云存储环境下基于生物特征的访问控制机制研究

陈志杰[1] 黄 昆[2] 鲜 明[2]
(国防科学技术大学训练部信息中心 长沙 410073)[1]
(国防科学技术大学电子科学与工程学院 长沙 410073)[2]

摘 要 云计算是一种新型的计算方式,通过网络共享方式为用户提供按需使用的计算资源。如何加强对云计算资源的访问控制,保护用户的敏感信息和密钥不受恶意服务器和外部攻击者的窃取成为重要的安全问题。生物特征在这方面具有显著优势,文中研究了如何使用生物特征实现云存储数据访问控制的方法。该方法结合模糊身份加密、生物特征认证和密钥隔离加密机制,加强了私钥管理的安全性。同时,当每次用户提出访问请求时,云服务器就更新对应的文件头,而该文件头只有合法用户才能够解密。

关键词 云计算,访问控制,基于身份的模糊加密,密钥隔离加密,生物特征
中图法分类号 TP393 **文献标识码** A

Research on Biometric Based Access Control for Cloud Storage

CHEN Zhi-jie[1] HUANG Kun[2] XIAN Ming[2]
(Information Center, Training Department, National University of Defense Technology, Changsha 410073, China)[1]
(College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)[2]

Abstract Cloud computing is an arresting emerging computing paradigm that offers users on demand network access to a large shared pool of computing resources. How to strengthen the access control of cloud computing resources and protect sensitive data along with private key confidential against malicious servers or other external attackers, have been an important security problem. Biometric possesses notable advantage in this field, and hence this paper focused on leveraging biometric identity to achieve access control in cloud. We exploited and combined techniques of fuzzy identity based encryption(FIBE), biometric measurement, and key insulated encryption which enables augmenting the security of private key management. Specifically, we based on the idea that when every time legal user or malicious one makes the request of accessing data of his interest, and the cloud severs will update the corresponding header file which only the legal user has the ability to decrypt.

Keywords Cloud computing, Access control, Fuzzy identity based encryption, Key insulated encryption, Biometric

云计算虽然拥有按需使用、管理方便等优点,但也面临很多挑战,这些问题处理不当就可能阻碍其发展。根据云安全联盟(CSA)最新的研究,2013年云计算领域面临的9个威胁都与云的共享、按需特性相关。数据破坏和丢失是其中的两个典型威胁,虽然有很多用于保护数据免遭破坏和丢失的措施,但这并不能解除用户对于存储在云中的数据私密性的顾虑。这种顾虑源自云存储器不在用户的信任域内,用户并不完全信任云服务商。因此,当用户将数据托管给云存储时需要加强数据对云服务商的机密性。

1984年,Shamir提出了一个崭新的概念——基于身份的加密[1]。在这种加密体制中,用户的公钥由他的身份信息如邮件地址等决定,对应的密钥由私钥生成器(PKG)根据其身份信息生成。由于身份是用户的自然属性,没必要将其与数字证书绑定。这样就可以成功避免使用传统公钥加密架构所需的证书。目前,大量基于身份的签名(IBS)架构被提出。不过标准的IBS都基于私钥安全存放的假设。然而,随着越来越多的加密系统应用到非安全环境中(如移动设备),密钥暴露的问题越来越严重。这个问题对于加密系统来说是最致命的,因为泄露私钥意味着安全性遭到彻底破坏。

为了应对密钥暴露问题,密钥演化协议应运而生。该机制包括入侵恢复[2]和密钥隔离[3,4]等。密钥隔离由Dodis等人在2002年欧洲密码会议上提出[3]。该模型包括物理安全但是计算能力受限的设备(称为助手节点)。完整的密钥分为两部分:辅助密钥和初始临时密钥。前者存储于助手节点中,后者由用户持有。系统的生命周期被分为离散的时间段。公钥在整个生命周期中保持不变,临时密钥周期性地更新:在每一个阶段的初始,用户从助手节点处获取当前时间段的辅助密钥,并结合前一阶段的临时密钥得到当前阶段的临时密钥。临时密钥被用于在相应阶段的消息签名。指定时间段的临时密钥暴露并不会影响剩下的时间段的密钥的安全。因此,这种机制可以最小化由于密钥暴露引起的损失。

