



(12) 发明专利

(10) 授权公告号 CN 102571810 B

(45) 授权公告日 2015.07.22

(21) 申请号 201210028535.0

第1段 - 说明书第9页第3段.

(22) 申请日 2012.02.09

CN 101216923 A, 2008.07.09, 全文.

(73) 专利权人 赵淦森

CN 101304317 A, 2008.11.12, 全文.

地址 510630 广东省广州市天河区石牌华南
师范大学计算机学院

审查员 谢正程

(72) 发明人 赵淦森 李子柳 汤庸 巴钟杰

(74) 专利代理机构 广州嘉权专利商标事务所有
限公司 44205

代理人 谭英强

(51) Int. Cl.

H04L 29/06(2006.01)

H04L 9/32(2006.01)

G06F 21/33(2013.01)

(56) 对比文件

CN 101350723 A, 2009.01.21, 说明书第3页

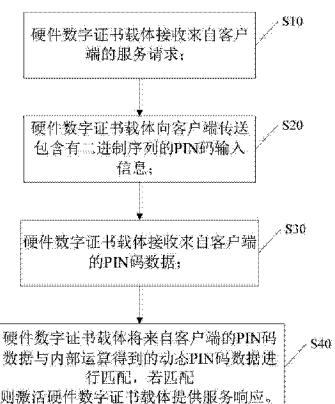
权利要求书2页 说明书5页 附图3页

(54) 发明名称

一种基于硬件数字证书载体的动态密码验证
方法及系统

(57) 摘要

本发明公开了一种基于硬件数字证书载体的动态密码验证方法及系统,该方法包括:硬件数字证书载体接收来自客户端的服务请求;硬件数字证书载体向客户端传送包含有二进制序列的PIN码输入信息;硬件数字证书载体接收来自客户端的PIN码数据;硬件数字证书载体将来自客户端的PIN码数据与内部运算得到的动态PIN码数据进行匹配,若匹配则激活硬件数字证书载体提供服务响应。本发明在用户获取硬件数字证书载体的使用权限进行PIN码认证时,通过与动态生成的二进制序列结合,要求用户输入动态的PIN码,从而使得即使系统被非法入侵时,入侵者也无法获取完整的PIN码,提高了硬件数字证书载体密码的安全性,保障了用户的合法利益。



1. 一种基于硬件数字证书载体的动态密码验证方法,其特征在于,该方法包括以下步骤:

硬件数字证书载体接收来自客户端的服务请求;

硬件数字证书载体向客户端传送包含有二进制序列的 PIN 码输入信息,所述硬件数字证书载体随机产生的二进制序列的刷新次数可以设置,当超过预定义的刷新次数后,硬件数字证书载体将进入锁定状态;

硬件数字证书载体接收来自客户端的对应二进制序列输入的 PIN 码数据;

硬件数字证书载体将来自客户端的 PIN 码数据与内部运算得到的动态 PIN 码数据进行匹配,若匹配则激活硬件数字证书载体提供服务响应。

2. 根据权利要求 1 所述的一种基于硬件数字证书载体的动态密码验证方法,其特征在于:

所述二进制序列是由硬件数字证书载体随机产生的数据,该二进制序列的位数与硬件数字证书载体原始 PIN 码的位数相同。

3. 根据权利要求 2 所述的一种基于硬件数字证书载体的动态密码验证方法,其特征在于:硬件数字证书载体接收来自客户端的服务请求之后并在向客户端传送包含有二进制序列的 PIN 码输入信息之前还包括:

对服务请求的指令完整性进行判断,若服务请求的指令完整并需要提升权限,则硬件数字证书载体向客户端传送包含有二进制序列的 PIN 码输入信息。

4. 根据权利要求 3 所述的一种基于硬件数字证书载体的动态密码验证方法,其特征在于:

所述硬件数字证书载体随机产生的二进制序列存储在缓冲存储模块,该缓冲存储模块内数据的存储时间可以设置,并且在二进制序列刷新时被新生成的二进制序列覆盖。

5. 一种基于硬件数字证书载体的动态密码验证系统,其特征在于,该系统包括:

