

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 9/32 (2006.01)

H04L 29/06 (2006.01)

H04L 12/56 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200810040674.9

[43] 公开日 2008 年 12 月 10 日

[11] 公开号 CN 101321064A

[22] 申请日 2008.7.17

[21] 申请号 200810040674.9

[71] 申请人 上海众恒信息产业有限公司

地址 200040 上海市延安西路 376 弄 22 号 6 层

[72] 发明人 高建强 顾国强 王占宏 孙圭宁
高念高

[74] 专利代理机构 上海明成云知识产权代理有限公司

代理人 周 成

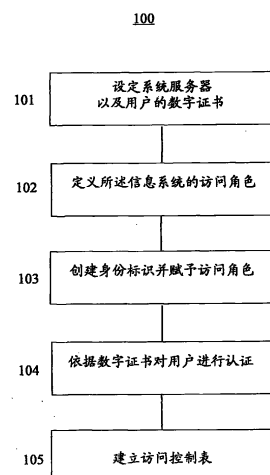
权利要求书 2 页 说明书 6 页 附图 3 页

[54] 发明名称

一种基于数字证书技术的信息系统的访问控制方法及装置

[57] 摘要

本发明揭示了一种基于数字证书技术的信息系统访问控制方法和装置，包括设定数字证书、定义访问角色、创建身份标识并将所述访问角色赋予所述身份标识，对请求登陆的用户进行认证并对通过认证的用户建立访问控制表。本发明所述的方法及装置一方面是基于数字证书技术的，数字证书技术通过其公钥和密钥可以更好的保证用户和系统之间数据交换的安全性，另一方面本方法及装置是基于访问角色的访问控制模型，这种方式只需把新的注册用户创建给已定义的访问角色即可，无需为用户重新指定资源和操作，因而简化了授权管理工作。



1、一种基于数字证书技术的信息系统访问控制方法，其特征在于，包括以下步骤：

- a、设定系统服务器数字证书以及用户数字证书；
- b、定义所述信息系统的访问角色，所述访问角色是所述信息系统不同访问权限的集合；
- c、向注册的用户创建身份标识，将所述 b 步骤定义的访问角色赋予所述身份标识；
- d、根据所述 a 步骤的数字证书对请求登陆的用户进行认证；
- e、根据所述 c 步骤的用户身份标识，对通过认证的用户建立访问控制表，所述访问控制表执行所述用户的访问控制。

2、如权利要求 1 所述的访问控制方法，其特征在于，所述 d 步骤包括：

1) 向请求登陆认证的用户发送服务器数字证书和随机数，用户签名随机数，并用服务器数字证书加密随机数，将用户数字证书、签名随机数和加密随机数返还至系统服务器；

2) 系统服务器解密所述随机数，并将解密后的随机数与原随机数比对，若一致则用户认证成功，若不一致则拒绝认证。

3、如权利要求 2 所述的访问控制方法，其特征在于，所述 a 步骤还定义了所述信息系统数据库的数据的保密等级，所述定义了保密等级的数据与所述访问角色匹配。

4、如权利要求 2 所述的访问控制方法，其特征在于，所述 a 步骤所述用户数字证书的密钥存储于客户端的存储器，所述系统服务器数字证书存储于系统服务器的存储器。

5、如权利要求 1 所述的访问控制方法，其特征在于，所述访问控制表包括所述访问角色与所述定义了保密等级的数据以及所述身份标识三者之间的联系规则，所述访问控制表存储在所述信息系统的数据库中。

6、如权利要求 1 所述的访问控制方法，其特征在于，所述访问控制表验证所述身份标识以及所述身份标识的访问目标的合法性。

7. 一种基于数字证书技术的信息系统的访问控制装置，其特征在于，包括：

注册模块，所述注册模块为所述信息系统的用户提供注册并设定系统服务器数字证书以及用户数字证书；

定义模块，定义所述信息系统的访问角色，向注册的用户创建身份标识，将所述访问角色赋予所述身份标识，所述访问角色是所述信息系统不同访问权限的集合；

控制模块，所述控制模块根据所述注册模块设定的数字证书对请求登陆的用户进行认证，并根据所述身份标识对通过认证的用户建立访问控制表，所述访问控制表执行所述用户的访问控制。

