,+\infty),(-\infty,k_B)$ 或 $(k_B,+\infty),(k_{\min B},k_{\max B})]=9$ 种情况，然而在有 ∞ 存在的情况下，k_A 都可以直接映射到 k_B。由于这种情况下不存在区间范围的冲突，因此只需要考虑 $(k_{\min A},k_{\max A})\times(k_{\min B},k_{\max B})$ 的情况。在这种情况下，根据区间范围的不同可以得出映射的公式如式(1)所示。例如在云 A 中属性安全等级在访问策略规定下的取值范围为[1,5]，而在云 B 中属性安全等级的取值范围为[1,9]，那么云 A 中安全等级属性值 3 就可以映射成云 B 中的安全等级属性值 5。

$$k_B=\frac{(k_{\max B}-k_{\min B})\times(k_A-k_{\min A})}{k_{\max A}-k_{\min A}}+k_{\min B} \tag{1}$$

表 1　属性值支持的类型和可取值范围

类型	可取值范围
字符型	—
日期型	—
整数型	①$(-\infty,+\infty)$ ②$(-\infty,k)$或$(k,+\infty)$ ③$(k_{\min},k_{\max})$

3.2　属性关系证书库

如果每次发生策略冲突时都要进行一次属性映射，那么系统的性能就会大大下降。因此，可以将每次属性映射的结果缓存起来，当发生冲突时只须查询缓存，如果缓存中已有映射结果，则直接返回结果；反之，再进行属性映射操作。于是，需要建立一个属性关系证书库(Attribute Relationship Certificate Database，ARCD)来存储属性映射的结果。其中属性关系证书(Attribute Relationship Certificate，ARC)由一个 5 元组表示，如式(2)所示。其中可选的属性值指字符型的属性值，类型表示是针对属性名还是属性值的查询(0 表示属性名，1 表示属性值)；关系用布尔值表示，真即为两个属性相同，假即为不同。ARCD 的职责不仅包括属性映射，还要负责维护 ARC 的创建、更新以及根据其中的过期时间周期性地删除过期的 ARC，同时还要负责响应 CSSP 的查询请求。

〈云标识符：[属性名，属性值]，云标识符：[属性名，属性值]，类型，关系，创建时间，[过期时间]〉　(2)

图 4 示出了一些 ARC 的例子。

〈A：manager，B：supervisor，0，True，2014-11-11〉

〈B：sex，C：gender，0，True，2015-10-10〉

〈A：PHD，C：doctor，1，False，2015-11-11，[2016-02-29]〉

图 4　ARC 的一些例子

由此可以给出相应的属性映射机制的算法(Attribute Mapping Algorithm，AMA)，如图 5 所示。

1. 输入：云 A 的属性和云 B 的属性
2. 查询 ARCD，如果命中，返回查询结果，否则转到步骤 4
3. 根据查询结果分别执行以下子步骤：
   3.1 结果为真且类型为 0：根据属性值类型分别执行以下步骤：
      3.1.1 字符型：转到步骤 2
      3.1.2 日期型：转化成整数型，转到步骤 3.1.3
      3.1.3 整数型：根据不同访问策略规定的取值范围进行属性值映射，转到步骤 6
   3.2 结果为真且类型为 1：转到步骤 6
   3.3 结果为假，转到步骤 7
4. 执行基于本体的属性映射方法
5. 映射结果为真则转到步骤 6，为假则转到步骤 7，同时创建 ARC
6. 返回成功及映射结果
7. 返回失败

