基于属性加密的气象云数据访问控制策略研究

方忠进[1,2,3] 夏志华[1,3] 周 舒[1,3]

(南京信息工程大学计算机与软件学院 南京 210044)[1] (南京信息工程大学滨江学院 南京 210044)[2]

(南京信息工程大学江苏省网络监控工程中心 南京 210044)[3]

摘 要 随着气象业务水平的不断提高,气象数据的云存储和即时共享问题也日益突出。针对云计算环境下气象数据存储与共享面临的身份认证和访问控制问题,提出了一种基于多方授权的属性加密的访问控制模型。该模型采用一种适合云环境下大数据的属性加密方案,解决了气象部门用户多类性情况下的资料细粒度访问控制问题,同时引入全局ID概念和多方授权机制,解决了不同机构用户在气象部门各资料存储机构间的访问权限问题。系统具有较高的安全性和良好的实用价值。

关键词 属性加密,气象数据,访问控制,细粒度

中图法分类号 TP391.4 **文献标识码** A

Research on Access Control Policy of Meteorological Cloud Data with Attribute-based Encryption

FANG Zhong-jin[1,2,3] XIA Zhi-hua[1,3] ZHOU Shu[1,3]

(School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing 210044, China)[1]

(Binjiang College, Nanjing University of Information Science & Technology, Nanjing 210044, China)[2]

(Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing 210044, China)[3]

Abstract The problems of meteorological cloud data storage and sharing have become increasingly serious with the increasing of meteorological services level. An access control model with multi-authority attribute-based encryption(ABE) was proposed against the problems of authentication and access control of meteorological cloud data storage and sharing. An attribute-based encryption scheme which is suitable for big data cloud environment is applied to solve the fine-grained data access control problems in case of multi-class users in meteorological department. The introduction of global ID and multi-authorization mechanism solves the access problem of different institutional users in different data storage departments. The system has high security and good practical value.

Keywords Attribute-based encryption, Meteorological data, Access control, Fine-grained

1 引言

随着中国气象业务现代化水平的不断提高,海量气象数据的存储、处理与利用给气象部门带来了全新的挑战。为了能够应对气象信息的海量存储和即时共享等问题,必须将技术与服务进行融合,将云计算应用落实到气象研究的信息化建设和应用中。目前国家气象信息管理部门利用高性能计算机网络系统,结合基本气象资料共享服务平台和在建的多种气象数据共享分系统组成分布式气象科学数据共享网络体系进行信息共享服务。这些模式仍然采用传统的用户管理模式,一用户一密钥,无法实现气象数据的精细化共享管理。

云计算环境下,气象数据管理面临身份认证和访问控制的安全问题[9],由于鉴别的措施太弱,导致数据或者存储的信息可能会被假冒和窃取。针对此问题,加密仍然是身份认证和访问控制领域的热点研究课题。近几年来,国内外研究者陆续提出了一系列的加密方案,如基于公钥的加密方案、透明加密方案、基于身份的加密方案[5]和基于属性的加密方案[1,4,6]等。1984年,Shamir提出了基于身份的加密(IBE)思想,其特点是利用用户的身份信息作为用户的公钥,因此该加密方案不需要数字证书,避免了传统公钥密码系统建立和管理的困难。用户的身份主要由其属性信息决定,因此,近些年来在身份基加密基础之上,Sahai和Waters等人提出了属性基加密机制(ABE),实现了基于属性的加解密。为了更加灵活地表示访问策略,学者们进一步提出了密钥-策略ABE(KP-ABE)和密文-策略ABE(CP-ABE)。ABE机制是非常复杂的,其复杂性也导致其本身存在一些需要解决的问题:1)公钥设计和策略设计的复杂性相关,访问结构较难设计;2)密钥与属性相关,属性的动态性增加了密钥撤销难度;3)分布式应用的多机构协作需求也对ABE的设计提出了挑战。

本文依据云计算环境下的气象数据管理特点,采用多方

到稿日期:2013-03-20 返修日期:2013-05-28 本文受国家自然科学基金(61173141),江苏省普通高校研究生科研创新计划项目(CXZZ12_0512),江苏省网络监控工程中心开放基金课题项目(KJR1106),江苏高校优势学科建设工程项目资助。

方忠进(1979—),男,博士生,讲师,主要研究方向为网络信息安全、云安全,E-mail:nuist@163.com;夏志华(1983—),男,博士,讲师,主要研究方向为信息安全、隐写分析;周 舒(1984—),女,硕士,助理研究员,主要研究方向为信息安全。