8. 如权利要求 7 所述的访问控制装置，其特征在于，所述控制模块对请求登陆的用户进行认证包括以下步骤：

1) 向请求登陆认证的用户发送服务器数字证书和随机数，用户签名随机数，并用服务器数字证书加密随机数，将用户数字证书、签名随机数和加密随机数返还至系统服务器；

2) 系统服务器解密所述随机数，并将解密后的随机数与原随机数比对，若一致则用户认证成功，若不一致则拒绝认证。

9. 如权利要求 8 所述的访问控制装置，其特征在于，所述定义模块还定义了所述信息系统数据库的数据的保密等级，所述定义了保密等级的数据与所述访问角色匹配。

10. 如权利要求 7 所述的访问控制装置，其特征在于，所述访问控制表包括所述访问角色与所述定义了保密等级的数据以及所述身份标识三者之间的联系规则，所述访问控制表存储在所述信息系统的数据库中。

一种基于数字证书技术的信息系统的访问控制方法及装置

技术领域

本发明涉及数据信息系统的安全技术，更具体地说，涉及一种基于数字证书技术的信息系统的访问控制方法及装置。

背景技术

目前越来越多的工作需要利用到各种各样的信息系统，而信息系统的安全性越来越得到人们的关注，例如在信息系统的访问控制方面就需要注重其安全性，在一个信息系统中具有级别不同的各种用户，特定的用户只能访问特定的数据，而如果安全措施不到位，那么会出现用户可以访问到其不该访问的数据，从而造成泄密等事故，就可能给国家和企业造成难以挽回的损失。一个信息系统会供给不同的部门和不同的人使用，这些不同的部门和不同的人的数据需求是不一样的，这就决定了对于不同级别的用户要创建不同的访问权限，这样才既能满足各用户的访问要求也能保证秘密数据不被泄漏。可见对于信息系统的用户访问需要进行相关安全策略的设计，从而达到对不同用户的访问进行控制的目的。

发明内容

本发明的目的在于提供一种基于数字证书技术的信息系统的访问控制方法及装置，以实现对不同用户的访问进行控制的目的。

根据本发明的第一方面，提供一种基于数字证书技术的信息系统的访问控制方法，包括以下步骤：

- a、设定系统服务器数字证书以及用户数字证书；
- b、定义所述信息系统的访问角色，所述访问角色是所述信息系统不同访问权限的集合；
- c、向注册的用户创建身份标识，将所述 b 步骤定义的访问角色赋予所述身份标识；

d、根据所述 a 步骤的数字证书对请求登陆的用户进行认证；

e、根据所述 c 步骤的用户身份标识，对通过认证的用户建立访问控制表，所述访问控制表执行所述用户的访问控制。

所述 d 步骤包括：

1) 向请求登陆认证的用户发送服务器数字证书和随机数，用户签名随机数，并用服务器数字证书加密随机数，将用户数字证书、签名随机数和加密随机数返还至系统服务器；

2) 系统服务器解密所述随机数，并将解密后的随机数与原随机数比对，若一致则用户认证成功，若不一致则拒绝认证。

所述 a 步骤还定义了所述信息系统数据库的数据的保密等级，所述定义了保密等级的数据与所述访问角色匹配。

所述 a 步骤所述用户数字证书的密钥存储于客户端的存储器，所述系统服务器数字证书的密钥存储于系统服务器的存储器。

所述访问控制表包括所述访问角色与所述定义了保密等级的数据以及所述身份标识三者之间的联系规则，所述访问控制表存储在所述信息系统的数据库中。

所述访问控制表验证所述身份标识以及所述身份标识的访问目标的合法性。

根据本发明的第二方面，提供一种基于数字证书技术的信息系统的访问控制装置，包括：

注册模块，所述注册模块为所述信息系统的用户提供注册并设定系统服务器数字证书以及用户数字证书；

定义模块，定义所述信息系统的访问角色，向注册的用户创建身份标识，将所述访问角色赋予所述身份标识，所述访问角色是所述信息系统不同访问权限的集合；

控制模块，所述控制模块根据所述注册模块设定的数字证书对请求登陆的用户进行认证，并根据所述身份标识对通过认证的用户建立访问控制表，所述访问控制表执行所述用户的访问控制。