数据接收模块,用于接收来自客户端的对应二进制序列输入的 PIN 码数据,包括服务请求和用户通过客户端输入的 PIN 码数据;

安全服务模块,用于生成包含有二进制序列的 PIN 码输入信息;

数据发送模块,用于将包含有二进制序列的 PIN 码输入信息传送给客户端;

比较模块,用于根据硬件数字证书载体的原始 PIN 码和二进制序列计算得到动态 PIN 码数据,并比较计算得到的动态 PIN 码数据与来自客户端的 PIN 码数据,若匹配则激活硬件数字证书载体提供服务响应。

6. 根据权利要求 5 所述的一种基于硬件数字证书载体的动态密码验证系统,其特征在于:

所述二进制序列是由安全服务模块随机产生的数据,该二进制序列的位数与硬件数字证书载体原始 PIN 码的位数相同。

7. 根据权利要求 6 所述的一种基于硬件数字证书载体的动态密码验证系统,其特征在于:

该系统还包括一指令处理模块,用于对服务请求的指令完整性进行判断,若服务请求的指令完整并需要提升权限,则安全服务模块生成包含有二进制序列的 PIN 码输入信息。

8. 根据权利要求 7 所述的一种基于硬件数字证书载体的动态密码验证系统,其特征在

于：

还包括一缓冲存储模块，用于存储安全服务模块随机产生的二进制序列，该缓冲存储模块内数据的存储时间可以设置，并且在二进制序列刷新时被新生成的二进制序列覆盖。

9. 根据权利要求 8 所述的一种基于硬件数字证书载体的动态密码验证系统，其特征在于：

还包括一刷新计数模块，用于对安全服务模块刷新二进制序列的次数进行计数，所述二进制序列的刷新次数可以设置，当超过预定义的刷新次数后，硬件数字证书载体将进入锁定状态。

一种基于硬件数字证书载体的动态密码验证方法及系统

技术领域

[0001] 本发明涉及数字证书认证技术,尤其是一种基于硬件数字证书载体的动态密码验证方法及系统。

背景技术

[0002] 随着电子商务和互联网的快速发展,USB Key 作为网络用户身份识别和数据保护的“电子钥匙”,正在被越来越多的用户所熟悉。

[0003] USB Key 是一种基于 USB 接口的智能存储身份认证设备,内置有智能卡 CPU、存储器、芯片操作系统(Chip Operating System,COS)和安全文件系统,用于在服务器和用户之间进行身份认证。

[0004] 由于USB Key 主要用于网络认证,其内部存储有用户的数字证书和用户私钥,利用其内置的公钥算法实现对用户身份的验证,用户的私钥和数字证书保存于 USB Key 安全存储区域中,理论上无法从外部获取,这就保证了用户私钥和数字证书的安全性。

[0005] USB Key 通过 PIN (Personal Identification Number,个人识别密码) 码来保护 USB Key 的使用权,PIN 码是 USB Key 的密码,只有拥有的该 USB Key 的 PIN 码,才可以进行 USB Key 操作。即使被人捡到,或电脑被入侵,也无法在不知道 PIN 码的情况下盗用用户的 USB Key。

[0006] 假如用户的系统被入侵,由于用户每次输入的皆为完整的 PIN 码,入侵者只要采用键盘记录工具或者其他方式即可获得用户的 PIN 码,这样入侵者就能获取用户 USB Key 的使用权,进行一些有损用户利益的操作。

发明内容

[0007] 本发明要解决的技术问题是:提供一种基于硬件数字证书载体的动态密码验证方法,该方法可以有效地提高用户使用硬件数字证书载体的信息安全性。

[0008] 本发明要解决的另一技术问题是:提供一种基于硬件数字证书载体的动态密码验证系统,该系统有效地保障了用户使用硬件数字证书载体的信息安全性。

[0009] 为了解决上述技术问题,本发明所采用的技术方案是:

[0010] 一种基于硬件数字证书载体的动态密码验证方法,该方法包括以下步骤:

[0011] 硬件数字证书载体接收来自客户端的服务请求;

[0012] 硬件数字证书载体向客户端传送包含有二进制序列的 PIN 码输入信息;

[0013] 硬件数字证书载体接收来自客户端的 PIN 码数据;

[0014] 硬件数字证书载体将来自客户端的 PIN 码数据与内部运算得到的动态 PIN 码数据进行匹配,若匹配则激活硬件数字证书载体提供服务响应。

[0015] 进一步作为优选的实施方式,所述二进制序列是由硬件数字证书载体随机产生的数据,该二进制序列的位数与硬件数字证书载体原始 PIN 码的位数相同。

[0016] 进一步作为优选的实施方式,硬件数字证书载体接收来自客户端的服务请求之后

并在向客户端传送包含有二进制序列的 PIN 码输入信息之前还包括：

[0017] 对服务请求的指令完整性进行判断,若服务请求的指令完整并需要提升权限,则硬件数字证书载体向客户端传送包含有二进制序列的 PIN 码输入信息。

[0018] 进一步作为优选的实施方式,所述硬件数字证书载体随机产生的二进制序列存储在缓冲存储模块,该缓冲存储模块内数据的存储时间可以设置,并且在二进制序列刷新时被新生成的二进制序列覆盖。

[0019] 进一步作为优选的实施方式,所述硬件数字证书载体随机产生的二进制序列的刷新次数可以设置,当超过预定的刷新次数后,硬件数字证书载体将进入锁定状态。

[0020] 一种基于硬件数字证书载体的动态密码验证系统,该系统包括:

[0021] 数据接收模块,用于接收来自客户端的数据,包括服务请求和用户通过客户端输入的 PIN 码数据;

[0022] 安全服务模块,用于生成包含有二进制序列的 PIN 码输入信息;

[0023] 数据发送模块,用于将包含有二进制序列的 PIN 码输入信息传送给客户端;

[0024] 比较模块,用于根据硬件数字证书载体的原始 PIN 码和二进制序列计算得到动态 PIN 码数据,并比较计算得到的动态 PIN 码数据与来自客户端的 PIN 码数据,若匹配则激活硬件数字证书载体提供服务响应。

[0025] 进一步作为优选的实施方式,所述二进制序列是由安全服务模块随机产生的数据,该二进制序列的位数与硬件数字证书载体原始 PIN 码的位数相同。

[0026] 进一步作为优选的实施方式,该系统还包括一指令处理模块,用于对服务请求的指令完整性进行判断,若服务请求的指令完整并需要提升权限,则安全服务模块生成包含有二进制序列的 PIN 码输入信息。

[0027] 进一步作为优选的实施方式,该系统还包括一缓冲存储模块,用于存储安全服务模块随机产生的二进制序列,该缓冲存储模块内数据的存储时间可以设置,并且在二进制序列刷新时被新生成的二进制序列覆盖。

[0028] 进一步作为优选的实施方式,该系统还包括一刷新计数模块,用于对安全服务模块刷新二进制序列的次数进行计数,所述二进制序列的刷新次数可以设置,当超过预定的刷新次数后,硬件数字证书载体将进入锁定状态。

[0029] 本发明的有益效果是:本发明基于硬件数字证书载体的动态密码验证方法及系统,在用户获取硬件数字证书载体的使用权限进行 PIN 码认证时,一改传统的直接输入全部 PIN 码的做法,而是通过与动态生成的二进制序列结合,要求用户输入动态的 PIN 码,从而使得即使系统被非法入侵时,入侵者也无法获取完整的 PIN 码,提高了硬件数字证书载体密码的安全性,保障了用户的合法利益。

附图说明

[0030] 下面结合附图对本发明的具体实施方式作进一步说明:

[0031] 图 1 是本发明基于硬件数字证书载体的动态密码验证方法实施例一的步骤流程图;

[0032] 图 2 是本发明基于硬件数字证书载体的动态密码验证方法实施例二的步骤流程图;