图 5　属性映射机制算法 AMA

4　访问控制模型

根据第 3 节设计的属性映射机制，将其整合进 MCSS 环境中基于 CP-ABE 的访问控制模型，如图 6 所示。

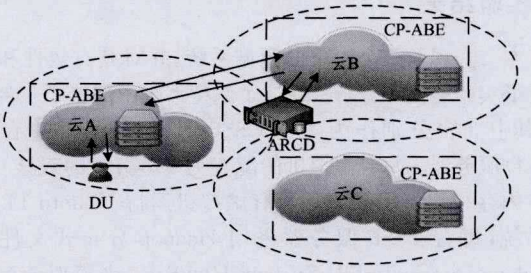

图 6　MCSS 环境中基于 CP-ABE 的访问控制模型

每个云内部分别实施基于 CP-ABE 的访问控制机制，并且其可以拥有不同的访问控制策略。具体的工作流程如图 7 所示。

1)云 A 中的用户 DU 向云 A 的 CSSP 提出访问云 B 中资源的请求；

2)云 A 的 CSSP 转发带有 DU 属性的访问请求给云 B 的 CSSP；

3)云 B 的 CSSP 在执行 CP-ABE 算法的过程中判断是否有语义的冲突，如果没有则转到步骤 4，否则转到步骤 5；

4)返回访问控制执行结果给云 A 的 CSSP；

5)向 ARCD 发起属性映射机制请求；

6)ARCD 执行 AMA 算法；

7)ARCD 返回执行结果；

8)云 B 根据 ARCD 返回的结果判断冲突是否已经消除；

9)如果是则继续执行 CP-ABE 算法，返回执行结果，否则返回失败信息给云 A 的 CSSP；

10)云 A 的 CSSP 将最终的结果返回给用户 DU。

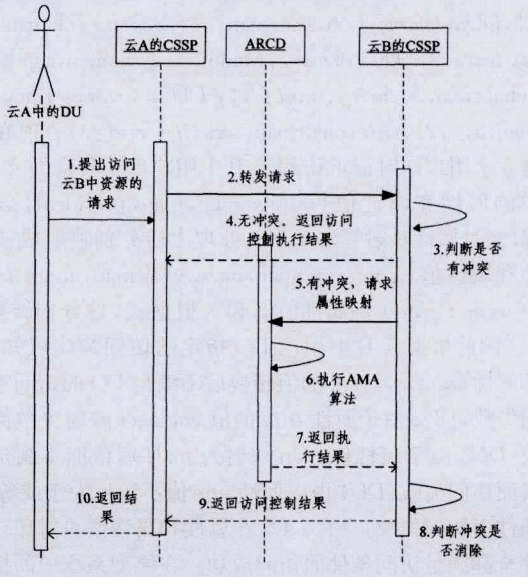

图 7　模型的工作流程

与文献[6-10]提出的基于 CP-ABE 的云存储访问控制模

型相比，该模型通过建立基于本体的属性映射机制，解决了MCSS环境中因不同CSSP存在不同的访问控制策略而引起策略冲突的问题，使其能够更好地满足新的多云协作的存储环境中对访问控制的需求。

同时，引入了属性关系证书库的概念来缓存本体映射结果，使得属性映射的请求可以由查询缓存来实现而不需要每次都进行复杂的本体映射算法。从理论上可以明显地看出该方法可以有效地提升系统的性能，第5节将通过实验测试作进一步的性能分析。