授权的密文策略属性加密(CP-ABE)方案，利用一系列的属性信息描述用户的身份，构建信息访问控制策略，从而既保护了用户隐私，又可以防止用户间的合谋攻击，保证了数据的机密性。本方案在气象信息共享细粒度访问控制领域具有良好的应用前景，有利于实现气象部门间和面向社会的气象信息高效共享和气象云平台的安全运行。

2 基于属性加密的访问控制模型设计

本节通过分析云环境下的气象数据服务对象的特征，对现有的属性加密机制进行分析，采用用户属性与全局身份(GID)绑定的方法，提高多方授权方案的易实现性和可操作性，建立适合云环境下气象数据管理模式的访问控制模型，使其能够更好地满足气象数据共享的多级、细粒度实际应用需求。模型建立过程如下(见图 1)：

1)初始化：气象数据管理部门设置全局参数并生成系统公钥和私钥。

2)密钥生成：每个气象数据管理部门为其管理的用户属性和 GID 对生成密钥。

3)设置访问结构：由数据管理工作人员利用属性集为不同文件设置访问策略并加密文件。

4)用户访问：不同授权机构的用户提供个人私钥和 GID 进行身份认证后，管理方分析用户的属性信息，进而生成可访问的文件结构。用户根据需要查看或复制数据。

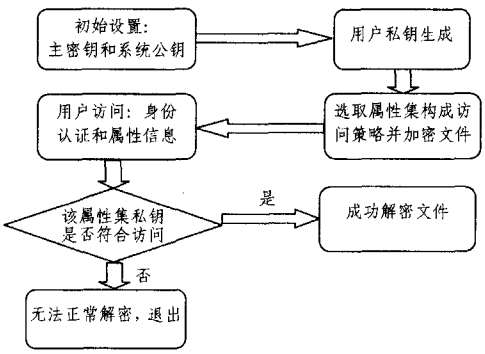

图 1 基于属性加密的访问控制模型

3 多方授权属性加密方案

本节给出了多方授权属性基加密的必备知识，并对方案的实现过程进行了描述，同时说明了该方案的特点。为了进一步阐明本方案的可用性，在本节最后对方案的安全性进行了分析。

3.1 定义

定义 1(访问结构) 假设$\{P_1,P_2,\cdots,P_n\}$是数据参与各方的集合，对于包含于集合 $P=2^{\{P_1,P_2,\cdots,P_n\}}$的集合 A，如果存在 B、C 满足以下条件，则 A 是单调的：$B\in A$ 并且 $B\subseteq C$，则 $C\in A$。访问结构 A 是集合$\{P_1,P_2,\cdots,P_n\}$的非空子集，即 $A\subseteq P\backslash\{\phi\}$。如果一个集合在 A 内，则称之为授权集，否则为非授权集。

在该方案中，参与各方的角色是由属性确定的。因此，访问结构 A 将包含属性的授权集。在下文中提到的访问结构都是单调的访问结构。

定义 2(双线性对) 设 G_1、G_2 和 G_T 是大素数阶 p 的 3 个循环群，双线性映射 e 为：$G_1\times G_2\rightarrow G_T$，其包含的性质如下：

(1)双线性，即对所有的 $g_1\in G_1$，$g_2\in G_2$，同时 $a,b\in Z_p^*$，有 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

(2)非退化性，即 $e(g_1,g_2)\neq 1$。

(3)可计算性，即对于任意的 $g_1\in G_1$，$g_2\in G_2$，存在一个有效的算法计算 $e(g_1,g_2)$。

定义 3(BDH 判定假设) 假设挑战者随机选择 $a,b,c\in Z_p^*$，且 $g_1\in G_1$，$g_2\in G_2$，BDH 判定假设就是指不存在攻击者在多项式时间内有不可忽略的优势将元组$(A=g_2^a,B=g_2^b,C=g_2^c,e(g_1,g_2)^{abc})$和$(A=g_2^a,B=g_2^b,C=g_2^c,e(g_1,g_2)^z)$进行区分。