- [0033] 图 3 是本发明基于硬件数字证书载体的动态密码验证系统实施例一的结构方框图；
- [0034] 图 4 是本发明硬件数字证书载体与客户端系统的数据流图；
- [0035] 图 5 是本发明基于硬件数字证书载体的动态密码验证系统实施例二的结构方框图；
- [0036] 图 6 是本发明基于硬件数字证书载体的动态密码验证系统实施例三的结构方框图。

具体实施方式

[0037] 现有的硬件数字证书载体的 PIN 码验证需要用户输入完整的 PIN 码，本发明采用输入动态的 PIN 码的方式以提高硬件数字证书载体 PIN 码的安全性。

[0038] 参照图 1，本发明基于硬件数字证书载体的动态密码验证方法实施例一的步骤流程如下：

- [0039] 步骤 S10：硬件数字证书载体接收来自客户端的服务请求；
- [0040] 步骤 S20：硬件数字证书载体向客户端传送包含有二进制序列的 PIN 码输入信息；
- [0041] 步骤 S30：硬件数字证书载体接收来自客户端的 PIN 码数据；
- [0042] 步骤 S40：硬件数字证书载体将来自客户端的 PIN 码数据与内部运算得到的动态 PIN 码数据进行匹配，若匹配则激活硬件数字证书载体提供服务响应。

[0043] 下面列举一个实际应用的例子，硬件数字证书载体以 USB Key 为例，假设该 USB Key 的 PIN 码为 123321123。

- [0044] 现有技术的 USB Key 的 PIN 码认证流程如下：
- [0045] A: 用户申请使用 USB Key 服务响应，通过客户端向 USB Key 服务请求；
- [0046] B: USB Key 接收服务请求后，向客户端返回 PIN 码认证请求，客户端弹出 PIN 码认证输入框；
- [0047] C: 用户通过客户端输入 PIN 码 123321123；
- [0048] D: USB Key 为用户提供服务响应。

- [0049] 在本发明中 USB Key 的 PIN 码认证流程如下：
- [0050] A: 用户申请使用 USB Key 服务响应，通过客户端向 USB Key 服务请求；
- [0051] B: USB Key 接收服务请求后，向客户端返回 PIN 码认证请求，客户端弹出 PIN 码认证输入框，客户端同时显示随 PIN 码认证请求接收的二进制序列，例如提示 00XXOX000（二进制序列由 USB Key 随机产生的，理论上每次得到的二进制序列无法预知，此序列的位数与 USB Key 的 PIN 码长度相等，0 表示其对应的 PIN 码相同位置的数字需要输入，X 表示不用输入）；
- [0052] C: 用户通过客户端输入 PIN 码 122123；
- [0053] D: USB Key 将用户输入的动态 PIN 码与内部计算获得 PIN 码进行匹配，若匹配为用户提供服务响应。
- [0054] 作为本发明基于硬件数字证书载体的动态密码验证方法的进一步改进，所述二进制序列是由硬件数字证书载体随机产生的数据，该二进制序列的位数与硬件数字证书载体

原始 PIN 码的位数相同。

[0055] 在上述实施例的基础之上，参照图 2，作为本发明基于硬件数字证书载体的动态密码验证方法的进一步改进，本发明动态密码验证方法实施例二在步骤 S10 和步骤 S20 之间还设有步骤 S11，步骤 S11 为对服务请求的指令完整性进行判断，若服务请求的指令完整并需要提升权限，则硬件数字证书载体向客户端传送包含有二进制序列的 PIN 码输入信息。

[0056] 进一步，所述硬件数字证书载体随机产生的二进制序列存储在缓冲存储模块，该缓冲存储模块内数据的存储时间可以设置，并且在二进制序列刷新时被新生成的二进制序列覆盖。

[0057] 进一步，所述硬件数字证书载体随机产生的二进制序列的刷新次数可以设置，当超过预定义的刷新次数后，硬件数字证书载体将进入锁定状态。例如设定刷新次数为 3 次，这样用户仅有三次输入动态 PIN 码通过认证的机会，避免了非法入侵者在获取部分 PIN 码的基础上通过多次刷新进行攻击。

