DOI:10.13413/j.cnki.jdxblxb.2011.04.004

基于信任服务IBE体系的权限管理

胡 亮,贺瑞莲,袁 巍,初剑峰
(吉林大学 计算机科学与技术学院,长春 130012)

摘要: 针对现有的基于身份加密(identity based encryption,IBE)体系中缺乏权限管理问题,提出一种基于信任服务IBE体系下的权限管理方案. 该方案采用门限的思想和算法对服务进行集中管理,并结合基于角色的访问控制管理权限,实现了细粒度的权限管理. 采用信任继承的思想为用户分配角色,并采用集中审计的思想维护系统,提高了系统的可靠性.

关键词: 计算机系统结构; 权限管理; 基于身份的加密; 门限; 信任继承; 集中审计
中图分类号: TP309.7 **文献标志码:** A **文章编号:** 1671-5489(2011)04-0703-10

Privilege Management of IBE System Based on Trust Service

HU Liang, HE Rui-lian, YUAN Wei, CHU Jian-feng
(*College of Computer Science and Technology, Jilin University, Changchun* 130012, *China*)

Abstract: The problem lacking privilege management still exits in the identity based encryption system. To solve this problem, a new scheme of the privilege management mechanism of identity based encryption system was put forward, which is named privilege management of identity based encryption system based on trust service. In the scheme, the idea and algorithm of the threshold are used to manage the services of the domain. Trust inheritance is applied in the researches of privilege management mechanism to assign roles to users. The privilege management mechanism also uses concentration audit to maintain system reliability.

Key words: computer system organization; privilege management; identity based encryption; threshold; trust inheritance; concentration audit

随着网络环境中信息系统规模的不断扩大、业务逻辑的复杂化以及信息资源的分布存储,传统的网络安全技术已经不适应新的网络需求,可信网络[1-2]的建立成为发展趋势. 如何保证系统中的资源既能被值得信赖的用户访问,又要防止非法用户的破坏和入侵,身份认证和权限管理是解决这类信息安全问题的重要环节[3-4].

Shamir[5]提出一种可以用任意字符串作为公共密钥的公钥加密方案. Boneh等[6]和Cocks[7]分别提出一种实用的IBE(identity-based ecryption,基于身份的加密)系统. IBE技术通过将用户公开的字符串信息(如邮件地址等)作为公钥的加密方式,为用户的身份认证提供了有效方法. 现有的IBE系统虽然在签名[8]、签密[9]、加密[10-11]、架构[12]、密钥的生成与分发[13]、认证[14]等多方面进行了改进,但IBE系统的服务仍不完善. 例如,在现有的IBE系统中只提供了用户的身份认证,而对于可信用户可以访

收稿日期: 2010-06-07.

作者简介: 胡 亮(1968—),男,汉族,博士,教授,博士生导师,从事网格计算与网络安全的研究,E-mail: hul@jlu.edu.cn.
通讯作者: 贺瑞莲(1986—),女,汉族,硕士研究生,从事网络与信息安全的研究,E-mail: heruilian1986@126.com.

基金项目: 国家自然科学基金(批准号: 60873235; 60473099)、国家重点基础研究发展计划973项目基金(批准号: 2009CB320706)、教育部新世纪优秀人才支持计划项目(批准号: NCET-06-0300)、吉林省重点科研项目(批准号: 20080318)和吉林大学研究生创新基金(批准号: 20080244).

问哪些服务没有任何管理与限制. 如果经过身份认证的可信用户可以访问可信域内任何服务，则系统的保密性和完整性就存在问题.

因此，为了更好地完善 IBE 体系，本文基于信任服务的 IBE 体系[15]，讨论了基于信任服务 IBE 体系下的权限管理机制. 结合 IBE 体系与基于角色的访问控制(role based access control，RBAC)[16-18]各自的优势，提出一种 IBE 体系下的权限管理机制，较好解决了域内服务的注册、可信用户的权限分配及访问判定等问题. 其中，信任继承实现了灵活的权限分配，门限访问控制规则实现了细粒度的权限管理，集中审计负责维护用户的信任度及系统日志，提高了系统的可用性，并为责任追究提供依据.

1 基于信任服务 IBE 体系模型

基于信任服务的 IBE 体系模型如图 1 所示，主要由标识管理机制、密钥管理机制、权限管理机制和域间互联机制组成. 其中标识管理机制主要实现用户注册信息的管理及统一身份的标识管理；密钥管理机制主要实现密钥的生成与分发及主密钥的定时更新[19]；权限管理机制主要实现域内服务和用户权限的管理；域间互联机制主要实现域间可信身份的移动及不同域之间的互相通信[20].

