

基于 CP-ABE 访问控制系统的设计与实现

周彦萍^{1,2}, 马艳东³

- (1. 河北省科学院 应用数学研究所, 河北 石家庄 050081;
2. 河北省信息安全认证工程技术研究中心, 河北 石家庄 050081;
3. 石家庄开发区冀科双实科技公司, 河北 石家庄 050081)

摘要:在访问控制中,传统公钥加密由于其需要对接收群体的每个成员用其公钥加密,再分发,因此需要获取接收群体中每个成员的身份。但是,在分布式应用中,却难以一次获取接收群体的规模与成员身份。如果列举用户身份,则会损害用户隐私。基于密文策略的属性加密体制(CP-ABE),由于其广播式的、授权人通过满足某些条件就能确定的特点,避免了由于必须获取这些信息而引出的数据安全问题。于是,文中给出了一种基于 CP-ABE 的混合加密访问控制系统的设计与实现方案。通过实际项目的成功应用,证明了该方案的可行性与优越性。

关键词:密文策略的属性加密;基于属性的加密体制;密文策略;访问控制

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2014)02-0145-04

doi:10.3969/j.issn.1673-629X.2014.02.035

Design and Implementation for Access Control System Based on CP-ABE

ZHOU Yan-ping^{1,2}, MA Yan-dong³

- (1. Institute of Applied Mathematics, Hebei Academy of Sciences, Shijiazhuang 050081, China;
2. Hebei Information Security Authentication Engineering Research Center, Shijiazhuang 050081, China;
3. SJZ JKSS Technology Co., Ltd, Shijiazhuang 050081, China)

Abstract: In access control, due to the need to encrypt with the public key for every member of group in traditional public encryption, then to distribute, so you need to get each member identity of the group. But it is difficult to get all information of receiving group. If list the users' identity, will damage the users' privacy. The CP-ABE, because of the characteristics of broadcasting, the authorized person by satisfying certain conditions to determine, avoids the problems of data security caused by having to get the information. So present a scheme of design and implementation of hybrid encryption access control system based on CP-ABE. Through the successful application of actual project, prove the feasibility and superiority of the scheme.

Key words: CP-ABE; attribute-based encryption; ciphertext-policy; access control

0 引言

随着信息技术与网络技术发展的日新月异,分布式应用得到了越来越广泛的应用。传统的加密体制^[1-3]如公钥基础设施(Public Key Infrastructure, PKI)及基于身份加密体制(Identity Based Encryption, IBE)^[4-5]的加密,在分布式应用中得到了广泛的应用。采用传统加密体制进行加解密处理的过程如下:

①首先列出要共享信息的所有用户,然后对用户逐一取出公钥;

②对信息共享群体中的每个用户,用其公钥对共享信息加密;

③将加密后的信息,逐一发给共享群体中的每个用户;

④用户对收到的密文用其私钥解密,得到信息的明文。

从上面的处理过程可知,对传统加密体制而言,首先必须列举共享群体中的用户并获取其公钥,然后须针对每一用户利用其公钥生成密文,加密次数就是共

享群体中的用户数。另外,在一些分布式的网络应用中,由于系统在地域上的广泛分布,信息共享的群体可能遍布全国甚至全球;或者是共享群体中的个体数量会极其庞大,不仅难以列举,还可能损害用户隐私。而信息共享的需求不仅安全性要求高,效率也有很高要求。面对这种情形,传统加密体制无能为力,不能满足信息共享的安全需求。

密文策略的属性加密 (Ciphertext–Policy Attribute–Based Encryption, CP–ABE) 是基于属性加密 (Attribute–Based Encryption, ABE)^[6] 机制的扩展延伸。ABE 机制将密文、用户私钥与属性关联,通过制定访问控制策略来限定用户的共享权限,极大地降低了数据共享处理的开销和占用的带宽。CP–ABE 能够更加灵活地表示访问控制策略,拥有更强的访问控制能力。CP–ABE 将用户的身份表示为一个属性集合,而加密数据则与访问控制结构相关联,一个用户能否解密密文,取决于用户身份所对应的访问控制结构与解密密文相关联的属性集合是否匹配。相对传统公钥加密,CP–ABE 机制需根据属性及访问结构加密与解密,无需关注信息共享群体中成员的规模和身份信息,具有高效性、抗串联性与策略表示灵活性等优点。