[0058] 参照图 3，在本发明基于硬件数字证书载体的动态密码验证系统实施例一中，该系统包括：

[0059] 数据接收模块 10，用于接收来自客户端的数据，包括服务请求和用户通过客户端输入的 PIN 码数据；

[0060] 安全服务模块 20，用于生成包含有二进制序列的 PIN 码输入信息；

[0061] 数据发送模块 30，用于将包含有二进制序列的 PIN 码输入信息传送给客户端；

[0062] 比较模块 40，用于根据硬件数字证书载体的原始 PIN 码和二进制序列计算得到动态 PIN 码数据，并比较计算得到的动态 PIN 码数据与来自客户端的 PIN 码数据，若匹配则激活硬件数字证书载体提供服务响应。

[0063] 进一步作为优选的实施方式，所述二进制序列是由安全服务模块随机产生的数据，该二进制序列的位数与硬件数字证书载体原始 PIN 码的位数相同。

[0064] 参照图 4，在本发明动态密码验证系统的实际工作中，数据的具体流向如下：

[0065] 1、用户向应用程序提交使用硬件数字证书载体的服务响应的请求；

[0066] 2、应用程序通过操作系统调用 CSP (Cryptographic service provider)，即 windows 平台最底层加密接口，通过 CSP 向硬件数字证书载体的 COS (Chip Operating System, 片上操作系统) 发送服务请求；

[0067] 3、COS 通过指令解析后，将随机生成的二进制序列和输入 PIN 码请求打包成 PIN 码输入信息，通过 CSP 传送给应用程序；

[0068] 4、应用程序显示 PIN 码输入框，并显示 PIN 码“输入提示”(即 0X00XX000 此类序列，此时它的表现形式应当还只是一个二进制数，如 101100111)；

[0069] 5、用户在客户端根据 PIN 码“输入提示”输入动态 PIN 码，应用程序经 CSP 将用户输入的动态 PIN 码转交给 COS。

[0070] 6、COS 经过对动态 PIN 码的验证，决定是否为用户提供服务响应。

[0071] 参照图 5，作为对本发明动态密码验证系统实施例一的进一步改进，在实施例二中该系统还包括一指令处理模块 50，用于对服务请求的指令完整性进行判断，若服务请求的指令完整并需要提升权限，则安全服务模块 20 生成包含有二进制序列的 PIN 码输入信

息。

[0072] 参照图 6, 作为对本发明动态验证系统实施例二的进一步改进, 在实施例三中该系统还包括一缓冲存储模块 60, 用于存储安全服务模块 20 随机产生的二进制序列, 该缓冲存储模块 60 内数据的存储时间可以设置, 并且在二进制序列刷新时被新生成的二进制序列覆盖。

[0073] 进一步, 该系统还包括一刷新计数模块 70, 用于对安全服务模块 20 刷新二进制序列的次数进行计数, 所述二进制序列的刷新次数可以设置, 当超过预定义的刷新次数后, 硬件数字证书载体将进入锁定状态。假定在实际应用中, 预定义二进制序列的刷新次数为三次, 用户每刷新一次二进制序列, 则缓冲存储模块 60 内的二进制序列被安全服务模块 20 新生成的二进制序列覆盖, 同时刷新计数模块 70 的计数器进行减 1 操作, 当用户在三次内未通过动态 PIN 码验证, 则硬件数字证书载体进入锁定模式, 用户将无法进行操作, 需要将硬件数字证书载体拔出后重新插入客户端方能使用。

[0074] 以上是对本发明的较佳实施进行了具体说明, 但本发明创造并不限于所述实施例, 熟悉本领域的技术人员在不违背本发明精神的前提下还可以作出种种的等同变形或替换, 这些等同的变形或替换均包含在本申请权利要求所限定的范围内。