该模型的工作机理如下:

1) 当标识管理机制接收到一个用户的登陆申请后，首先验证用户的合法性，然后发放一次性数字签名，最后记录该用户的其他特征信息. 2) 标识管理机制分别向密钥管理、域间互联、权限管理机制注册该用户的一次性签名、标识、IP 地址等特征信息. 3) 向用户返回可以使用信任体系下相应服务的信息. 4) 当用户使用域内的某个服务时，权限管理机制先审核该用户是否有权限使用该服务. 如果该用户有权限使用，则权限管理机制将该用户的特征信息和标识管理机制所发放的一次性数字签名发送给服务. 该服务再使用用户的特征信息和一次性数字签名为对称密钥对数据报 AES 加密，与用户通信. 5) 当标识管理机制接收到一个合法用户的安全退出申请时，标识管理机制先向密钥管理、域间互联、权限管理机制注销该用户，然后权限管理机制再删除所有关于该用户的权限信息，更新权限管理机制中的数据.

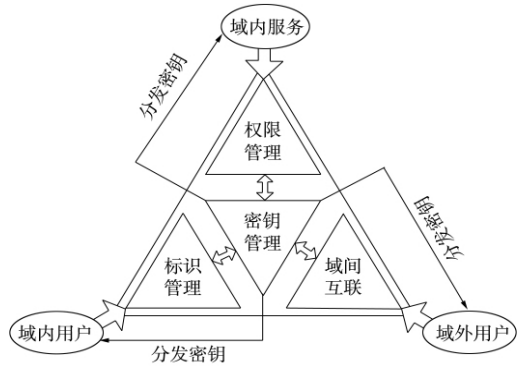

图 1 基于信任服务的 IBE 模型

Fig. 1 Model of IBE system based on trust service

由此可见，基于信任服务的 IBE 体系通过密钥管理机制、标识管理机制、权限管理机制和域间互联机制 4 个模块形成了一个信任服务区，权限管理机制只信任域内的密钥管理、标识管理和域间互联机制，它们之间的通信采用可信的紧耦合方式，权限管理机制只向其信任的密钥管理、标识管理、域间互联机制和域内可信的用户和服务发放权限.

本文研究基于信任服务 IBE 体系下的权限管理机制，该机制是信任体系内的合法用户提交具体服务请求时，信任体系提供的一种安全策略. 权限管理机制主要是为保证域内的可信用户能合理使用域内的服务和资源，实现体系的安全粒度细化. 此外，权限管理机制负责对注册服务的管理，是责任追究的支撑系统之一.

2 权限管理机制模型

2.1 体系结构

由于 IBE 体系采用集中式的密钥管理方式，所以更适用于要求基于公钥体系下的服务及数据报可以定时销毁的电子政务和电子军务领域. 因此，本文根据电子政务和电子军务领域等级分明的特点设计权限管理机制的结构模型，如图 2 所示.

该模型由访问者、服务、策略实施点(policy executed point，PEP)、策略决策点(policy decision point，PDP)、权限分配器(privilege assignment，PA)、LDAP 数据库以及审计 7 部分组成.

模型的组成要素及其语义如下：

1）访问者（user）：发起访问请求的用户. 2）服务（service）：权限管理机制所保护的对象. 3）策略实施点（PEP）：用于接受用户的访问请求，根据标识管理机制给出的用户身份信息、要访问的服务信息及访问动作和相关信息生成授权决策请求信息，然后向策略决策点发出决策请求，并接收决策结果. 决策过程对用户透明，用户看不到决策过程. 4）策略决策点（PDP）：即访问控制模块，用于判断用户是否有权限访问服务. 接收决策请求信息，检索策略规则，计算用户的权限，查找服务门限表，根据决策请求信息、用户权限、服务门限表和策略规则做出决策，将决策结果返回给策略实施点. 5）权限分配器（PA）：用于权限的分配. 权限分配器根据策略为服务划分权限区及为各个权限区分配门限，为角色分配权限值，为用户分配角色，并将结果存入 LDAP 数据库中. 其中策略是根据应用机构的安全要求、服务的特征信息、用户的身份及其属性信息制定. 6）LDAP 数据库：用于存放用户身份信息、服务信息、角色信息及权限信息. 7）审计（audit）：用于记录用户的行为和对服务的访问活动. 当出现问题时用于检测问题出现的原因，并维护权限管理机制.