3.2 基本结构

支持多方授权的 CP-ABE 方案包含的内容如下：

(1)全局初始化 *GloSetup*：算法根据输入的安全参数 λ 输出全局参数 GP。

(2)系统初始化 *Setup*：输入全局参数 GP，输出各授权机构的公共密钥 PK 和私钥 SK。

(3)密钥生成 *KeyGen*：输入 GID、全局参数 GP、属于授权机构的属性 i 和 SK，算法为每个属性、身份对输出一个密钥 $K_{i,GID}$。

(4)加密 *Encrypt*：输入公共密钥组$\{PK\}$、消息 M、访问矩阵(A,ρ)和公共参数 GP，输出密文 CT，只有满足访问结构的用户才能解密该密文。

(5)解密 *Decrypt*：输入包含访问矩阵的密文 CT、公共参数 GP 和用户的属性、身份对密钥组$\{K_{i,GID}\}$，当属性 i 满足访问矩阵条件时，算法解密输出 M。

3.3 方案实现

(1)全局初始化 $GloSetup(\lambda)$

G 为一个阶为 $N=p_1p_2p_3$ 的双线性群，全局参数 GP 包含 N 和 G_{p1} 的生成元 g_1。哈希函数 $H:\{0,1\}^*\rightarrow G$，其功能是将全局 GID 映射为 G 中的元素。

(2)系统初始化 $Setup(GP)$

对于每个属于授权机构的属性 i，授权机构随机选择两个参数 $\alpha_i,y_i\in Z_n$，输出公共密钥 $PK_j=\{e(g_1,g_1)^{\alpha_i},g_1^{y_i}\ \forall i\}$ 和私钥 $SK=\{\alpha_i,y_i\ \forall i\}$。

(3)密钥生成 $KeyGen(GID,i,SK,GP)$

输入 GID、属于一个授权机构的属性 i、授权机构私钥 SK 和公共参数 GP，算法为每个用户属性、身份对输出密钥 $K_{i,GID}=g_1^{\alpha_i}H(GID)^{y_i}$。

(4)加密 $Encrypt(M,(A,\rho),GP,\{PK\})$

输入消息 M、$n\times l$ 的访问矩阵 A(ρ 将行映射为属性)、全局参数 GP、公共密钥组$\{PK\}$。算法选择随机的 $s\in Z_n$，随机矢量 $v\in Z_n^l$(s 为其第一项)，λ_x 表示 $A_x\cdot v$(A_x 表示 A 的第 x 行)，选择随机矢量 $w\in Z_N^l$(0 为其第一项)，ω_x 表示 $A_x\cdot w$。对于 A 的每一行，算法随机选择 $r_x\in Z_n$，输出密文 CT 表示如下：$C_0=Me(g_1,g_1)^s$，$C_{1,x}=e(g_1,g_1)^{\lambda_x}e(g_1,g_1)^{\alpha\rho(x)r_x}$，$C_{2,x}=g_1^{r_x}$，$C_{3,x}=g_1^{y\rho(x)r_x}g_1^{\omega_x}\ \forall x$。

(5)解密 $Decrypt(CT,\{K_{i,GID}\},GP)$

输入包含访问矩阵的密文 CT、公共参数 GP 和用户的属性、身份对密钥组$\{K_{i,GID}\}$，算法执行过程如下：

$C_{1,x}\cdot e(H(GID),C_{3,x})/e(K_{\rho(x)},GID,C_{2,x})=e(g_1,g_1)^{\lambda_x}e(H(GID),g_1)^{\omega_x}$，算法选择常数 $c_x\in Z_N$，满足$\sum_x c_xA_x$

$=(1,0,\cdots,0)$，计算 $\prod_x (e(g_1,g_1)^{\lambda_x} e(H(GID),g_1)^{\omega_x})^{c_x} = e(g_1,g_1)^s$，其中 $\lambda_x = A_x \cdot v, \omega_x = A_x \cdot w, v \cdot (1,0,\cdots,0) = s$，$w \cdot (1,0,\cdots,0) = 0$，则可获得明文 $M = C_0 / e(g_1,g_1)^s$。

3.4 方案特点

(1)功能完善

因为加密方法使用了以前已经有的 ABE 系统，本系统可以达到与之前系统相同的安全表现，同时可以根据任一布尔表达式设计属性策略。任何一方都可以创建和发布与本部门管理的属性相关的验证密钥来成为一个分授权机构。系统需要分授权机构间的合作很少，在正常情况下，不同的授权机构间不需要合作，甚至不需要觉察到对方。