接着Dodis等人的开创工作,几种密钥隔离机制被提出,包括基于身份的密钥隔离加密[4,5],以及密钥隔离签名[6,7]。为了最小化IBS中由于密钥暴露引起的损失,Zhou等人将密

陈志杰 女,硕士,副教授,高级工程师,主要研究方向为计算机网络与安全,E-mail:zzjjchen@163.com;黄 昆 男,博士生,主要研究方向为网络安全与分布式存储系统,E-mail:khuang_123@163.com(通信作者);鲜 明 男,博士,教授,主要研究方向为态势评估、网络与信息安全。

钥隔离机制应用到 IBS 中，并提出了第一个基于身份的密钥隔离签名(IBKIS)框架 ZCC[8]。然而，ZCC 框架中密钥完全存储于助手节点中，因此不能满足强密钥隔离安全的需求。攻击者如果控制了用户助手节点，就可以得到该用户的所有临时密钥。

本文着重于解决云访问控制中的密钥暴露问题。不同于 Dodis 提出的模型，本文使用访问的次数取代时间段来代表密钥更新的间隔。通过精心设计，该机制能做到类似于一次一密机制，而一次一密加密方式在密钥管理中被公认是绝对安全的。

1 技术基础

基于身份的模糊加密(FIBE)是一种公钥加密体制[9]，最开始用于一对多的通信。在 FIBE 中，用户的身份被看作一组可描述的属性。FIBE 体制允许使用私钥 ω 来解密用 ω' 加密的密文，前提是 ω 和 ω' 足够接近。这种接近程度用集合重叠的程度来衡量。FIBE 的容错性能正好可用于克服生物特征采样时产生的噪声，从而利用生物特征作为身份来实现加密和访问控制。

在构建访问控制的框架之前，先回顾一下加密技术。G_1 是素数特征为 p 的双线性组，g 是 G_1 的生成元。用 $G_1\times G_1\to G_2$ 表示双线性映射。安全参数 κ 决定双线性组的大小。为了使密钥 ω 能解密用 ω' 加密的秘文，设定一个阈值 d，满足 $|\omega\cap\omega'|\geqslant d$。此外，定义拉格朗日系数 $\Delta_{i,S}$，对于任意 $i\in Z_p$，和以 Z_p 中元素组成的集合 S，有：

$$\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j} \tag{1}$$

用集合 U 的元素代表身份属性，并将每一个元素与一个 Z_p^* 中的特定的整数相关。FIBE 架构由 4 种算法组成，分别描述如下：

初始化：首先，定义集合 U。为了简便，使用 Z_p^* 的前 $|U|$ 个元素作为集合 U，即整数 $1,\cdots,|U|(\mathrm{mod}\ p)$。接下来从 Z_p 中统一随机选取 $t_1,\cdots,t_{|U|}$。最后 Z_p 从中随机选取 y。公钥：$PK=(T_1=g^{t_1},\cdots,T_{|U|}=g^{t_{|U|}},Y=e(g,g)^y)$，主密钥是 $MK=(t_1,\cdots,t_{|U|},y)$。其中 PK 对系统中各方都是公开的，MK 由授权方秘密保存。

加密：使用公钥 ω' 加密消息 $M\in G_2$。首先选取随机数 $s\in Z_p$。密文发布如下：$E=(\omega',E'=MY^s,\{E_i=T_i^s\}_{i\in\omega'})$。注意身份 ω' 包含在密文中。

密钥生成：为了生成 $\omega\in U$ 对应的私钥，采用以下措施。随机产生一个 $d-1$ 次的多项式 q，使得 $q(0)=y$。私钥由 $(D_i)_{i\in\omega}$ 组成，其中对于任意 $i\in\omega$，有 $D_i=g^{\frac{q(i)}{t_i}}$。