为解决传统公钥加密机制在访问控制中面临的问题,同时,考虑到 CP–ABE 所表现出来的优点,文中提出一种基于 CP–ABE 的访问控制的设计方案。通过实际项目的验证,证明该方案设计的正确性与先进性。

1 系统设计

1.1 需求分析

对现有分布式应用中的安全问题进行研究,经过分析,利用传统加密体制共享信息主要有两方面不足:

一是资源提供方需要用接收群体中每个用户的公钥加密消息,并将密文再分送给相应的用户,导致处理开销大和占用带宽多;

二是要求资源提供方在加密前获取全部接收用户的身份信息,但分布式应用难以一次获取接收群体的规模与成员身份,而列举用户身份还可能损害用户隐私。

针对以上不足,利用 CP–ABE 具有广播式的、授权人通过满足某个条件^[7–8]就能确定的特点,设计一种混合加密的访问控制方案,该方案能满足如下需求:

(1) 某些信息只对特定人群开放,但这个特定人群并不能具体地确定到人;

(2) 当被赋予访问权限的某个用户要实施访问行为时,还要判定运行环境是否满足允许访问的条件;

(3) 某些重要信息的访问还须满足是否在访问开放期、访问次数是否超限等约束条件。

1.2 总体设计

1.2.1 基于 CP–ABE 的访问控制设计

(1) CP–ABE 方案选取。

J. Bethencourt 等人^[8]于 2007 年提出的 CP–ABE 方案非常贴合于实际应用场景,方案效率高。因此,文中将其提供的 CP–ABE 算法运用到访问控制中,实现了基于 CP–ABE 的访问控制。J. Bethencourt 等人的 CP–ABE 方案有四个算法:

① 初始设置 Setup()。

输入系统安全参数 Para, Setup() 输出系统公共参数 PK 和主密钥 MK。

(PK, MK) = Setup(Para)

② 加密算法 Encrypt()。

输入系统公共参数 PK、访问结构 T 和明文 M , Encrypt() 输出密文 CT。

CT = Encrypt(PK, M , T)

③ 密钥抽取 KeyGen()。

输入系统主密钥 MK 和属性集合 S , KeyGen() 输出对应于 S 的解密密钥 KS。

KS = KeyGen(MK, S)

④ 解密算法 Decrypt()。

输入系统公共参数 PK、用访问结构 A 加密的密文 CT, 及对应于属性集合 S 的解密密钥 KS。如果属性集合 S 满足访问结构 T , 则 Decrypt() 输出消息 M 。

M = Decrypt(PK, CT, KS)

(2) 属性集合。

利用授权管理基础设施 (Privilege Management Infrastructure, PMI) 的属性证书 (Attribute Certificate, AC) 来描述 CP–ABE 中的属性集合^[8]。

用户通过属性来描述,用 AC 作为用户属性的凭证。AC 根据用户提交的描述信息生成,并采用颁发者的 IBE 私钥签名。AC 采用符合国际标准 X.509 V4 的国标 GB/T 16264.8–2005^[9–11] 证书格式及抽象语法规符号 (Abstract Syntax Notation One, ANS.1) 的编码格式来描述。

(3) 访问结构。

利用可扩展的标记语言 (eXtensible Markup Language, XML) 文档记录 CP–ABE 中的访问结构^[8]。

信息发布者定义能共享信息的用户,授权用户应该满足的条件形成 XML 文档后经加密再存储到属性描述符证书 (Attribute Descriptor Certificate, ADC) 中。

(4) 访问控制模型。

采用可扩展访问控制标记语言 (eXtensible Access Control Markup Language, XACML) 来构建访问控制模型,系统采用 XACML 2.0 标准^[12]。