(2)可信度高

中央授权机构的存在，在传统的属性基加密中可能被认为是缺点。但在本系统中，中国气象局气象信息中心作为中央授权机构的存在是必要的，符合目前气象部门数据的实际管理模式。在实际管理中，气象部门中央机构拥有最高权限和可信性，可以很好地验证分授权机构的合法性，并保障授权的安全性。

(3)安全性好

全局 ID 的引入使得用户具有了一个全局统一的身份，并通过哈希函数将每个 ID 映射为双线性群元素 $H(GID)$，将用户分属于不同分授权机构的属性相关 keys 捆绑到一起使其成为一个有机整体以应对用户间的合谋攻击。同时用户的全局 ID 是唯一的，因此即使在后续管理过程中，中央授权机构偶尔出现故障，本系统也能够正常运行。

(4)方便灵活

在整个属性基加密方案中，由于各个分授权中心管理自己的属性并各自维持自己的属性私钥和机构标识，因此，每个密钥分配中心都可以分别分发属于自己的属性相关的私钥。新属性产生时，可以方便地加入到分授权机构的属性集，系统整体参数不需要改变。同时，如果有一个新的属性分配机构加入到系统中，也不需要更新系统参数，只需要调用密钥生成算法 *KeyGen* 来建立该用户属性和全局 ID 相关的属性、身份对密钥 $K_{i,GID}$ 即可，同时不需要与其他已经存在的属性机构进行交互。

3.5 安全性分析

本算法利用 GID 解决了位于不同机构内的用户直接攻击和合谋攻击的问题。通过使用 GID 将不同属性绑定到一起，使用 $e(g_1,g_1)^s$ 使 M 致盲（g_1 是 G_{p1} 的生成元，s 是 Z_n 中的随机取值），值 s 和 0 分别被封装成由 λ_x 和 ω_x 组成的表达式，解密者必须引入 $e(H(GID),g_1)^{\omega_x}$，使用属性、身份对$(i,$ GID$)$等匹配密钥才能够恢复得到 s。以下通过解密过程进行分析。

步骤 1　计算 $C_{1,x} \cdot e(H(GID),C_{3,x}) / e(K_{\rho(x),GID}, C_{2,x})$，其中 $C_{1,x} = e(g_1,g_1)^{\lambda_x} e(g_1,g_1)^{\alpha_{\rho(x)} r_x}$，$C_{2,x} = g_1^{r_x}$，$C_{3,x} = g_1^{y_{\rho(x)} r_x} g_1^{\omega_x}$。如果用户属性在访问策略中，则 $\rho(x)$ 映射为属性 i，否则不做映射。假设用户属性可以映射，则

原式

$$= \frac{e(g_1,g_1)^{\lambda_x} e(g_1,g_1)^{\alpha_{\rho(x)} r_x} \cdot e(H(GID),g_1^{y_{\rho(x)} r_x} g_1^{\omega_x})}{e(g_1^{\alpha_i} H(GID)^{y_i}, g_1^{r_x})}$$

$$= \frac{e(g_1,g_1)^{\lambda_x} e(g_1,g_1)^{\alpha_i r_x} \cdot e(H(GID),g_1)^{y_i r_x} \cdot e(H(GID),g_1)^{\omega_x}}{e(g_1,g_1)^{\alpha_i r_x} \cdot e(H(GID),g_1)^{y_i r_x}}$$

$$= e(g_1,g_1)^{\lambda_x} \cdot e(H(GID),g_1)^{\omega_x}$$

在这一步骤中，由于计算是针对单个属性进行的，因此不论属性是否属于同一个 *GID*，都可以得出结果，只是结果的值不同，例如对于用户 *GID* 和 *GID′* 得到的结果分别为 $e(g_1,g_1)^{\lambda_x} \cdot e(H(GID),g_1)^{\omega_x}$ 和 $e(g_1,g_1)^{\lambda_x} \cdot e(H(GID'),g_1)^{\omega_x}$。

步骤 2　计算 $\prod_x (e(g_1,g_1)^{\lambda_x} e(H(GID),g_1)^{\omega_x})^{c_x}$，其中 $\lambda_x = A_x \cdot v, \omega_x = A_x \cdot w$，常数 $c_x \in Z_N$，满足 $\sum_x c_x A_x = (1,0,\cdots,0)$，则