解密：假设密文 E 由身份 ω' 的密钥加密生成，私钥 ω' 满足 $|\omega\cap\omega'|\geqslant d$。选择任意包含 d 个 $\omega\cap\omega'$ 元素的子集 S，解密过程如下：

$$\frac{E'}{\prod_{i\in S}(e(D_i,E_i))^{\Delta_{i,S(0)}}}=\frac{Me(g,g)^{sy}}{\prod_{i\in S}(e(g^{\frac{q(i)}{t_i}},g^{st_i}))^{\Delta_{i,S(0)}}}$$

$$=\frac{Me(g,g)^{sy}}{\prod_{i\in S}(e(g,g)^{sq(i)})^{\Delta_{i,S(0)}}}=\frac{Me(g,g)^{sy}}{e(g,g)^{s\sum_{i\in S}q(i)\Delta_{i,S(0)}}}=M \tag{2}$$

其中最后一个等式通过使用多项式插值得到。$d-1$ 次的多项式 $sq(x)$ 可由 d 个点插值运算得到。

2 具体方案

下面将在系统层构建访问控制框架，包括系统创建、文件创建和文件访问等。

系统创建：数据拥有者选择安全参数 κ 并调用算法层接口函数 $FIBESetup(\kappa)$，输出系统公钥 PK 和主密钥 MK。

文件创建：在将文件上传到云服务器之前，数据拥有者按如下流程处理文件(见图 1)：

为该文件选择用户的独有的身份 ID，如用户生物特征属性；

随机选择对称加密密钥 $DEK\leftarrow K$，其中 K 是密钥空间，并使用 DEK 加密文件；

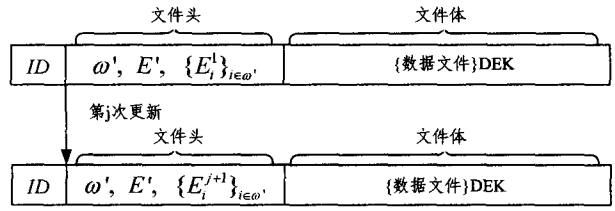

图 1 云存储数据文件更新格式

选择采样自用户的一组生物属性集 ω'，并根据 FIBE 算法用 ω' 加密 DEK，即 $(\omega',E',\{E_i^1\}_{i\in\omega'})\leftarrow FIBEEncrypt(\omega',DEK,PK)$。

文件访问：该操作中，CS 响应用户的文件访问请求，然后更新文件头。同时，计数器 CR_{cloud} 加 1(初始计数为 0)。之后，CS 发送更新的文件头、请求文件体的密文以及计数值 CR_{cloud} 给用户。一旦收到 CS 的响应，用户就比较两个计数器 CR_{cloud} 和 CR_{user} 的计数值，接着根据两者之间的差异更新其密钥。最后，用户通过调用 $FIBEEncrypt(\omega,\omega',D_i^{j+1},E_i^{j+1})_{i\in(\omega\cap\omega')}$ 解密 DEK 并通过 DEK 解密数据文件。

正确性：根据密钥隔离机制原理，

$$\frac{E'}{\prod_{i\in S}(e(D_i^{j+1},E_i^{j+1}))^{\Delta_{i,S^{(0)}}}}=\frac{DEK\cdot e(g,g)^{sy}}{\prod_{i\in S}(e(g^{\frac{st_i}{\prod_{k=j}^{k=j}x_k}},g^{\frac{q(i)\prod_{k=1}^{k=j}x_k}{t_i}}))^{\Delta_{i,S^{(0)}}}}$$

$$=\frac{DEK\cdot e(g,g)^{sy}}{\prod_{i\in S}(e(g,g)^{sq(i)})^{\Delta_{i,S^{(0)}}}}=\frac{DEK\cdot e(g,g)^{sy}}{e(g,g)^{s\sum_{i\in S}q(i)\Delta_{i,S^{(0)}}}}=DEK \tag{3}$$

这与式(2)对应。

3 评估

3.1 安全性分析

定义 1(修改的双线性迪夫-霍尔曼 MBDH 假设[9]) 假设挑战者随机选择 $a,b,c,z\in Z_p$，那么没有多项式时间，攻击者是不可能分辨出 $(A=g^a,B=g^b,C=g^c,Z=e(g,g)^z)$ 与 $(A=g^a,B=g^b,C=g^c,Z=e(g,g)^{\frac{ab}{c}})$ 的。