5 实验结果

本文实现了一个简单的原型系统，并对其有效性和性能进行了实验验证和分析。在这个原型系统中部署了4台虚拟机，其中3台分别作为3个CSSP服务器，另外1台作为ARCD服务器。每台虚拟机的配置为2.8GHz的双核CPU，4GB内存和500GB硬盘。所有虚拟机运行Ubuntu 14.04操作系统，每台CSSP服务器采用Hadoop分布式文件系统(Hadoop Distribute File System，HDFS)[13]来模拟云存储环境作为底层的文件存储系统，其中访问控制模块采用CP-ABE工具包[5]实现，属性名的映射采用基于CODI[14]本体映射的方法。ARCD服务器采用MySQL数据库存储ARC。云内的用户信息采用企业领域本体(Enterprise Ontology，EO)[15]中的组织部分表示。为了模拟属性冲突，修改各个云内部分属性的定义，使其能够产生语义的冲突。修改后云A中安全策略规定属性 *sex* 的取值为{man，women}，属性 *title* 的取值为{staff，manager，engineer，president}，属性 *security level* 的取值范围为[1，4]。云B中的用户DO为其共享大小为10MB的文件制定了访问策略：{*age*>=20，*gender*=female，*title*=chairman，*access level*>5}，其中安全策略规定属性 *gender* 的取值为{male，female}，属性 *title* 的取值为{staff，manager，chairman}，*access level* 的取值范围为[1，10]。根据云B中DO制定的访问策略，为了验证访问策略中的每一项条件，在云A中设计了5个用户 *DU*1，*DU*2，*DU*3，*DU*4 和 *DU*5，这4个用户的身份信息分别为：*DU*1：{*name*：Lily，*sex*：women，*age*：20，*title*：president，*security level*：2}，*DU*2：{*name*：Jane，*sex*：women，*age*：21，*title*：engineer，*security level*：3}，*DU*3：{*name*：Bob，*sex*：man，*age*：22，*title*：chairman，*security level*：3}，*DU*4：{*name*：Mandy，*sex*：women，*age*：19，*title*：chairman，*security level*：3}，*DU*5：{*name*：Lucy，*sex*：women，*age*：21，*title*：chairman，*security level*：3}。现在云A中这5个用户同时请求访问云B中用户DO共享的文件，云A中的属性和属性值{*sex*，women，man，president，*security level*}经过属性映射算法AMA处理之后分别映射成云B中属性和属性值{*gender*，female，male，chairman，*access level*}，其中 *security level* 的属性值2和3根据式(1)分别转换成4和7。因此根据云B中用户DO指定的访问策略可知，*DU*1由于属性 *security level* 的值转换后不满足DO的访问策略而访问失败，*DU*2 由于属性 *title* 的值 engineer 映射失败而访问失败，*DU*3 由于属性值 man 映射为 male 后依旧不满足访问策略而访问失败，*DU*4 由于属性 *age* 值不满足大于或等于20的条件而访问失败，只有 *DU*5 在属性和属性值映射和转化后能够全部满足访问条件而访问成功。在原型系统中的执行访问之后，实验的结果如表2所列，可知实验访问的结果和预期结果是一致的，证明了该模型是可行的。

表2 跨云访问预期结果和实验结果对比

用户	预期结果	实验结果
DU1	失败	失败
DU2	失败	失败
DU3	失败	失败
DU4	失败	失败
DU5	成功	成功

最后，对该原型系统的性能进行了实验分析。在云A中随机生成50个用户，每次随机选择10个用户同时跨云访问云B中DO共享的文件，一共进行10次访问，每次访问系统的响应时间变化如图8所示。从图8中可知，第一次跨云访问的延迟要比后面几次高出很多，而在第三次以后系统的延迟较低且趋于稳定，由于访问成功用户数量不同，经过CP-ABE算法解密文件的时间不同，导致每次响应的结果稍有不同。这是因为第一次进行跨云访问时，系统性能主要消耗在属性和属性值的本体映射和ARC插入ARCD中，在第一次映射结束之后结果就会存入ARCD中，在后续的访问中遇到属性冲突时只需要查询ARCD缓存而不需要再次执行本体映射的操作。由此可知，通过引入ARC和ARCD概念可以有效提升系统的性能。