所述控制模块对请求登陆的用户进行认证包括以下步骤：

1) 向请求登陆认证的用户发送服务器数字证书和随机数, 用户签名随机数, 并用服务器数字证书加密随机数, 将用户数字证书、签名随机数和加密随机数返还至系统服务器;

2) 系统服务器解密所述随机数, 并将解密后的随机数与原随机数比对, 若一致则用户认证成功, 若不一致则拒绝认证。

所述定义模块还定义了所述信息系统数据库的数据的保密等级, 所述定义了保密等级的数据与所述访问角色匹配。

所述访问控制表包括所述访问角色与所述定义了保密等级的数据以及所述身份标识三者之间的联系规则, 所述访问控制表存储在所述信息系统的数据库中。

采用本发明所述的一种基于数字证书技术的信息系统的访问控制方法及装置, 本发明所述的方法及装置一方面是基于数字证书技术的, 数字证书技术通过其公钥和密钥可以更好的保证用户和系统之间数据交换的安全性, 另一方面本方法及装置是基于访问角色的访问控制模型, 即先定义访问角色, 然后将此访问角色赋予注册的合法用户, 再建立用户的访问控制表, 把“用户 访问角色 操作 数据”关联到一起, 实现非自主型访问控制策略, 使用基于访问角色的访问控制模型可以减轻安全管理工作, 这种方式只需把新的注册用户创建给已定义的访问角色即可, 无需为用户重新指定资源和操作, 因而简化了授权管理工作。

附图说明

图 1 为本发明所述的访问控制方法的流程示意图;

图 2 为本发明所述的访问控制装置的原理示意图;

图 3 为本发明所述的访问控制方法及装置的工作流程示意图。

具体实施方式

下面结合附图和实施例进一步说明本发明的技术方案。

参考图 1, 图 1 是本发明所述的访问控制方法 100 的流程示意图, 包括以下步骤:

101、设定系统服务器以及用户的数字证书。

PKI (公开密钥系统), 是应用公钥概念和公钥密码技术为全社会广泛实施和提供信息化安全及信任服务的安全基础设施。在 PKI 中, 为了确保用户及其所持有密钥的正确性, 需要一个值得信赖而且独立的第三方机构充当 CA 认证中心 (Certification Authority), 来确认声称拥有公开密钥的实体的真正身份。要确认一个公开密钥, CA 首先制作一张“数字证书”, 它包含用户身份的部分信息及用户所持有的公开密钥, 然后 CA 利用本身的密钥为数字证书加上数字签名, 所述用户数字证书的密钥 (私钥) 存储于客户端的存储器, 所述系统服务器数字证书的密钥 (私钥) 存储于系统服务器的存储器, 这样一个属于这个实体的数字证书就完成了。

102、定义所述信息系统的访问角色。所述访问角色是所述信息系统不同访问权限的集合, 在一实施例中还定义了所述信息系统数据库的数据的保密等级, 这些被定义了保密等级的数据与访问角色匹配, 即什么样的访问角色能访问什么样的保密等级的数据。

103、创建身份标识并赋予访问角色。向注册的用户创建身份标识, 将所述访问角色赋予所述身份标识, 创建的身份标识是唯一存在的。将访问角色赋予身份标识, 使每个身份标识对应相应的访问角色, 这样每个身份标识就有了对所述信息系统访问的访问权限。

104、依据数字证书对用户进行认证。包括以下步骤:

1) 向请求登陆认证的用户发送服务器数字证书和随机数, 用户签名随机数, 并用服务器数字证书加密随机数, 将用户数字证书、签名随机数和加密随机数返还至系统服务器;

2) 系统服务器解密所述随机数, 并将解密后的随机数与原随机数比对, 若一致则用户认证成功, 若不一致则拒绝认证。

对于系统服务器, 首先, 系统服务器要接受很多客户端的服务要求, 这就要建立合适的数据库, 以便保存用户的数据信息, 并方便维护和管理, 提供查找修改等功能。还要提供数据库的备份设备, 以防数据被破坏。其次, 服务器端的网页要进行适当的修改, 提供用户登陆的界面, 显示用户登录后的信息, 满足用户的一些基本要求。再次, 服务器端要注册 COM 动

