基于CP-ABE和XACML多权限安全云存储访问控制方案

刘晓建 王力生 廖新考
(同济大学电子与信息工程学院 上海 201804)

摘 要 为了保护云存储系统中用户数据的机密性和用户隐私,提出了一种基于属性加密结合XACML框架的多权限安全云存储访问控制方案。通过CP-ABE加密来保证用户数据的机密性,通过XACML框架实现基于属性细粒度访问控制。云存储系统中的用户数据通过对称加密机制进行加密,对称密钥采用CP-ABE加密。仿真实验表明,该方案是高效灵活并且安全的。安全性分析表明,该方案能够抵抗共谋攻击,具有数据机密性以及后向前向保密性。

关键词 云存储,访问控制,密文策略属性加密,XACML

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.3.024

Multiple Permissions Secure Access Control Scheme Combining CP-ABE and XACML in Cloud Storage

LIU Xiao-jian WANG Li-sheng LIAO Xin-kao
(College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China)

Abstract In order to protect the confidentiality of user data and user privacy in cloud storage system, multiple permissions secure access control scheme combining ciphertext-policy attribute-based encryption(CP-ABE) and XACML was proposed. The confidentiality of user data is ensured by CP-ABE encryption and properties of fine-grained access control are implemented by XACML framework. In cloud storage system user data is encrypted by symmetric encryption mechanism, and symmetric key encryption uses the CP-ABE. Simulation results show that the model is efficient, flexible, and secure. Security analysis shows that the scheme can resist collusion attacks, has data confidentiality and backward forward confidentiality.

Keywords Cloud storage, Access control, Ciphertext-policy attribute-based encryption, XACML

1 引言

云存储是一种从云计算衍生和发展起来的数据外包存储服务技术,能够使用户远程存储并按需随时随地访问云存储中的数据。云存储依靠其成本低、易于使用的接口和高扩展性的商业优势得到了业内的广泛关注。然而,云用户在享受云存储带来多种便利的同时,也面临着数据脱离自身控制域而担心数据的安全和隐私问题[1]。Google、Docs、The Linkup等多家著名云服务提供商曾多次出现过各种安全问题,导致了严重的后果[2],安全隐患已成为云存储大规模发展亟需解决的关键问题。

访问控制是实现用户数据机密性和进行隐私保护的主要工具之一,然而云存储的外包存储服务模式导致特权用户的存在,其具有非授权访问用户数据的权利,导致用户数据信息和隐私泄露等内部攻击问题。针对上述安全问题,引入基于模糊身份加密的ABE(Attribute-based Encryption)加密访问控制技术。

基于属性的加密技术一般分为密钥策略属性基加密(Key-policy Attribute-based Encryption, KP-ABE)和密文策略属性基加密(Ciphertext-policy Attribute-based Encryption, CP-ABE)。Goyal等人[3]将用户私钥关联到访问控制结构树,密文关联到属性集,若用户的属性集满足访问控制树,则该用户可以解密数据,否则,该用户无法解密数据。Bethencourt等人[4]将用户私钥关联到属性集,密文关联到访问控制树,属性集满足该访问控制树的用户具有解密数据的能力。KP-ABE方案中的加密者不能直接控制哪些用户能访问密文数据,而CP-ABE方案中的用户可以直接决定哪些用户能够访问密文数据,显然CP-ABE方案更适用于云存储服务。

基于CP-ABE的云存储访问控制方案也存在一定的不足,即面临单一信任授权机构、属性和用户撤销等困难问题。

文献[5]为云用户的私钥嵌入失效时间属性,失效时间到期,用户将不能访问密文。这种周期性访问控制方法要求所有用户周期性更新私钥,从而导致整个云系统效率低下。

王鹏翩等人[6]提出基于CP-ABE直接撤销模式下支持完全细粒度属性的撤销方案,而该撤销方案利用用户撤销列表实现细粒度属性的撤销。

文献[7]在个人健康记录云计算环境中划分公共领域和私人领域,根据两种领域不同的属性特质,采用不同的密钥管理和分配方式。比如私人领域为数据属主的亲人、朋友等,公共领域为各个医生、护士和保险公司的工作人员等。