定理 1 在本文的攻防模型中，访问控制框架可以免受外部攻击者的窃取，并支持安全密钥更新。

证明：在证明之前，先赋予攻击者更大的能力，即获取用户生物特征采样的能力和获取用户临时密钥 x_j 的能力。本文的模型中，用户的生物特征并不用作私钥，因为这种特征容易被高级技术人员获取，根据 Waters 等提出的选择 ID 攻击

(下转第 267 页)

图像数字水印[J]. 计算机应用研究,2010,27(2):798-800
[2] 何冰,朱志平. 基于奇异值分解的抗几何攻击鲁棒性盲水印算法[J]. 技术研究,2012,11(3):71-73
[3] 张翼,唐向宏. 基于图像归一化的抗几何攻击水印技术[J]. 电路与系统学报,2009,14(6):53-58
[4] Pereira A,Pun T. Robust template matching for affine resistant image watermarks [J]. IEEE Transactions on Image Processing,2000,9(6):1123-1129
[5] 楼偶俊. 基于 Contourlet 域特征点的抗几何攻击水印方法[J]. 计算机研究与发展,2010,47(1):113-120
[6] 陈利利,王向阳. 基于 SIFT 的椭圆区域鲁棒数字水印方案[J]. 计算机工程与应用,2012,48(1):98-101,107
[7] 赵文娴,王玲,杨锴饴. 基于 SIFT 的 NSCT-SVD 域水印算法[J]. 计算机工程与应用,2012,48(10):106-110
[8] Candes E J,Wakin M B. An introduction to compressive sampling[J]. IEEE Signal Processing Magazine,2008,25(2):21-30
[9] Baraniuk R,Davenport M,Devore R,et al. A simple proof of the restricted isometry property for random matrices[J]. Constructive Approximation,2008,28(3):253-263
[10] Dossal C, Reyre G, Fadili J. A numerical exploration of compressed sampling recovery[J]. Linear algebra and Its Applications,2010,432(7):1663-1679
[11] Low D G. Object recognition from local scale-invariant features [C]// International Conference on Computer Vision. Corfu, Greece,1999(9):1150-1157
[12] Lowe D G. Distinctive image features from scal-invariant key points[J]. Internatonal Journal on computer Vision, 2004, 60 (2):91-110

(上接第 251 页)

模型[9],这种情况下框架的安全性降低到决策 MBDH 假设的程度。

假设部分攻击者有能力获得用户的生物特征采样、临时密钥 D^j 和临时关键字 x_{j-1},他就可以利用用户的生物特征顺利访问数据拥有者的文件。然而,一旦攻击者提出访问请求,CS 就会使用密钥隔离机制更新文件头并将更新后的文件头和文件体一起发送给攻击者,基于这种更新机制的特性,攻击者仅有微乎其微的概率解密出文件头。相反,合法用户可以根据公式 $x_j=H((x_0^*)^j) \bmod p$ 将其私钥从 x_{j-1} 更新为 x_j。此外,合法用户可通过 $D_i^{j+1}=(D_i^j)^{x_j}$ 计算更新密钥 $D_{i\in\omega\cap\omega'}^{j+1}$。

因此,该框架是受到严格的保护的,此外,基于密钥隔离机制还可实现安全密钥的更新。

3.2 性能分析

该部分通过数值分析评估本文提出的访问控制框架的性能,包括由于 CS 和用户的更新操作引起的性能开销。

引理 1 在一个素数顺序为 p 的组中,任意元素 g 的 y 次方(y 是在 Z_p 中随机选取的)可以通过最多 $O(\ln p)$ 次乘法运算计算得到。

证明:首先用二进制表示 y,$y=y_0\cdot 2^0+y_1\cdot 2^1+\cdots+y_n\cdot 2^n$,其中 $2^n<y\leqslant 2^{n+1}$,$y_i=0$ 或 1。从而有 $g^y=\prod_{i=0}^{i=n}(((g^{y_i})^2)^{\cdots})^2$。这样计算 g^y 最多需要 n 次平方运算和 n 次乘法运算,相当于总共需要 $O(\ln p)$ 次乘法运算,$n\approx O(\ln y)$ 与 $O(\ln p)$ 是同一个数量级。