态链接文件，安装数字证书管理器，以保证登陆地网页和程序能正确地调用 SafeEngine 等库函数。

对于用户（客户端），要安装数字证书管理器，以能将私钥装入并正确获得证书。对于安全级别较高地用户要使用硬件加密设备，例如明华 USB 棒等。数字证书管理器可以通过 CAB 包从网页中下载安装。

当用户端登陆服务器时，服务器端初始化，得到服务器数字证书，并产生一个随机数，然后把服务器证书和随机数发给客户端。客户端初始化硬件加密设备，获得客户端的用户数字证书和所述随机数，验证服务器数字证书，验证通过后用户用其私钥签名所述随机数，并用服务器数字证书加密所述随机数，然后把用户数字证书、随机数签名和随机数加密发给服务器。

服务器收到返回的数据后，用其私钥初始化，并取出服务器数字证书。然后验证客户端数字证书，验证通过后用自己的私钥解密随机数，并用客户端数字证书对收到的随机数签名进行验证，再检查解密的随机数与原来发送的随机数是否一致，若一致则用户认证成功，若不一致则拒绝认证。

105、建立访问控制表。用户通过认证后，根据所述用户的身份标识，对通过认证的用户建立访问控制表，所述访问控制表执行所述用户的访问控制并验证所述身份标识以及所述身份标识的访问目标的合法性。所述访问控制表包括所述访问角色与所述定义了保密等级的数据以及所述身份标识三者之间的联系规则，所述访问控制表存储在所述信息系统的数据库中。

参考图 2，所述访问控制装置包括以下模块：

注册模块 201，所述注册模块 201 为所述信息系统的用户提供注册并设定系统服务器数字证书以及用户数字证书；

定义模块 202，定义所述信息系统的访问角色，向注册的用户创建身份标识，将所述访问角色赋予所述身份标识，所述访问角色是所述信息系统不同访问权限的集合；所述定义模块还定义了所述信息系统数据库的数据的保密等级，所述定义了保密等级的数据与所述访问角色匹配。

控制模块 203，所述控制模块 203 根据所述注册模块 201 设定的数字证书对请求登陆的用户进行认证，并根据所述身份标识对通过认证的用户

建立访问控制表，所述访问控制表执行所述用户的访问控制。所述访问控制表包括所述访问角色与所述定义了保密等级的数据以及所述身份标识三者之间的联系规则，所述访问控制表存储在所述信息系统的数据库中。

所述控制模块 203 对请求登陆的用户进行认证过程同于所述访问控制方法 100 的步骤 104，包括以下步骤：

1) 向请求登陆认证的用户发送服务器数字证书和随机数，用户签名随机数，并用服务器数字证书加密随机数，将用户数字证书、签名随机数和加密随机数返还至系统服务器；

2) 系统服务器解密所述随机数，并将解密后的随机数与原随机数比对，若一致则用户认证成功，若不一致则拒绝认证。

下面结合图 3 说明一下本发明所述技术方案的一具体实施例的工作流程：

301、用户登录（包括通过 IC 卡等方式）：系统对其进行验证，只有通过验证才可以进入下一步。

302、通过浏览器或前台系统的查询界面发出查询请求。

303、检索用户的角色组成和相关角色权限（用户访问角色），组织用户的权限列表（访问控制表）。

304、检查查询的目标（数据表），同时检查用户的业务、地域属性是否符合查询目标的业务、地域限制，不满足则返回“没有权限”的提示，并封锁此用户没有权限检索的字段。

305、将相关的记录级权限限制（如可访问的记录密级限制）作为查询的限制条件组织查询语句，提交给综合信息数据库进行查询。

306、将数据库的查询结果返回给用户。

另外，除了数据封锁之外，用户进行每一项操作时，系统也要检查该用户的权限，并根据该权限所具有的操作功能决定哪些功能对该用户开放，哪些功能不能执行。

本技术领域中的普通技术人员应当认识到，以上的实施例仅是用来说明本发明，而并非用作为对本发明的限定，只要在本发明的实质精神范围内，对以上实施例的变化、变型都将落在本发明的权利要求书范围内。