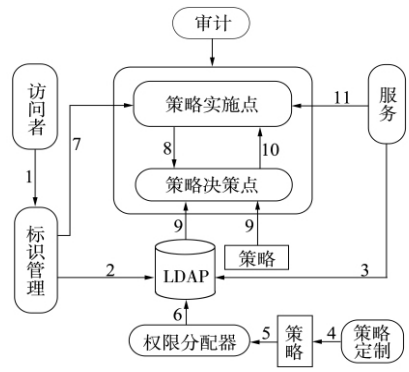

图 2　权限管理模型

Fig. 2　Model of privilege management

2.2　工作流程

权限管理机制模型工作流程如下：

1）用户登录时，标识管理机制验证用户的合法性，然后发放一次性数字签名，并且记录该用户的其他特征信息.

2）标识管理机制向权限管理机制等注册该用户的一次性签名、标识、IP 地址等特征信息；权限管理机制将用户的所有信息存入 LDAP 数据库.

3）服务注册. 当有一个新的服务开通时，权限管理机制将服务的特征信息存入 LDAP 数据库，给服务注册一个标识.

4）根据应用机构的实际情况及安全需求定制权限管理机制的授权策略. 包括服务划分策略、角色定义策略、角色权限分配策略、用户角色分配策略及角色间的约束.

5）安全管理员根据策略划分服务的权限区及根据权限区的层次关系为每个权限区设定门限值；根据角色定义，权限分配器为每个角色分配权限值；根据策略、用户身份和属性信息为用户分配角色. 启动策略实施点，使用指定的策略和相关信息初始化策略决策服务器.

6）权限分配器将服务门限表、角色权限表及用户角色表存入 LDAP 数据库.

7）标识管理机制将用户的访问请求发送给权限管理机制. 策略实施点接收用户的访问请求，对用户的请求进行解析并重新打包、添加用户身份信息.

8）策略实施点将打包后的访问请求发给策略决策点，驱动策略决策点验证其权限.

9）根据用户的访问请求从 LDAP 数据库中检索，返回用户的权限信息和服务门限表.

10）策略决策点根据策略、用户的权限和服务的门限值对请求进行判断，返回决策结果.

11）策略实施点根据决策结果决定该用户是否可进行访问.

在用户访问过程中，审计模块对用户的访问行为和服务权限分配与决策过程进行记录与监测，当安全管理员的误操作导致越权行为发生时，根据日志查找问题出现的原因，维护权限管理机制.

权限管理机制初始化时分别设置系统管理员、安全管理员及审计管理员 3 个角色. 其中系统管理员负责激活服务、定义和删除角色及创建和注销用户；安全管理员负责策略定制、角色授权和撤销及用户角色的分配和撤销；审计管理员则负责系统中安全日志的管理. 3 个角色间职责分离，符合最小特权原则. 权限管理机制主要解决如何给用户授予合理的权限、如何进行权限判定及如何进行审计维护这 3 个关键问题.

3 服务注册

基于信任服务的IBE体系中，对服务采用集中管理的方式，所有服务必须向权限管理机制进行注册，权限管理机制为每个服务划分权限区并为每个权限区设置门限值.

3.1 服务开通

每个新的服务开通时，都需要向权限管理机制进行注册. 任一域内服务S，其开通过程如下: 1) S首先向权限管理机制提交申请，权限管理机制为S分配唯一的标识obj; 2) S向权限管理机制提交自己的属性特征信息; 3) 系统管理员激活S，使其成为合法服务; 4) 密钥管理机制为S发放私钥.

服务开通后，权限管理机制为服务划分权限区，并为每个权限区设定门限.

3.2 服务权限区的划分

每个权限区是一组操作的集合. 由于每个服务对权限的要求各不相同，因此权限管理机制需要根据服务提交的属性信息，协同服务提供者定制服务的权限区划分策略为每个权限区设置门限值.

权限区划分过程如下:

1) 确认可能使用服务的对象; 2) 根据各类型对象权限范围的不同划分权限区.

权限区的划分规则: (设服务S划分为两个权限区op1和op2，op为S提供所有的操作集合) $(op1 \cap op2 = \emptyset) \vee (op1 \cup op2 = op)$.

服务权限区划分完成后，为每个权限区设定门限值.

3.3 权限区门限

权限区门限值根据权限区的访问策略设置. 设OBS和OPS分别表示服务集和权限区集; 表示自然数集.

定义1(服务门限函数) threshold( ):

theshold(obj: OBS，op: OPS) → //将服务的各个权限区映射到其门限值.

定义2(服务门限的集合) ST: $ST = \{(obj, op, t) \mid obj \in OBS, op \in OPS, t \in \ \}$.

门限设置过程(设S的权限区op1):

1) 根据权限区op1的重要程度确定重要系数k(其中$k \geqslant 1$，且$k \in$)，k也是一个权限片段的权限值. 2) 确定用户访问权限区op1需要满足的最低要求，即访问权限区需要的最大权限片段数. 若只需要一个权限片段，则op1的门限$t = k$; 若需要n个权限片段，则$t = n \cdot k$($n \geqslant 1$，且$n \in$).