引理 2 对于任意元素 $\beta\in Z_p^*$,其中 p 是素数,给定一个数 $x\in Z_p^*$,$\beta^{\frac{1}{x}}$ 的计算开销为 $O(\ln p)$ 次乘法运算。

证明:由于 p 是素数,x 对于是 p 相对素数。根据 Euclid 算法,存在整数 a,b 满足 $ax+bp=1$,容易得到:

$$\beta=\beta^{ax+bp}=\beta^{ax},\beta^{\frac{1}{x}}=\beta^a \tag{4}$$

从上面的等式中可知,计算 $\beta^{\frac{1}{x}}$ 大概需要 $O(\ln p)$ 次乘法运算。

CSP 更新开销:从式(3)中可知,每次 CS 更新文件头仅需要执行 $|\omega'|\cdot O(\ln p)$ 次乘法运算(见表 1),同时 CS 删除原来的文件头并通过加 1 更新 CR_{cloud},这个更新操作的开销可忽略不计。

用户更新开销:用户想访问其感兴趣的文件,首先请求 CS 提供 CR_{cloud},将得到的 CR_{cloud} 与 CR_{user} 比较。接下来用户根据两者的不同更新其私钥。根据引理 1,用户需要{$|\omega'|\cdot O(\ln p)$}次乘法运算(见表 1)。

表 1 计算复杂度

操作	复杂度
文件访问——CSP 更新	$\|\omega'\|\cdot O(\ln p)$
文件访问——用户更新	$\|\omega'\|\cdot O(\ln p)$

结束语 本文中研究了云计算中基于生物特征的访问控制问题和密钥暴露问题。为了保护敏感数据和私钥的机密性,以免受到恶意云服务器和外部攻击者的攻击,并克服生物特征噪声大的缺点,本文提出了一种更新 FIBE 框架,即持续地在 CS 和用户之间执行更新操作。在文件创建过程中利用 FIBE 的特性提供基于生物特征的访问控制。此外,通过使用密钥隔离框架,本文的访问控制架构可以更新安全密钥,类似于一次一密机制。通过安全分析和性能分析,证明该架构是安全和轻量级的。

参 考 文 献

[1] Shamir A. Identity-Based cryptosystems and signature schemes [C]// Procedings of the Crypto 1984. volume 196 of LNCS, 1984:47-53
[2] Itkis G, Reyzin L. SiBIR: Signer-base intrusion-resilient signatures [C]// Procedings of the Crypto 2002. volume 2442 of LNCS,2002:499-514
[3] Dodis Y,Katz J,Xu S,et al. Key-Insulated Public-Key Cryptosystems[C]// Procedings of EUROCRYPT 2002. volume 2332 of LNCS,2002:65-82
[4] Bellare M, Palacio. Protecting against key exposure: Strongly key-insulated encryption with optimal threshold [EB/OL]. [2002]http://eprint. iacr. org/2002/064
[5] Hanaoka, Imai. Parallel key-insulated public key encryption [C]// Procedings of the PKC 2006. volume 3958 of LNCS,2006:105-122
[6] Katz D, Xu Yung. Strong key-insulated signature schemes [C]// Procedings of the PKC 2003. volume 2567 of LNCS,2003:130-144
[7] Le Z,Ouyang Y,Ford J,et al. hierarchical key-insulated signature scheme in the CA trust model [M]// Information Security and Cryptology. Springer,2006
[8] Zhou Y,Cao Z,Chai Z. Identity based key insulated signature [C]// Procedings of the ISPEC 2006. volume 3903 of LNCS, 2006:226-234
[9] Sahai A,Waters B. Fuzzy Identity Based Encryption [C]// Proceedings of EUROCRYPT 2005. volume 3494 of LNCS, 2005: 457-473