到稿日期:2015-09-16 返修日期:2015-12-24 本文受国家高技术研究发展计划(863项目)(2013AA040302)资助。

刘晓建(1982-),男,博士生,主要研究方向为云计算、访问控制,E-mail:liuxiaojian1982@qq.com;王力生(1954-),男,教授,主要研究方向为云计算、访问控制、嵌入式系统、并行计算等;廖新考(1986-),男,博士生,主要研究方向为云计算、信任计算等。

针对上述问题，本文提出一种基于 CP-ABE 与 XACML 相结合的安全云存储访问控制方案。该方案采用 CP-ABE 加密机制保护云存储用户数据的机密性，通过 XACML 框架实现高效、细粒度、动态和可扩展的访问控制，并实现高效的用户撤销。

2 预备知识

2.1 密文策略属性基加密(CP-ABE)

1. 双线性对

双线性对是 ABE 加密方案设计中非常关键的工具之一。

设 G 和 G_T 是阶为素数 p 的群，存在一个可有效计算的双线性映射 $e:G\times G\rightarrow G_T$，该映射具有以下性质：

a)双线性：对于所有的 $a,b\in Z_p$ 和所有的 $g,h\in G$，满足 $e(g^a,h^b)=e(g,h)^{ab}$。

b)非退化性：存在 $g,h\in G$，使得 $e(g,h)\neq 1$。即不能将所有 $G\times G$ 的元素都映射到 G_T 中的某个相同的元素。

c)可计算性：对于所有的 $g,h\in G$，$e(g,h)$ 都是可以有效计算的。

2. 访问结构

设 $P=\{P_1,P_2,\cdots,P_n\}$ 为所有属性的集合，某个用户 u 的属性集 A 是 P 的一个非空子集，$A\subseteq\{P_1,P_2,\cdots,P_n\}$，则 N 个属性可用于鉴别 2^N 个用户。

访问结构 T 是集合 $\{P_1,P_2,\cdots,P_n\}$ 的一个非空子集，$T\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}\backslash\{\emptyset\}$。$T$ 代表一个属性判断条件：在 T 中的属性集合称为授权集，不在 T 中的属性集合称为非授权集。

3. 困难假设

设 G 是素数阶 p 的双线性群，g 是 G 的生成元，随机指数 $a,b,s\in Z_p$。若将一个元组 $(g,g^a,g^b,g^s)\in G^4$ 和一个元素 $z\in G_T$ 作为输入，则将决定 $z=e(g,g)^{abs}$ 的输出。如果下式成立：

$$|P_r[\beta(g,g^a,g^b,g^s,e(g,g)^{abs})=0]-P_r[\beta(g,g^a,g^b,g^s,z)=0]|\geqslant\varepsilon$$

表明存在一个算法 β 输出 $b\in\{0,1\}$，在 G 上具有优势 ε 解决 DBDH 难题。如果没有多项式时间算法具有不可忽略的优势解决 DBDH 难题，可以说 DBDH 假设在 G 上成立[8]。

4. CP-ABE 算法

CP-ABE 主要包含有 4 个算法，各算法描述如下：

1)初始化算法 $Setup$：生成主密钥 MK 和公共参数 PK。

2)密钥生成算法 $SK=KeyGen(MK,A)$：使用 MK 和用户属性集 A 生成用户的私钥 SK。

3)加密算法 $CT=Encrypt(PK,M,T)$：使用公共参数 PK、需加密的数据明文 M 和访问结构 T 进行加密，得到密文 CT。

4)解密算法 $M=Decrypt(CT,SK)$：用户使用私钥 SK 解密密文 CT，得到明文数据 M。

2.2 可扩展的访问控制标识语言(XACML)