权限区的门限值设置完成后，权限管理机制将服务门限集合ST存入LDAP数据库. 以上步骤完成后，服务S正式为用户提供服务. 为了使用户可以合理地访问服务S，需为用户分配权限.

4 权限分配

权限分配[21-22]主要包括3个方面: 1) 定义角色集合ROLES，为角色分配相应的权限; 2) 为用户分配角色; 3) 维护用户-角色表RU、角色-权限表PR.

4.1 角色的权限值

首先根据应用系统的组织结构和服务定义角色. 每个角色代表一个权限的集合，每个服务对应一组角色. 安全管理员为每个角色分配对应权限区的权限值，角色的权限值根据角色权限分配策略分配. 策略是系统初始化时由安全管理员和应用系统的相关管理人员根据应用系统的实际情况制定.

定义3(角色的权限值集合) PV: $PV = \{(obj, op, p) \mid obj \in OBS, op \in OPS, p \in \ \}$，表示在服务S的权限区op中角色的权限值为$p$.

本文用"×"表示笛卡尔乘积，PR表示角色权限列表，则$PR \subseteq PV \times ROLES$是一个从权限值集合到角色集合的多对多映射，表示角色被授予的权限. 设ρ(ROLES)表示角色集合ROLES的幂集，则PR(ρ(ROLES))表示角色集合ρ(ROLES)中每个角色所拥有的权限列表集合.

4.1.1 角色权限分配算法 GrantRolePV(r: ROLES; pv: PV): 表示授予角色r关于服务S权限区op的权限值.

```
GrantRolePV( r: ROLES; pv: PV)
{
if( ∃pv ∈ PR( { r: ROLES} ) )
return;
else
PR = PR ∪ ( r,pv)
}
```

4.1.2　**角色继承**

定义 4(角色继承关系)　RH: RH ⊆ ROLES × ROLES，表示角色与角色间的继承关系，记作 ≥.

若 role_a ≥ role_b，则表示角色 role_a 的权限包含 role_b 的权限，role_a 的用户都是 role_b 的用户.

由于角色间的继承关系存在多重继承的可能性，因此对服务 S 的权限区 op，设安全管理员授予角色 role_b 的权限值为 p_b，且 role_a ≥ role_b，当且仅当 p_b 是所有与 role_a 有继承关系的低层角色权限值的最大值时，role_a 继承自低级角色的权限值为 p_b.

由于角色间存在继承关系，所以角色的权限值由两部分组成: PA 授予角色的权限值和角色继承自低级角色的权限值. 因此，role_a 的实际权限值为 p_a + p_b.

4.2　信任继承

在系统中，安全管理员并不了解每个用户的可信度，因此权限管理机制采用信任管理[23-24]的方式为用户授权. 考虑到 IBE 系统更适用于等级分明的电子政务及电子军务领域，因此，本文采用信任继承的思想为用户分配角色.

定义 5　当应用系统规模很大时，授权源 SOA(source of authority) 可根据可信用户的信任度授予其部分或全部授权能力，称为信任继承. 这些可信用户称为授权管理者 AM(authorized manager) .

为了实现信任继承，权限管理机制需要根据可信用户的职责和行为计算用户的信任度. 只有可信用户的信任度不低于该角色的信任度阈值时，可信用户才能将该角色授予其他可信用户. 权限管理机制还需要维护信任继承树，用于显示用户间的信任关系.

4.2.1　**角色信任度阈值分配**　角色定义完后，安全管理员为每个角色设置一个信任度阈值. 该信任度阈值表示只有可信用户的信任度大于等于该阈值时，可信用户才可将该角色授予他所信任的用户.

定义 6(角色信任度阈值集合)　T: $T = \{ (\text{obj}, \text{r}, t) \mid \text{obj} \in \text{OBS}, \text{r} \in \text{ROLES}, t \in \ \}$，表示角色 r 对于服务 S，其信任度阈值为 t.

角色信任度阈值设置过程如下(设角色 role) :

1) 根据角色 role 的权限范围确定一个系数 $k1$(其中 $k1 \geqslant 1$，且 $k1 \in \ $) ;

2) 确定授权者将这个角色授予其信任的用户需要满足的最小条件，设 role 最多需要 n 个授权者联合授权才可以将 role 授予其他用户，则 role 的信任度阈值 $t = n \cdot k1$($n \geqslant 1$，且 $n \in \ $) .

当角色的信任度阈值设置完成后，权限管理机制将集合 T 存入 LDAP 中.