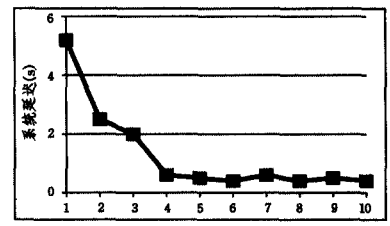

图8 多次跨云访问系统响应时间变化

结束语 云存储已经从单个云朝着多云协作的方向发展，同时也对其数据安全的保障提出了新的挑战。当将单个云内基于CP-ABE的访问控制方案应用于新的MCSS环境中时，各个云内可能采用不同的访问控制策略，从而引起访问策略的冲突。在这里，主要是由于用户属性的语义冲突引起的。针对这个问题，本文设计了一个属性映射机制，通过AMA算法来解决属性语义冲突，通过扩展CP-ABE机制，提出了一个适用于MCSS环境的访问控制模型。该模型为MCSS环境的访问控制研究提出了一个方向，对于促进云存储安全的健康发展具有理论价值和实际意义。

接下来将继续完善该模型的原型系统。同时还需要针对不同CP-ABE的访问结构设计不同的映射机制以满足实际的需求，同时支持更多类型的属性值映射。最后还需要增加对用户属性信息的隐私保护机制等，为创造一个安全的云存储环境而努力。

参 考 文 献

[1] SNIA Technical Position. Cloud data management interface (cdmi) v1.0.2 [EB/OL]. [2015-11-13]. http://snia.org/sites/default/files/CDMI%20v1.0.2.pdf

[2] Sahai B J A，Waters B. Ciphertext-policy attribute-based encryption [C]// Proceedings of the 28th IEEE Symposium on Security and Privacy. Piscataway：IEEE，2007：321-334

[3] Cloudfuze [EB/OL]. [2015-11-13]. http://www.cloudfuze.com

[4] Livenson I，Erwin L. Towards transparent integration of heterogeneous cloud storage platforms [C]// Proceedings of the 4th International Workshop on Data-intensive Distributed Computing. New York：ACM，2011：27-34

(下转第179页)

行数据交互，在 $Client_X$ 处记录从发出 TCP SYN 数据包到收到 TCP SYN 确认数据包的时间，然后停止 CAKCA Daemon，记录同样的时间作为对比。重复实验 10 次，结果如图 9 所示。

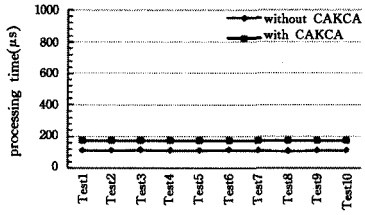

图 9　CAKCA 数据包处理时延的测试结果

由结果可知，CAKCA 的部署使得网关处的数据包处理时延有一定的增加，但增幅较小，也就是说攻击者无法通过比对数据包处理时延来确定 CAKCA 的部署。

结束语　网络用户身份认证是网络安全的核心问题之一。随着网络攻击技术的不断多样化、复杂化，阻止未授权用户对关键主机的访问是尽量保证网络安全的有效手段。本文提出一种协同地址碰撞技术，基于 IPv6 地址的新特性，结合秘密分享方法，通过多个节点的协同碰撞，实现对用户身份的隐蔽认证。本文的研究成果有望为基于 IPv6 新特性提出云计算环境下网络安全防护新技术提供一些思路。

参 考 文 献

[1] Yu Neng-hai, Hao Zhuo, Xu Jia-jia, et al. Review of Cloud Computing Security[J]. Acta Electronica Sinica, 2013, 41(2): 371-381(in Chinese)
俞能海，郝卓，徐甲甲，等. 云安全研究进展综述[J]. 电子学报，2013，41(2)：371-381

[2] Reeja S L. Role Based Access Control mechanism in cloud computing using cooperative secondary antuorization recucling methd[J]. International Journal of Emerging Technology and Advanced Engineering, 2012, 2(10): 444-450

[3] Rodas O, Morales G, Alvarez J. A reliable and scalable classification-based hybrid IPS[C]// IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA). Gwangiu: IEEE, 2015: 599-604

[4] Barham P, Hand S, Isaacs R, et al. Techniques for lightweight concealment and authentication in IP networks: Technical Report IRB-TR-02-009[R]. Berkeley: Intel Research, 2002