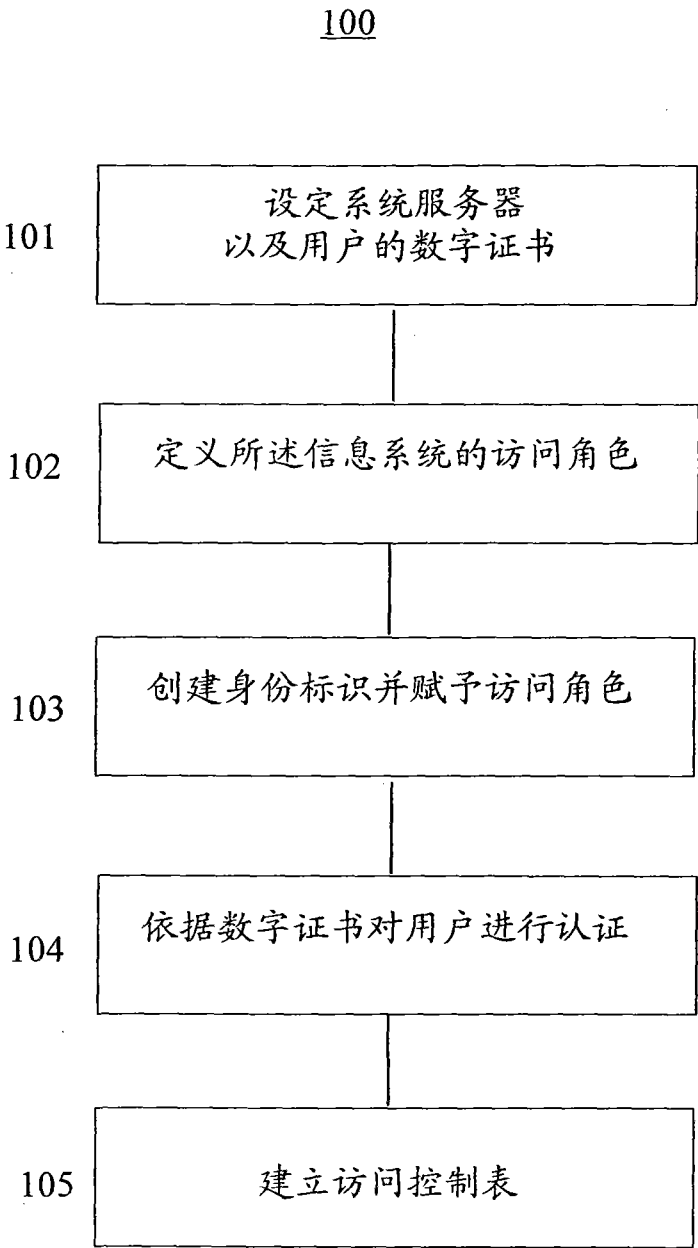


图 1

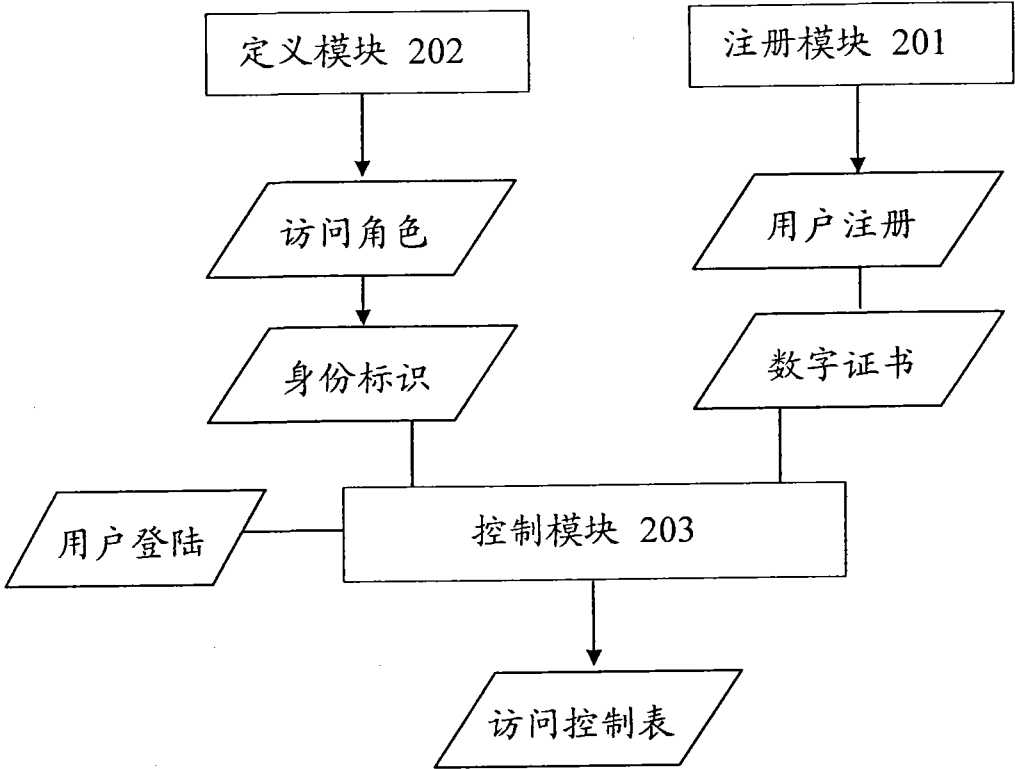