原式 $= \prod_x (e(g_1,g_1)^{A_x \cdot v} e(H(GID),g_1)^{A_x \cdot w})^{c_x}$

如果表达式中所有用户属性属于同一个用户，则在上式连乘运算中 $e(H(GID),g_1)^{A_x \cdot w})^{c_x}$ 拥有相同的底，则原式 $= e(g_1,g_1)^{\sum c_x \cdot A_x \cdot v} e(H(GID),g_1)^{\sum c_x \cdot A_x \cdot w}$，由于 $v \cdot (1,0,\cdots,0) = s, w \cdot (1,0,\cdots,0) = 0$，原式 $= e(g_1,g_1)^s$。

如果出现用户利用属性合谋参与解密，则由于 *GID* 不同，属于不同用户的属性 x 会出现 $\prod_x (e(g_1,g_1)^{A_x \cdot v} e(H(GID),g_1)^{A_x \cdot w})^{c_x} \cdot \prod_x (e(g_1,g_1)^{A_x \cdot v} e(H(GID'),g_1)^{A_x \cdot w})^{c_x}$，由于 $e(H(GID),g_1)^{A_x \cdot w \cdot c_x}$ 和 $e(H(GID'),g_1)^{A_x \cdot w \cdot c_x}$ 底不相同，不能进行合并，也就无法得到 $e(g_1,g_1)^s$。

步骤 3　$M = c_0 / e(g_1,g_1)^s$。

在 $e(g_1,g_1)^s$ 正确的情况下，通过计算可以将密文与致盲元素相除得到明文。

通过上述分析，不管是同一授权机构内的用户还是不同授权机构间的用户，如果希望进行合谋来获得明文都是不可能的。因为在无密钥的情况下解密密文 *CT*，则需要知道 $e(g_1,g_1)^s$，而由于参与计算用户的 *GID* 不同，解密时 $e(g_1,g_1)^s$ 无法通过计算得出。而对于合谋攻击者（如 *GID* 和 *GID′*）来说，想要通过共有属性满足 (A,ρ) 矩阵规则来获得明文信息也是不可能的，因为对于表达式 $\prod_x (e(g_1,g_1)^{\lambda_x} e(H(GID),g_1)^{\omega_x})^{c_x} = e(g_1,g_1)^s$ 来说，其组成部分分别为 $e(H(GID),g_1)^{\omega_x}$ 和 $e(H(GID'),g_1)^{\omega_x}$，$\omega_x$ 拥有不同的底，其值不可能相同，解密模块无法计算出正确的结果。

4　系统模拟

本系统采用 XenServer 构建模拟气象云数据中心作为实验平台，并使用各类真实的气象数据作为服务数据，并建立终端客户节点、中央机构节点和分机构节点，使得实验平台的环境尽可能接近于实际的气象云数据中心服务环境。在模拟环境中，各个节点承担着属性加密方案中不同实体的角色，分别介绍如下：

(1)中央机构节点。在云数据属性加密系统中，需要专门设置一台虚拟机承担类似于气象部门信息中心角色的中央机构节点，负责运行 GloSetup 算法，通过输入必须的参数后输出全局参数。参数生成以后，中央节点的任务就转到 *Encrypt* 算法，负责运算量巨大的文件加密阶段的工作。除了以上功能外，中央机构节点也有授权权限，承担和分机构节点一样的工作。在终端客户节点访问时负责分析用户属性，并执行 *Decrypt* 算法。

(2)分机构节点。分授权机构节点负责运行系统初始化

（下转第 228 页）

quent itemsetalgorithm[J]. IEEE Transactions on Knowledge and Data Engineering,2005,17(11):1490-1504

[3] Gouda K, Zaki M J. Efficiently mining maximal frequent itemsets[C]// Proceedings of the 2001 IEEE International Conference on Data Mining. San Jose,2001:163-170

[4] 吉根林,杨明,宋余庆,等.最大频繁项目集的快速更新[J].计算机学报,2005,28(1):128-135

[5] Uno T,Kiyomi M,Arimura H. LCM ver. 2:Efficient mining algorithms for frequent/closed/maximal itemsets[C]// Proceedings of the 2004 IEEE ICDM Workshop on Frequent Itemset Mining Implementations. Brighton,2004:1-11

[6] Uno T,Kiyomi M,Arimura H. Lcm ver. 3:Collaboration of array,bitmap and prefix tree for frequent itemset mining[C]// Proceedings of the 1st International Workshop on Open Source Data Mining:Frequent Pattern Mining Implementations. New York,2005,77-86

[7] Grahne G,Zhu J. High performance mining of maximal frequent itemsets[C]// Proceedings of the 6th International Workshop on High Performance Data Mining. 2003:1-10