4.2.2　**用户信任度计算**　1) 用户信任度初始化为 0，授权源 SOA 的信任度初始化为所有角色中信任度阈值的最大值. 2) 根据用户所分配的角色及用户的访问行为计算用户的信任度. 本文选择计算用户在时间段 t 内用户 n 次访问行为的信任度. 先计算用户 t 时段内的 m 次访问行为的信任度值，再计算用户 t 时段内 n 次访问行为的信任度值. 若 $m < n$，则其他 $n - m$ 次访问行为的信任度置为 0. 最后，取两次计算得到信任度的最小值作为用户的信任度值. 3) 用户信任度值的上限为用户所分配角色的信任度阈值.

4.2.3　**信任继承树**　信任继承树用于记录用户间的信任关系及每个用户的角色分配者，每个服务对应一颗信任继承树，如图 3 所示. 信任继承树的创建过程如下(设有 n 个用户) :

1) 当安全管理员进行系统初始化时，初始化权限分配器 PA 中的信任继承树，此时每个服务所对应的信任继承树只有一个节点，即授权源 SOA;

2) 当用户 i($i < n$) 申请某个权限时，授权源根据用户的身份信息及信任度授予用户相应角色，并

且权限分配器 PA 将该节点作为授权源节点的孩子节点插入到信任树中.

当用户 $k(k<n)$ 向用户 i 申请某个权限时，用户 i 根据用户 k 的身份信息、授权策略和信任度授予用户 k 合理的角色，PA 将用户 k 作为用户 i 的孩子节点插入到信任继承树中.

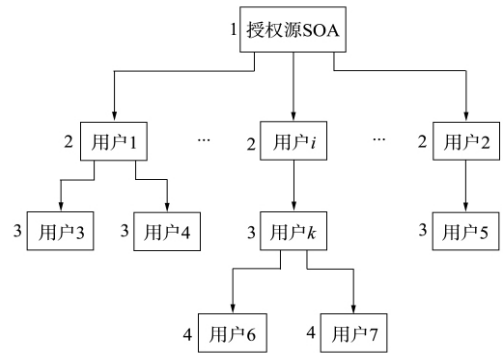

图3 信任继承树

Fig. 3 Tree of trust inheritance

4.2.4 用户角色的分配 假设用户 a 请求用户 b 为用户 a 分配关于服务 S 的 op 权限区的权限. 过程如下: 1) 标识管理机制确认用户 a 的身份. 2) 身份确认后，标识管理机制将用户 a 的访问请求发送给权限管理机制. 3) 权限管理机制将用户 a 的请求发送给用户 b. 4) 用户 b 根据用户 a 的身份、信任度和授权策略为用户 a 分配一个合理的角色(设为 role)，并将分配角色 role 的请求发送给权限管理机制. 5) 权限管理机制查找角色 role 的信任度阈值 x 及用户 b 的信任度 y. 如果 $x\leqslant y$，则数据(用户 a 的标识，服务，角色，有效期，授权者)存入 LDAP 数据库，且节点 a 作为节点 b 的子节点插入到信任继承树中. 否则，拒绝用户 b 的请求.

用户角色分配算法:

```
GrantUserRole ( a: USERS; role: ROLES; obj: OBS): //表示对于服务 obj 授予用户 a 角色 role.
GrantUserRole ( a: USERS; role: ROLES; obj: OBS)
{
  if ( ∃( a,role,obj) ∈ RU( { a: USERS} ) )
  return;
  else
  RU = RU ∪ ( a,role,obj)
}
```

4.3 表的维护

由于用户的动态性，权限管理机制不仅需要为角色分配权限值，为用户分配角色，而且需要维护角色权限列表 PR 及用户角色表 RU.

4.3.1 角色权限列表的维护 根据实际情况，系统需要删除角色或撤销角色的权限，这时就要求权限管理机制动态维护角色权限列表 PR.

1) 角色的删除.

根据实际需要，角色已经不存在，权限管理机制删除已经撤销的角色，不失一般性，假设删除角色 r. 由于角色 r 需要删除，则所有与角色 r 关联的记录都必须删除. 首先删除 PR 表中关于 r 的所有权限分配记录; 其次，查找 RU 表中的所有分配有角色 r 的用户，删除这些用户中关于 r 的记录; 最后，查找角色继承关系 RH 与 r 有继承关系的角色，删除 RH 中包含 r 的记录.

2) 角色权限的撤销.

设系统撤销角色 r 的权限为 pv，算法如下:

```
RevokePV ( r: ROLES; pv: PV)
{
  if ( ∃pv ∈ PR ( { r: ROLES} ) )
  PR = PR - ( r,pv) ;
  else
  return;
}
```

4.3.2　用户角色表的维护　若系统中的用户需要删除或撤销用户的权限，则权限管理机制应该实时动态地维护用户角色表 RU. 设用户 U 的标识为 uid，现假设 U 退出 IBE 信任服务域，则将 RU 中关于 uid 关联的所有的记录全部删除.