ADC 中存储的访问结构是访问控制策略的主要

组成部分,除此之外,访问控制策略还包括环境约束和策略约束等条件,这些以 XACML 策略文件的方式存储,纳入 XACML 控制模型来处理。

(5) 环境和策略约束。

环境和策略约束条件一般用于对授权用户行使访问行为时,其所处环境或权限应该满足的限定条件。比如,对于那些密级较高的文档,只要系统察觉用户电脑能与外网有链接或能够使其上的数据向外部传送(如有 U 盘、光盘等设备在使用等),即使他是授权用户,系统也不会让他共享该文档;另外,有些文档特定时间段里才能共享,访问次数或共享的用户总数有规定等。

针对这种情形,利用 XACML 的策略文件考虑 CP-ABE 访问控制要求的运行环境条件和策略约束条件。即在 XACML 访问控制模型中,增加 CP-ABE 策略,以表示文档共享时要满足的运行环境条件和策略约束条件,这些条件与 XACML 原有的策略处理方式一样,用 XACML 策略文件存储,策略决策点(PDP)对此进行评估与判决。评估通过了,用户才能够收到用 CP-ABE 加密过的文件,存储在 AC 中的用户属性满足 ADC 中的访问结构后才能顺利对收到密文解密。

1.2.2 CP-ABE 与 IBE 相结合

系统中的每个用户(包括服务器端的系统管理员)都拥有专门的数字存储设备 USB Key 或专用的手机 TF 卡。该设备中存放着用户的私密信息。每个用户有两对 IBE 密钥对,一对用于数字签名,一对用于加密。私钥存储在 USB Key 或 TF(Trans-Flash)手机卡中,公钥存于服务器中。每个用户的 CP-ABE 私钥也存在该设备中。

为了保证 CP-ABE 访问结构的安全,方案对描述访问结构的 XML 文件加以防护,利用发布人的私钥签名、系统的公钥加密,保证访问结构 XML 文件的不可抵赖性与不被篡改,保证传输中不被窃取。

1.2.3 混合加密框架

CP-ABE 和 IBE 都属于非对称加密算法,与对称加密相比效率较低,难以直接用于加密大量数据,因此系统采用混合加密框架,即先使用对称密钥对数据加密,而后使用 CP-ABE 或 IBE 加密该对称密钥。混合加密框架下的工作流程如图 1 所示。

1.2.4 授权过程

资源提供方需要定义共享用户、制定环境和策略约束条件。

(1) 定义授权用户。

通过指定授权用户应该满足的条件来限定授权人群,并由此生成 XML 文件,加密后存入属性描述符证书中。

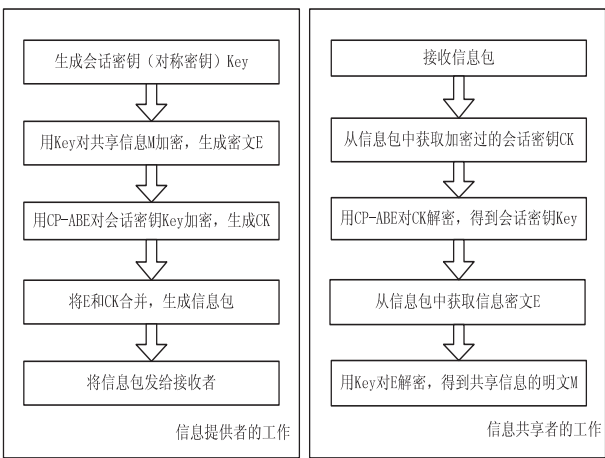


图 1 混合加密框架工作流程

(2) 制定环境和策略约束条件。

制定出授权用户实施访问行为应该满足的环境与策略约束条件,形成 XACML 策略文件,以便 PDP 评估与判决。

1.2.5 信息共享方式

当一个电子文档需要被共享时,文档提供者、XACML 访问控制系统及共享用户所做工作如下:

(1) 文档提供者的工作。

文档提供者的工作如图 2 所示。

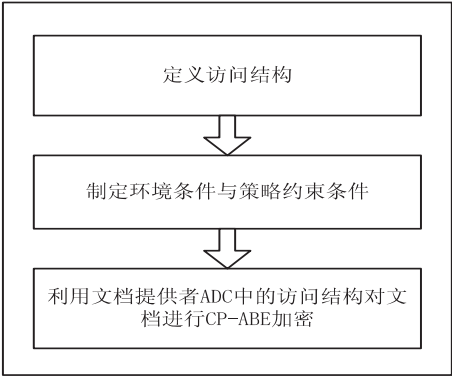


图 2 信息共享中文档提供者的工作

具体步骤如下:

①该文档提供者定义授权用户应满足的条件即访问结构,形成 XML 文档,并以其属性描述符证书存储之;

②该文档提供者制定环境与策略约束条件,形成 XACML 策略文件;

③系统利用文档提供者属性描述符证书中的访问结构对文档 CP-ABE 加密,加密过程如下:

- 生成会话密钥 Key;
- 用会话密钥 Key 对要共享的电子文档内容进行加密,形成密文 $E(F)$;
- 用系统授权管理员的签名私钥对 $E(F)$ 签名,形成签名 SIG;
- 获取资源提供者的属性描述符证书,从中获取

访问结构的 XML 文件,生成访问结构 T ;

●利用 CP-ABE 体制,对会话密钥 Key 加密,结果为 CT , $CT = \text{Encrypt}(PK, Key, T)$;

●生成加密信息包, $CT + E(F) + \text{SIG}$, 并存入数据库或发送给请求共享的用户。

(2) XACML 访问控制系统的工作。

XACML 访问控制系统的工作如图 3 所示。

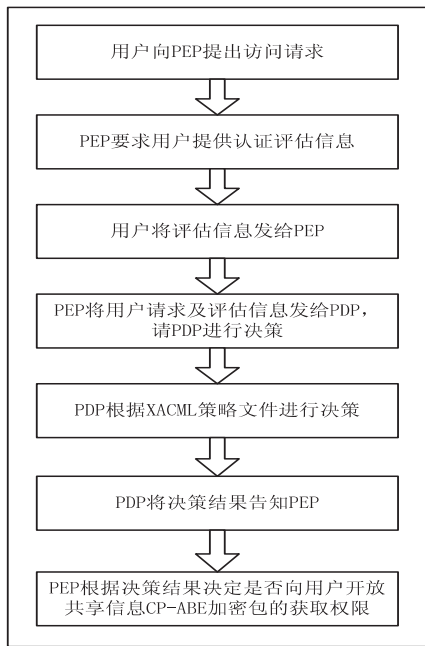


图 3 信息共享中 XACML 访问控制系统的工作
具体步骤如下:

①用户向策略执行点(PEP)提出该文档的访问请求;

②PEP 进行响应,并要求用户提供相关的认证评估信息;

③用户将收集到的评估信息发送给 PEP;

④PEP 将用户提供的访问请求及相关评估信息发给 PDP 进行决策;

⑤PDP 根据 XACML 策略文件判定系统环境是否满足访问请求,策略约束条件是否也能够满足,若有任何一项不满足,则 PDP 就会判为拒绝访问;

⑥PDP 将决策结果告知 PEP;

⑦PEP 接收到的 PDP 决策结果若为允许访问,则对用户放开该文档加密包的获取权限,用户获得该加密信息包,然后就可以进行 CP-ABE 解密了。

(3) 共享用户的工作。

共享用户得到该文档的 CP-ABE 加密信息包后的工作如图 4 所示。具体步骤如下:

①由加密信息包获取签名 SIG;

②获取系统授权管理员的 IBE 签名公钥;

③用系统授权管理员的 IBE 签名公钥验证签名 SIG,通过后继续,否则结束;