[8] Grahne G, Zhu J. Efficiently using prefix-trees in mining frequent itemsets[C]// Proceedings of the Third FIMI Workshop on Frequent Itemset Mining Implementations. Florida, 2003:123-132

[9] Goethals B,Zaki M J. Advances in frequent itemset mining implementations:report on FIMI'03[J]. ACM SIGKDD Explorations Newsletter,2004,6(1):109-117

[10] Han J,Pei J,Yin Y. Mining frequent patterns without candidate generation[J]. ACM SIGMOD Record,2000,29(2):1-12

[11] 牛新征,佘堃. 面向大规模数据的快速并行聚类划分算法研究[J].计算机科学,2012,39(1):134-137

(上接第 207 页)

Setup 算法,通过获得中央节点分发的全局参数 GP,生成各节点的公钥组和私钥组,并根据输入的 GID 值,为属于本授权机构的每个用户属性、身份对输出密钥 $K_{i,GID}$。

(3)终端客户节点。客户节点拥有分属于不同分机构节点的属性,访问数据时通过登录提交相应的属性,并提交密钥 $K_{i,GID}$,若属性符合访问矩阵则可获得所需的数据明文。

结束语 本文将属性加密机制应用到气象云数据的管理研究中,给出了一种基于多方授权的属性加密的访问控制模型。通过引入多方授权方案,很好地解决了实际使用中需要有多个授权机构情况下的文件共享访问问题,同时通过引入系统用户全局唯一的身份标识 GID 来有效避免不同用户间的合谋攻击问题。因此,本系统方案具有较高的安全性和很好的实用价值。

参 考 文 献

[1] Hur J,Noh D K. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems[J]. IEEE Transactions on Parallel and Distributed Systems,2011,22(7)

[2] Yang Ming. An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control[C]//2011 International Conference on Instrumentation, Measurement, Computer,Communication and Control. 2011

[3] Jia Hong-yong. Efficient and Scalable Multicast Key Management Using Attribute Based Encryption[C]// 2010 International Conference on Information Theory and Information Security. 2010

[4] 苏金树,曹丹,王小峰,等.属性基加密机制[J].软件学报,2011,22(6)

[5] Subashini S,Kavitha V. A survey on security issues in service delivery models of cloud computing[J]. Journal of Network and Computer Applications,2011,34

[6] 张磊,曹珍富.一个适合分布式网络的属性基加密方案[J].上海交通大学学报,2010,44(11)

[7] 陈勤,党正芹,张金漫,等.一种多认证机构可验证的属性基加密方案[J].计算机应用研究,2012,29(1)

[8] Liu Yu-chao. A Method for Trust Management in Cloud Computing:Data Coloring by Cloud Watermarking[J]. International Journal of Automation and Computing,2011,8(3)

[9] Sakr S,Liu A. A Survey of Large Scale Data Management Approaches in Cloud Environments[J]. IEEE Communications Surveys & Tutorials,2011,13(3)

[10] Yu Shu-cheng, Wang Cong. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing[C]// IEEE INFOCOM. 2010

[11] Zissis D,Lekkas D. Addressing cloud computing security issues[J]. Future Generation Computer Systems,2012,28(3)

[12] Hay B, Nance K, Bishop M. Storm Clouds Rising: Security Challenges for IaaS Cloud Computing[C]//Proceedings of the 44th Hawaii International Conference on System Sciences. 2011

[13] Rodero-Merino L. Building safe PaaS clouds:A survey on security in multitenant software platforms[J]. Computers & Security, 2012,31

[14] Blandford R. Information security in the cloud[M]. Network Security,April 2011

[15] Walters R. Managing privileged user activity in the datacentre [M]. Network Security,November 2010

[16] Zhuo Hao. A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability[J]. IEEE Transactions on knowledge and data engineering,2011,23(9)

[17] Jia Wei-wei. SDSM:A Secure Data Service Mechanism in Mobile Cloud Computing[C]// The First International Workshop on Security in Computers,Networking and Communications. 2011

[18] Pearson S, Mont M C. Sticky Policies: An Approach for Managing Privacy across Multiple Parties[J]. Computer, 2011, 44(9):60-68

[19] Garber L. Serious Security Flaws Identified in Cloud Systems [J]. Computer,2011,44(12):21-23

[20] Song D,Shi E,Fischer I. Cloud Data Protection for the Masses [J]. Computer,2012,45(1):39-45