可扩展访问控制标识语言(eXtensible Access Control Markup Language，XACML)是用于决定请求/响应的通用访问控制策略语言和执行授权策略的框架，它在传统的分布式环境中被广泛用于访问控制策略的执行。XACML 访问控制架构[9]主要由策略执行点(Policy Enforcement Point，PEP)、策略决策点(Policy Decision Point，PDP)、策略管理点(Policy Administration Point，PAP)、策略信息点(Policy Information Point，PIP)和上下文处理器组成，如图 1 所示。

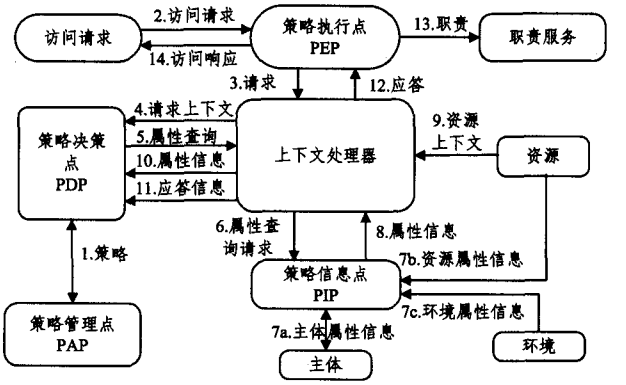

图 1 XACML 访问控制架构

XACML 访问控制流程如下：首先 PEP 接受原始的访问请求(origiNal Access Request，NAR)，并转发给上下文处理器，由其解析为 XACML 规范的请求并传递给 PDP，PDP 根据从 PAP 所获得的策略以及从 PIP 获取的实体属性对 XACML 规范请求进行判定，并将判定结果发给 PEP，最后由 PEP 执行访问判定结果。

3 CP-ABE 和 XACML 多权限安全云存储访问控制方案

3.1 总体方案

CP-ABE 和 XACML 结合实现多权限安全云存储访问控制方案的总体架构如图 2 所示。

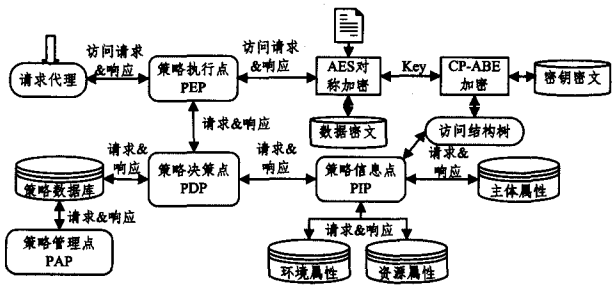

图 2 云存储访问控制方案

从图中可以看出，该架构与 XACML 架构的主要区别是策略集中的规则可以由 CP-ABE 加密算法中的访问控制结构树转换而来。通过将 CP-ABE 加密过程中采用的访问控制结构树转换为 XACML 的策略规则，应用 XACML 框架实现细粒度多权限访问控制机制。为保护用户敏感数据的机密性，首先，系统采用 AES 对称加密算法对数据明文进行加密，得到数据密文；其次，对称密钥采用 CP-ABE 算法进行加密，得到密钥密文；最后，将数据密文和密钥密文按照系统设计格式保存至云存储系统中。当某用户请求访问数据时，采用 XACML 机制控制用户的多种权限，若访问用户的主体属性通过 XACML 的策略规则，就可以访问密钥密文，通过解密密钥密文得到对称密钥，从而解密数据密文得到数据明文。XACML 策略规则不仅可以从 CP-ABE 访问控制结构树转换而来，也可以单独进行添加修改。

3.2 方案实现

本文方案基于开源项目 Sun's XACML[11] 和 cpabe Toolkit[12] 在 OpenStack 子项目 Swift 对象存储项目上实现。

3.2.1 系统初始化

方案中采用属性权威(Attribute Authority,AA)管理和分配实体(包括资源、主体和环境)的属性。主体属性包括用户姓名、用户 ID、部门、职务和入职时间等;资源属性包括名称、主题、资源大小、创建者和创建日期等;环境属性包括有时间、网络状况、资源使用率等。