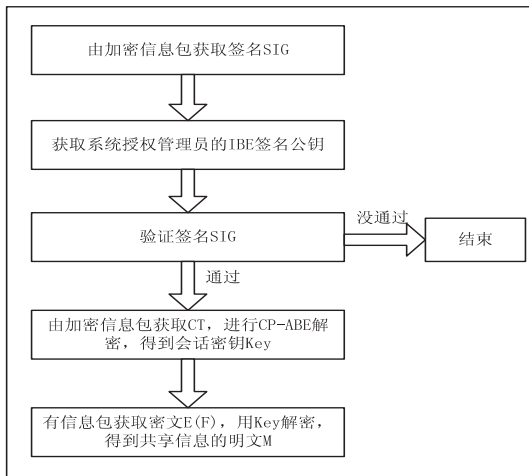


图 4 信息共享中共享用户的工作

④由信息包获取 CT , 利用 CP-ABE 加密体制,用自己 USB Key 设备或手机 TF 卡中的属性密钥 SK 对 CT 解密,得到会话密钥 Key 。 $Key = \text{Decrypt}(CT, SK)$, 只有授权用户才能正确解密;

⑤由信息包获取 $E(F)$, 用 Key 对其解密,得到要访问的信息明文。

2 结束语

文中提出的基于 CP-ABE 的混合访问控制方案,在笔者单位开发的《婴幼儿在线专家诊断系统》和《基于 PMI 的内网安全系统》中得到应用。前者通过该方案的应用,用户可以制定年龄、性别、地域等条件/属性以形成朋友圈。在朋友圈中,用户对孩子们的发育情况进行曲线、表格等形式进行比对和互访。这样,特定人群只须满足某种条件,而不必一一指定,避免了因为不能列举共享人群而带来的信息难以共享的问题。后者利用该方案进行访问控制。在电子文档共享时,不用事先确定每个共享用户,且对所有共享用户只须执行一次加密。因此,没有再出现原访问控制方案中明显的延迟现象。而且,从技术上来说,原有访问控制方案不用改动,只须在此基础上增加 CP-ABE 相关的一些功能,实施起来非常简单。由此可见,新方案在增加少量工作的情况下,避免了原方案在采用 PKI 进行信息共享时,信息提供者需要先列出所有共享用户,再实行一对一加密而导致的加密次数多、共享延迟、用户隐私被侵犯等问题。

文中通过研究基于传统公钥加密机制在分布式应用中所面临的窘境,并深入研究 CP-ABE 所具有的优势,提出了基于 CP-ABE 的混合加密访问控制系统。经过实际项目应用验证,证明该设计方案能够降低共享处理的开销和加密次数,增强了系统的安全性,提高了运行效率。然而,CP-ABE作为一种相对较新的理

(下转第 152 页)

信息整合成二维表(属性、属性值)的形式,以信息增益作为挑选属性和分配权重因子的标准,应用机器学习的算法让系统进行学习,使系统对恶意软件形成了良好的识别能力。需要进一步探究的是:

1)内核调用的选取方法,在该方法中,是通过分析恶意行为在底层内核调用的实现方法,确定保留哪些内核调用;其科学性有待严谨的实验证明;

2)Android 平台恶意软件的动态检测系统的实现要充分考虑到它的特殊性,既要保证能在本地执行检测,又要尽量少地占用硬件资源。

参考文献:

- [1] Zhou Yajin, Jiang Xuxian. Dissecting Android malware: Characterization and evolution[C]//Proc of IEEE symposium on security and privacy. [s. l.]:[s. n.],2012.
- [2] Schmidt A D, Schmidt H G, Batyuk L, et al. Smartphone malware evolution revisited; Android next target[C]//Proc of 4th IEEE international conference on malicious and unwanted software. [s. l.]:[s. n.],2009.
- [3] 符易阳,周丹平. Android 安全机制分析[J]. 信息安全,2011(9):23-25.
- [4] 廖明华,郑力明. Android 安全机制分析与解决方案初探[J]. 科学技术与工程,2011,11(26):6350-6355.
- [5] Shabtai S, Kanonov U, Elovici Y. "Andromaly": A behavioral malware detection framework for Android devices[J]. Journal

of intelligent information systems,2012,38:161-190.