5　权限决策

权限决策主要是通过得到用户的权限值和服务的门限值，决定用户是否可以访问.

5.1　角色权限值的计算

角色权限值的计算包括权限管理机制授予的权限值和继承自低级角色的权限值.

1) 权限管理机制根据角色的属性授予角色权限值，该权限值只是权限管理机制根据角色的可信度授予的权限值. 角色 r 被授予权限值的计算方法如下:

```
GetRoleAuthorizPV ( r: ROLES; obj: OBS; op: OPS)
{
  if ( ∃( obj,op,i) ∈ PR ( { r: ROLES} ) )
  return ( obj,op,i) ;
  else
  return ( obj,op,0) ;
}
```

2) 在角色间存在多继承的情况下，角色所继承的权限值是该角色继承所有低级角色权限值的最大值，因为权限值越大，表示角色的权限范围越大. 角色继承自低级角色权限值的计算方法如下(其中: AncestorPVSet 表示角色继承的权限集合; AncestorSet 表示角色 r 的所有有继承关系的角色集) :

```
GetRoleInheritPV ( r: ROLES; obj: OBS; op: OPS)
{
AncestorPVSet = Ø;
AncestorSet = Ancestor ( r) ;
AncestorPVSet = { ( obj,op,i) | ( obj,op,i) ∈ PR ( AncestorSet) } ;
if ( AncestorPVSet = Ø)
  output = ( obj,op,0) ;
else
  return( obj,op,i_max) ;
}
```

3) 角色 r 实际的权限值包括权限管理机制授予角色 r 的权限值和角色 r 继承自低级角色的权限值两部分. 算法如下:

```
GetRolePV ( r: ROLES; obj: OBS; op: OPS)
{
( obj,op,sum) = ( GetRoleInheritPV ( r,obj,op) + GetRoleAuthorizedPV ( r,obj,op) ;
return ( obj,op,sum) ;
}
```

5.2　用户权限值的计算

基于角色的访问控制将角色应用到用户和权限间，用户的权限通过拥有角色获得，因此权限管理机制中并不维护权限用户表，用户的权限通过用户拥有的角色动态计算得出. 用户集记为 USERS. 用户关于服务 obj 某一权限区 op 的权限值通过计算用户所拥有角色的权限值得到. 如果用户所拥有的角色集合中没有角色有此权限，则返回(obj,op,0) . 算法如下:

```
GetUserPV ( user: USERS; obj: OBS; op: OPS)
{
```

```
    role = RU (user,obj,op);
    if (role = Ø)
    return (obj,op,0);
    else
    returnGetRolePV (role,obj,op);
}
```

5.3 访问判定

不同的权限区其门限也不同，而同一角色对于不同的权限区，其权限值也不同. 因此访问判定过程如下:

1) 根据用户的标识查找用户角色表，得到用户在服务 obj 的 op 权限区的权限值 p;

2) 查找服务门限表，得到服务 obj 的权限区 op 的门限 t;

3) 比较 p 与 t: 若 $p \geqslant t$，则返回允许; 若 $p < t$，则返回拒绝.

算法如下:

```
bool IsSatisfied (user: USERS; obj: OBS; op: OPS)
{
    if (GetUserPV (user,obj,op) = (user,obj,0)
    return false;
    if (GetUserPV (user,obj,op) < Threshold (obj,op))
    return false;
    else
    return ture;
}
```

6 集中审计

由于权限管理机制采取服务集中管理的方式，因此，系统可以对域内所有服务的审计数据进行集中管理与分析. 所谓集中审计就是审计模块集中收集系统中关于服务的访问、权限分配过程及权限决策过程的审计数据，并对审计数据进行关联分析，从而维护系统. 其中，审计数据只有审计管理员可以查看，系统管理员、安全管理员及普通用户都不能查看.

通过分析，本文对权限管理机制的几个关键之处设置了审计点:

1) 对权限管理机制的操作提供审计;

2) 对系统管理员及安全管理员的管理操作提供审计;

3) 在策略决策点 PDP 处，对决策过程提供审计;

4) 对服务的注册过程、权限区的划分过程及每个权限区门限的设置提供审计;

5) 对角色的权限值分配、角色信任度阈值设置操作提供审计;

6) 对用户角色的分配操作提供审计;

7) 对用户的访问行为提供审计.

集中审计模块如图 4 所示. 该模块主要通过对用户对服务的访问、角色用户表、角色权限表及服务的门限表的分析检测用户的行为，再根据分析结果，进一步维护系统的角色用户表、角色权限值表、服务的门限表及信任继承树.