图 2

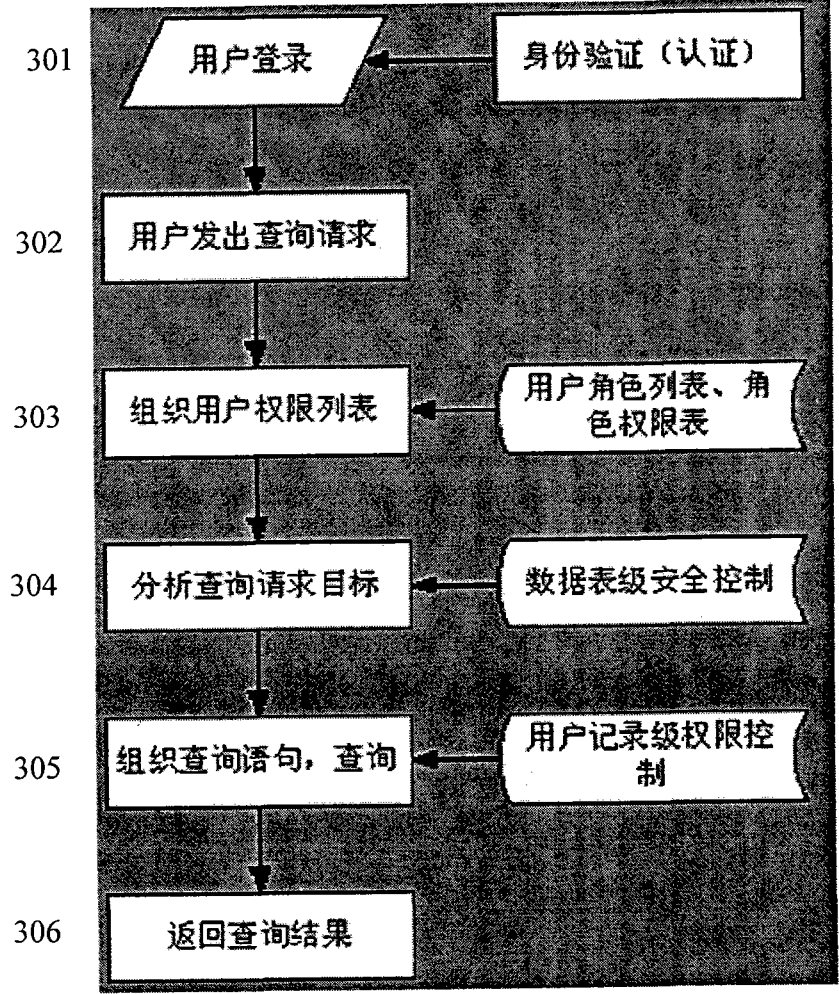


图 3