运行 cpabe Toolkit 初始化算法 *Setup* 生成主密钥 MK 和公共参数 PK。

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

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

其中,G_0 为生成元为 g、阶为 p 的双线性群,随机参数 $\alpha,\beta\in Z_p$。

3.2.2 新文件创建

数据所有者上传机密数据到云存储服务器时,需要对数据进行如下处理:

1)DO 为文件 F 选择唯一标识号 ID_F,随机选择对称密钥 Key_F 加密 F 得到 C_F。

2)DO 指定访问控制结构树 T 并调用 CP-ABE 加密算法 $Encrypt(PK,M,T)$ 加密对称密钥 Key_F 得到 CT[4]。

假设 Y 是访问结构树 T 所有叶子节点的集合,记访问结构树 T 的根节点为 r,设节点 t 的门限值为 k_t,为节点 t 生成一个 k_t-1 次的随机多项式 q_t,$q_t(0)$ 代表该节点的秘密。定义函数 $ind(x)$ 返回节点 x 的索引编号,函数 $par(x)$ 返回节点 x 的父节点,函数 $att(y)$ 返回叶子节点 y 对应的属性。

随机选择参数 $s\in Z_p$,令 $q_r(0)=s$,对于其他节点 x,$q_x(0)=q_{par(x)}(ind(x))$。$Encrypt(PK,M,T)$ 加密算法加密对称密钥 Key_F 得到的的密钥密文 CT 如下:

$CT=(T,\tilde{C}=Key_F\cdot e(g,g)^{\alpha s},C=g^{\beta s},\forall y\in Y:C_y^{(1)}=g^{q_y(0)},C_y^{(2)}=H(attr(y))^{q_y(0)})$

3)文件在云存储服务器中的存储格式为 (ID_F,C_F,CT)。

4)云服务提供商根据 DO 上传数据中的访问控制树 T,解析并生成 XACML 使用的策略规则文件并存储于策略数据库中。云用户还可以根据资源属性和环境属性定义策略规则。

3.2.3 文件访问

当有云用户申请访问云存储数据时,需要进行以下处理。

1)云服务器首先验证云用户的有效性。

2)XACML 访问控制对用户的数据访问请求按照访问策略进行决策,流程如图 1 所示。若实体属性与访问控制策略匹配,则 XACML 决策为接受访问;否则拒绝访问请求。

3)若用户 u 通过 XACML 验证,根据用户的主体属性集 A 生成对应的私钥 SK_u。

$SK_u=(D=g^{(\alpha+\gamma)/\beta},j\in A:D_j=g^{\gamma}H(j)^{\gamma_j},D_j'=g^{\gamma_j})$

其中随机参数 $\gamma\in Z_p$,属性 $j\in A$。

4)执行解密算法 $Decrypt(CT,SK)$ 得到对称密钥 Key_F,使用该密钥解密数据密文得到明文,解密过程如下[4]:

首先定义递归运算 $DecryptNode(CT,SK,x)$,令 $i=attr(y)$,每个叶子节点 x 计算:

当 $i\notin A$ 时,$DecryptNode(CT,SK,x)=\perp$;

当 $i\in A$ 时,$DecryptNode(CT,SK,x)=\dfrac{e(D_i^{(1)},C_x^{(1)})}{e(D_i^{(2)},C_x^{(2)})}=e(g,g)^{\gamma q_x(0)}$。

对于非叶子节点 z,需要利用 k_z 个叶节点的 $DecryptNode(CT,SK,x)$ 作为拉格朗日插值定理的插值点,计算得到 $e(g,g)^{\gamma q_z(0)}$。

设访问控制树 T 的根节点为 R,令 $e(g,g)^{\gamma q_R(0)}=e(g,g)^{\gamma s}=B$,则解密明文 $M=\tilde{C}/(e(C,D/B)=\tilde{C}/(e(h^s,g^{(\alpha+\gamma)/\beta})/e(g,g)^{\gamma s})$。

3.2.4 权限撤销和策略更新

数据所有者要撤销某用户 u 对文件 F 的访问权限时,需要通过如下两种方式实现处理:

1)更新文件 F 对应的 XACML 访问控制策略,添加拒绝访问规则。

2)修改 CP-ABE 访问控制结构树 T,生成新的对称密钥进行加密,重加密方案采用云服务器端代理重加密机制[13]。

4 安全性分析

4.1 数据机密性

为保证用户数据的机密性和隐私,首先,用户数据通过 AES 对称加密算法加密;然后,应用 CP-ABE 算法加密其对称密钥;最后,对于 CP-ABE 加密得到的密钥密文采用 XACML 框架进行访问控制。Bethencourt 等人在文献[4]中已经证明 CP-ABE 的安全性是基于 DBDH 困难假设之上的,从而保证对称密钥的安全性,因此整个访问控制方案保证了用户数据的安全性和隐私。应用 XACML 细粒度授权架构保证只有合法用户在权限范围内才能访问、操作资源。

4.2 抗合谋攻击

假设云服务器是"诚实但好奇"的。假设进行合谋攻击的用户的联合属性集满足访问控制结构树,但其各自的属性集都不能完全满足访问结构树,由用户属性产生的私钥组件 $D_j=g^{\gamma}H(j)^{\gamma_j}$,显然合谋用户的属性不同,使得他们无法解密对称密钥,当然无法访问数据;即使用户合谋进行攻击,也不能恢复 $e(g,g)^{\gamma s}$,因此无法解密密钥文件。Goyal 等学者在文献[3]中已经证明 ABE 对于合谋攻击是安全的,本文方案是基于 CP-ABE 加密算法构建的访问控制机制,所以本文方案对于合谋攻击也是安全的。

4.3 后向前向安全

本方案无论对于新加入的用户还是已经撤销的用户,都保证外包云存储数据的后向和前向安全性。

当某个用户在某时刻获得满足密文访问策略的属性集时,与该属性相关的属性组密钥需要进行更新,并用更新的新属性组密钥进行重加密。用户即使保存以前系统中的密文,也不能准确解密得到明文,因为即使能够从密文中计算得到 $e(g,g)^{\gamma(s+s')}$ 的值,由于 s' 是随机值,不能获得,因此也不能准确计算出 $e(g,g)^{\gamma s}$。所以,该访问控制方案具有后向安全性。同理,当某用户被撤销权限时,系统采用新的密钥进行重加密,因此该算法同样具有前向安全性。

5 仿真及性能分析

实验机器：Inter(R) Core(TM) i7-4720HQ、16GB DRR3内存，操作系统为 Windows8. 1。实验环境：VMware Workstation 11. 1. 2 上安装 Ubuntul4. 04，采用开源云 OpenStack 构建云计算环境，Keystone 作为认证服务，Swift 作为云存储服务。实验代码基于 sunxacml-1. 2 和 cpabe-0. 11 库编写，对称加密算法采用基于 openssl-1. 0. 1j 库的 128bit AES 加密算法。

实验中，对基于 CP-ABE 和 XACML 结合访问控制方案的加密和解密时间开销进行评估。方案中，用户数据首先通过对称加密算法 AES-128 加密，CP-ABE 加密的仅仅是128bits 的对称密钥，整个方案中对于 CP-ABE 加密不同数据大小实验并没有真正的意义，本文实验采用不同的访问控制结构树与加解密时间之间的关系。访问控制结构树的叶子表示用户属性，所以节点的数目就是用户属性复杂度的体现。实验一测试了用户私钥产生时间与用户属性数量之间的关系，如图 3 所示。

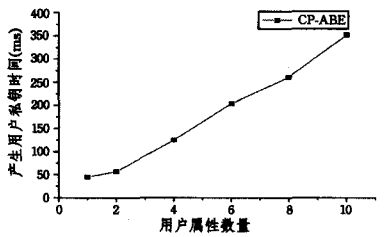

图 3 用户产生私钥时间与用户属性数量的关系

实验中，当用户属性数量为 2 时，不妨假设用户属性为 a_1 和 a_2，该用户的密钥生成时间为 57ms；当用户属性数量为 6 时，设用户属性为 $a_1, a_2, \cdots, a_6$，该用户私钥产生时间为 204ms。从图 3 可以看出，用户私钥产生时间与用户属性数量的关系成正比。