- [6] Isohara T, Takemori K, Kubota A. Kernel-based behavior analysis for Android malware detection[C]//Proc of seventh international conference on computational intelligence and security. [s. l.]:[s. n.],2011.
- [7] Burguera I, Zurutuza U, Nadjm-Tehrani S. Crowdroid: Behavior-based malware detection system for Android[C]//Proceedings of the 1st ACM workshop on security and privacy in smartphones and mobile devices. New York:[s. n.],2011.
- [8] Felt A P, Finifter M, Chin E, et al. A survey of mobile malware in the wild[C]//Proceedings of the 1st ACM workshop on security and privacy in smartphones and mobile devices. New York:[s. n.],2011.
- [9] Felt A P, Greenwood K, Wagner D. The effectiveness of application permissions[C]//Proc of USENIX WebApps. [s. l.]:[s. n.],2011.
- [10] 路程. Android 平台恶意软件检测系统的设计与实现[D]. 北京:北京邮电大学,2012.
- [11] Han K S, Kang B. Malware classification using instruction frequencies[C]//Proc of ACM symposium on research in applied computation. [s. l.]:[s. n.],2011.
- [12] Firdausi I. Analysis of machine learning techniques used in behavior-based malware detection[C]//Proc of advances in computing, control and telecommunication technologies. [s. l.]:[s. n.],2010.

(上接第 148 页)

论还存在着不足之处,这将作为下一步工作的重点。并针对大规模分布式应用的特殊需求,进一步优化、扩展该方案,使得该方案能够在大规模分布式应用中,在安全性与效率上有更好的表现。

参考文献:

- [1] 宁葵. 访问控制安全技术及应用[M]. 北京:电子工业出版社,2005.
- [2] 王连强,张剑,吕述望,等. 一种基于密码的层次访问控制方案及其分析[J]. 计算机工程与应用,2005,41(33):7-10.
- [3] 陈原,王育民,肖国镇. 公钥密码体制与选择密文安全性[J]. 西安电子科技大学学报(自然科学版),2004,31(1):135-139.
- [4] 王圣宝,曹珍富,董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报,2007,30(10):1842-1852.
- [5] 曾梦歧,卿昱,谭平璋,等. 基于身份的加密体制研究综述[J]. 计算机应用研究,2010,27(1):27-31.
- [6] 苏金树,曹丹,王小峰,等. 属性基加密机制[J]. 软件学报,2011,22(6):1299-1315.
- [7] 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. Alexandria, VA, USA:[s. n.],2006:89-98.

- [8] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//Proc of IEEE symposium on security and privacy. Oakland, California, USA:[s. n.],2007:321-334.
- [9] ITU-T Rec. X509(2000)|ISO/IEC 9594-8:2000, The Directory; Public-key and attribute certificate framework[S/OL]. 2000. <http://www.iso.org/iso/store.htm>.
- [10] ITU-T Rec. X509(2005)|ISO/IEC 9594-8:2005, The Directory; Public-key and attribute certificate framework[S/OL]. 2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43793.
- [11] 中华人民共和国信息产业部. GB/T 16264.8-2005, 信息技术开放系统互连目录第 8 部分:公钥和属性证书框架[S]. 北京:中国标准出版社,2005.
- [12] OASIS Standard, eXtensible Access Control Markup Language (XACML) Version 2.0[S/OL]. 2005. <http://www.oasis-open.org/committees/xacml>.

基于CP-ABE访问控制系统的设计与实现

作者:

[周彦萍, 马艳东, ZHOU Yan-ping, MA Yan-dong](#)

作者单位:

[周彦萍, ZHOU Yan-ping\(河北省科学院 应用数学研究所, 河北 石家庄 050081; 河北省信息安全认证工程技术研究中心, 河北 石家庄 050081\), \[马艳东, MA Yan-dong\\(石家庄开发区冀科双实科技公司, 河北 石家庄, 050081\\)\]\(#\)](#)

刊名:

[计算机技术与发展](#)

ISTIC

英文刊名:

[Computer Technology and Development](#)

年, 卷(期):

[2014\(2\)](#)

本文链接: http://d.wanfangdata.com.cn/Periodical_wjfz201402036.aspx