[5] Ali F H M, Yunos R, Alias M A M. Simple port knocking method: against TCP replay attack and port scanning[C]// International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). Kuala Lumpur: IEEE, 2012: 247-252

[6] Mehran P, Reza E A, Laleh B. SPKT: Secure port knock-tunneling, an enhanced port security authentication mechanism[C]// IEEE Symposium on Computers & Informatics (ISCI). Malaysia: IEEE, 2012: 145-149

[7] Srivastava V, Keshri A K, Roy A D, et al. Advanced port knocking authentication scheme with QRC using AES[C]// Proceeding of Trends in Networks and Communications. Chennai: Springer, 2011: 159-163

[8] Sahu P, Singh M, Kulhare D. Implementation of modified hybrid port knocking (MHPK) with strong authentication[J]. Journal of Commerce and Management Thought, 2013, 4(2): 490-504

[9] Hadi A H, Al-Bahadili H. A Hybrid Port-knocking technique for host authentication[M]// Simulation in Computer Network Design and Modeling: Use and Analysis. 2012: 336

[10] Liew J H, Lee S, Ong I, et al. One-time knocking framework using SPA and IPsec[C]// Proceeding of 2nd International Conference on Education Technology and Computer. 2010: v5-209-v5-213

[11] Singh K, Zhong J, Mirchandani V, et al. Securing data privacy on mobile devices in emergency health situations[M]// Security and Privacy in Mobile Information and Communication Systems. Springer Berlin Heidelberg, 2012: 119-130

[12] Dunlop M, Groat S, Urbanski W, et al. MT6D: a moving target IPv6 defense[C]// Proceeding of the 2011 Military Communication Conference-Track3-Cyber Security and Network Operations. Baltimore, MD: IEEE, 2011: 1321-1326

(上接第 168 页)

[5] Bethencourt J, Sahai A, Waters B. The cpabe toolkit [EB/OL]. [2015-11-13]. http://acsc.csl.sri.com/cpabe

[6] Wang G, Liu Q, Wu J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services [C]// Proceedings of the 17th ACM Conference on Computer and Communications Security. Chicago: ACM, 2010: 735-737

[7] Wan Z, Liu J E, Deng R H. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing [J]. Information Forensics and Security, 2012, 7(2): 743-754

[8] Li M, Yu S, Ren K, et al. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings [M]// Security and Privacy in Communication Networks. Berlin: Springer, 2010: 89-106

[9] Barua M, Liang X, Lu R, et al. ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing [J]. International Journal of Security and Networks, 2011, 6(2/3): 67-76

[10] Yin K Z, Wang H H. A cloud storage system with fine-grained access control and low storage space overhead [J]. Journal of Computer Applications, 2015, 35(12): 3413-3418(in Chinese)
印凯泽，汪海航. 具有细粒度访问控制和低存储空间开销的云存储系统[J]. 计算机应用，2015，35(12)：3413-3418

[11] Doan A H, Madhavan J, Domingos P, et al. Learning to map between ontologies on the semantic web [C]// Proceedings of the 11th International Conference on World Wide Web. Honolulu: ACM, 2002: 662-673

[12] Wiederhold G. An algebra for ontology composition [C]// Proceedings of 1994 Monterey Workshop on Formal Methods. Monterey, 1994, 56: 61

[13] Borthakur D. The hadoop distributed file system: architecture and design [EB/OL]. [2015-12-15]. http://hadoop.apache.org/docs/r1.2.1/hdfs_design.html

[14] Noessner J, Niepert M. CODI: Combinatorial Optimization for Data Integration-Results for OAEI 2010 [C]// Proceedings of the 5th International Workshop on Ontology Matching. Shanghai, 2010: 142-149

[15] Enterprise Ontology [EB/OL]. [2016-04-25]. http://www.aiai.ed.ac.uk/project/enterprise/enterprise/ontology.html