方案中应用 CP-ABE 加密对称密钥，所以假设加密文件大小为 1kB 固定不变。分别对不同属性数量的访问控制结构树进行加密解密实验，时间开销如图 4 所示。

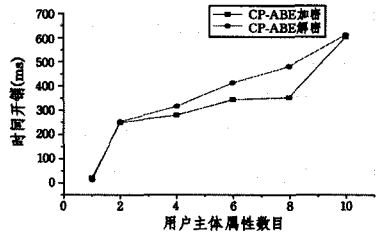

图 4 用户属性数目与加密解密时间的关系

图 4 展示了基于 CP-ABE 算法的加密与解密时间开销与用户主体属性数目(访问控制结构树中叶子节点数目)之间的关系。用户属性数目越多，加密、解密所用时间亦越多，所以在实际系统中，需要根据实际系统制定合适数目的用户属性。

结束语 本文提出基于属性加密结合 XACML 多权限安全云存储访问控制方案，保证云用户机密数据的安全和用户隐私不被泄漏；通过将 CP-ABE 访问控制结构树转换为适用于 XACML 应用的策略规则，将两者有机结合，构造具有细粒度、多权限、可扩展的访问控制方案；充分考虑了 CP-ABE 加密解密算法的效率，云存储中大量数据的重加密运算移交于云服务器端实现。下一步工作将对方案中的属性撤销效率进行研究。

参 考 文 献

[1] Larry D. Cloud computing hasn't gone Fortune 500 yet, But it's coming[EB/OL]. (2008-03). http://www.zdnet.com/article/cloud-computing-hasnt-gone-fortune-500-yet-but-its-coming

[2] Christian C, Idit K, Alexander S. Trusting the cloud[J]. Acm Sigact News, 2009, 40(2): 81-86

[3] 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

[4] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//IEEE Symposium on Security and Privacy. California, 2007: 321-334

[5] Pirretti M, Traynor P, McDaniel P, et al. Secure attribute-based systems[C]// Proceedings of the 13th ACM conference on Computer and communications security. New York: ACM, 2006: 99-112

[6] Wang Peng-pian, Feng Deng-guo, Zhang Li-wu. CP-ABE Scheme Supporting Fully Fine-Grained Attribute Revocation[J]. Journal of Software, 2012, 23(10): 2805-2816(in Chinese)
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

[7] Li Ming, Yu Shu-cheng, Zheng Yao. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption[J]. Parallel and Distributed Systems, 2013, 24(1): 131-143

[8] Brent W. Public Key Cryptography-PKC 2011 [M]. Berlin: Springer, 2011: 53-70

[9] 马恒太，李鹏飞，颜学雄，等. Web 服务安全[M]. 北京：电子工业出版社，2007：280-319

[10] Niu De-hua, Ma Jian-feng, Ma Zhuo, et al. Enhanced cloud storage access control scheme based on arrtibute[J]. Journal on Communications, 2013, 34(Z1): 276-284(in Chinese)
牛德华，马建峰，马卓，等. 基于属性的安全增强云存储访问控制方案[J]. 通信学报，2013，34(Z1)：276-284

[11] Sun's XACML Implementation[EB/OL]. http://sunxacml.sourceforge.net/

[12] Advanced Crypto Software Collection [EB/OL]. http://acsc.cs.utexas.edu/cpabe/

[13] Chen Yan-li, Song Ling-ling, Yang Geng. Efficient Aceess Control Scheme Combining CP-ABE and SD in Cloud Computing [J]. Computer Science, 2014, 41(9): 152-157, 168(in Chinese)
陈燕俐，宋玲玲，杨庚. 基于 CP-ABE 和 SD 的高效云计算访问控制方案[J]. 计算机科学，2014，41(9)：152-157，168