由于管理员的误操作而导致越权时，审计管理员就会根据日志记录、服务门限表、角色-权限表和用户-角色表进行分析，针对这些原因维护权限管理机制.

如果发生越权事件，审计模块分析日志，查找事故原因可能有如下几种情况:

1) 服务的权限区门限值设定错误. 针对这种原因，系统会根据越权情况重新对服务的权限区进行划分，并重新设定各权限区的门限值. 2) 角色的权限值分配错误. 针对该原因检查授予用户的角色与

各角色间的继承关系及其约束关系，检查各角色的权限值，查找错误，从而进行修正. 3) 用户的角色分配错误.

假设用户 k 越权，审计模块根据用户 k，沿着其授权路径进行回溯，一直回溯到根节点，将这条路径上所有用户节点的权限值降低，并且这些用户的信任度将下降为 0；将用户 k 为根节点的子树上所有用户节点的权限值置 0，并将该子树全部删除，则图 3 所示的信任继承树将变为如图 5 所示的信任继承树.

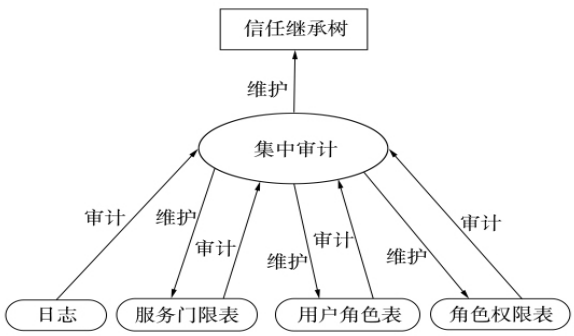

图 4　集中审计模块

Fig. 4　Module of concentration audit

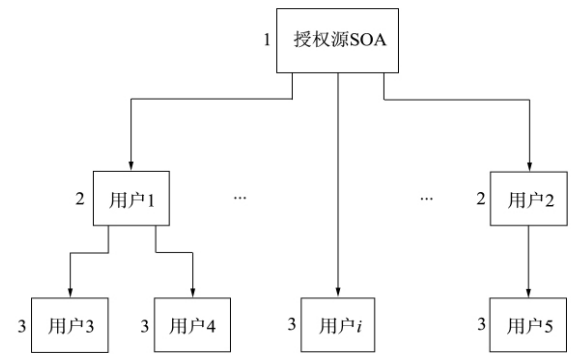

图 5　审计后的信任继承树

Fig. 5　Tree of trust inheritance after audit

综上所述，本文针对现有 IBE 系统内的可信用户可以访问域内任何服务的问题，提出一种基于信任服务 IBE 体系的权限管理机制，解决了 IBE 体系下，服务的注册和权限划分问题及域内的可信用户的权限分配与管理问题. 基于角色的访问控制为权限管理提供了用户与权限的灵活分配，但不能灵活控制服务权限管理的粒度，本文采用门限的思想和算法为服务划分权限. 由于 IBE 体系主要采用集中式的密钥管理方式，主要适用于电子政务和电子军务领域，因此本文根据 IBE 的适用领域等级分明的特点，采用信任继承的思想为用户分配角色，并采用集中审计的方法维护系统，进一步提高了系统的可靠性.

参　考　文　献

[1] LIN Chuang, PENG Xue-hai. Research on Trustworthy Networks [J]. Chinese Journal of Computers, 2005, 28(5): 751-758. (林闯，彭雪海. 可信网络研究 [J]. 计算机学报，2005，28(5)：751-758.)

[2] LIN Chuang, WANG Yuan-zhuo, TIAN Li-qin. Development of Trustworthy Network and Facing Scientific Challenges [J]. ZTE Communications, 2008, 14(1): 13-16. (林闯，王元卓，田立勤. 可信网络的发展及其面对的技术挑战 [J]. 中兴通讯技术，2008，14(1)：13-16.)

[3] ITU-T Recommendation. ISO/IEC 9594-8: Public-Key and Attribute Certificate Frameworks [S]. Information Technology Open System Interconnection, 2001.

[4] SHEN Hong, FAN Ya-qin. Design of Underhandedness Information Transmission System with Local Area Network [J]. Journal of Jilin University: Information Science Edition, 2009, 27(3): 324-328. (沈泓，范亚芹. 企业局域网机密信息传输系统设计 [J]. 吉林大学学报：信息科学版，2009，27(3)：324-328.)

[5] Shamir A. Identity-Based Cryptosystems and Signature Schemes [C] //Proc of the CRYPTO'84 on Advances in Cryptology. New York: Springer, 1985: 47-53.

[6] Boneh D, Franklin M K. Identity-Based Encryption from Weil Pairing [C] //Proceedings of the 21th Annual International Cryptology Conference on Advances in Cryptology. London: Springer, 2001: 213-229.

[7] Cocks C. An Identity Based Encryption Scheme Based on Quadratic Residues [C] //Proceedings of the 8th IMA International Conference on Crytography and Coding. London: Springer, 2001: 360-363.

[8] Libert B, Quisquater J J. Identity Based Undeniable Signatures [C] //CT-RSA 2004. Berlin: Springer-Verlag, 2004: 112-125.

[9] Chow S M, Yiu S M, Hui L C K, et al. Efficient Forward and Provably Secure ID-Based Signcryption Scheme with

Public Verifiability and Public Cipher Text Authenticity [C]//Proceedings on the 6th Annual ICISC 2003. Berlin: Springer-Verlag, 2004: 352-369.

[10] Boneh D, Boyen X. Efficient Selective-ID Secure Identity Based Encryption without Random Oracles [C]//Eurocrpyt 2004. International Association for Cryptologic Research. Berlin: Springer, 2004: 223-238.

[11] Brent W. Efficient Identity-Based Encryption without Random Oracles [C/OL]//Eurocrypt 2005. [2009-05-13]. http://libeccio.dia.unisa.it/CRYPT007/Papers/Waters.pdf.

[12] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography [C]//Asiacrypt 2003. International Association for Cryptologic Research. Berlin: Springer, 2003: 452-473.

[13] Lee B, Boyd C, Dawson E, et al. Secure Key Issuing in ID-Based Cryptography [C]//Proceedings of the Second Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation. Darlinghurst, Australia: Australian Computer Society, 2004: 69-74.

[14] Chen L, Harrison K, Moss A, et al. Certification of Public Keys within an Identity Based System [C]//Proceedings of the 5th International Conference on Information Security. London: Springer-Verlag, 2002: 322-333.

[15] HU Liang, CHU Jian-feng, LIN Yu, et al. IBE System Based on Trust Service [J]. Journal of Jilin University: Engineering and Technology Edition, 2009, 39(3): 737-742. (胡亮, 初剑峰, 林宇, 等. 基于信任服务的IBE系统[J]. 吉林大学学报: 工学版, 2009, 39(3): 737-742.)

[16] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based Access Control Models [J]. IEEE Computer, 1996, 29(2): 38-47.

[17] Sandhu R. Role Hierarchies and Constraints for Lattice-Based Access Control [C]//Proc of Fourth European Symposium on Research in Computer Security. London: Springer-Verlag, 1996: 65-79.

[18] Kern A, Schaad A, Moffett J. An Administration Concept for the Enterprise Role-Based Access Control Mode [C]// Proceedings of the 8th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2003: 3-11.

[19] HU Liang, CHU Jian-feng, LIN Hai-qun, et al. The Key Management Mechanism of IBE System [J]. Chinese Journal of Computers, 2009, 32(3): 543-551. (胡亮, 初剑峰, 林海群, 等. IBE体系的密钥管理机制[J]. 计算机学报, 2009, 32(3): 543-551.)

[20] MENG Xin, HU Liang, CHU Jian-feng, et al. The Cross-Domain Authorization of Heterogeneous Trustworthy Domains [J]. Journal of Jilin University: Science Edition, 2009, 48(1): 89-93. (孟欣, 胡亮, 初剑峰, 等. 异构信任域的跨域授权[J]. 吉林大学学报: 理学版, 2009, 48(1): 89-93.)

[21] Ferraiolo D F, Barkley J F, Kuhn D R. A Role-Based Access Control Model and Reference Implementation with in a Corporate Intranet [J]. ACM Trans on Information and System Security, 1999, 2(1): 34-64.

[22] Ferraiolo D F, Sandhu R, Gavrila S, et al. Proposed NIST Standard for Role-Based Access Control [J]. ACM Trans on Information and System Security, 2001, 4(3): 224-274.

[23] LIN Chuang, TIAN Li-qin, WANG Yuan-zhuo. Research on User Behavior Trust in Trustworthy Network [J]. Journal of Computer Research and Development, 2008, 45(12): 2033-2043. (林闯, 田立勤, 王元卓. 可信网络中用户行为可信的研究[J]. 计算机研究与发展, 2008, 45(12): 2033-2043.)

[24] ZHAI Zheng-de, FENG Deng-guo, XU Zhen. Fine-Grained Controllable Delegation Authorization Model Based on Trustworthiness [J]. Journal of Software, 2007, 18(8): 2002-2015. (翟征德, 冯登国, 徐震. 细粒度的基于信任度的可控委托授权模型[J]. 软件学报, 2007, 18(8): 2002-2015.)