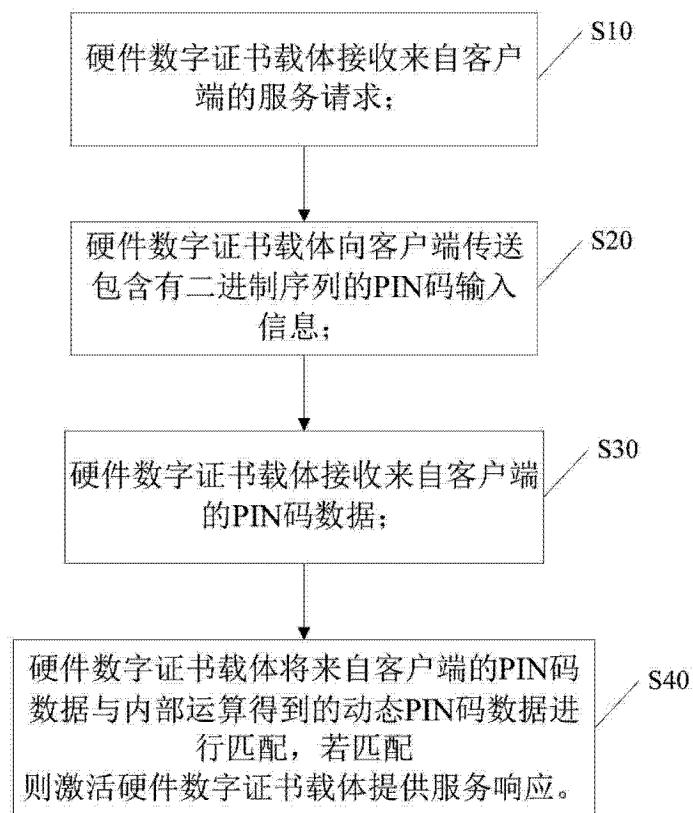


图 1

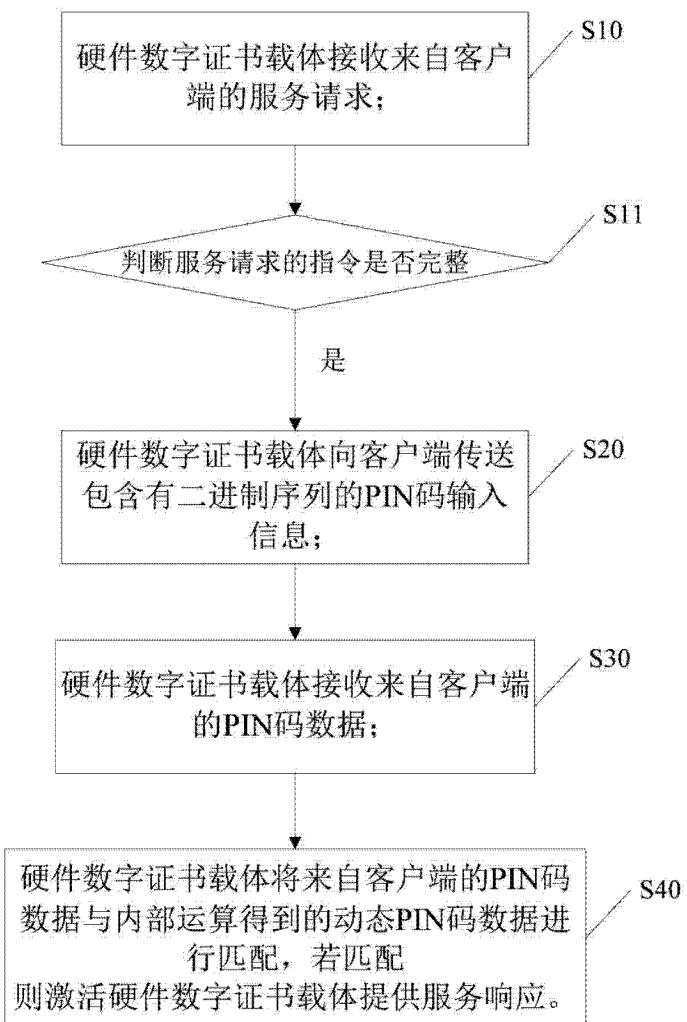


图 2

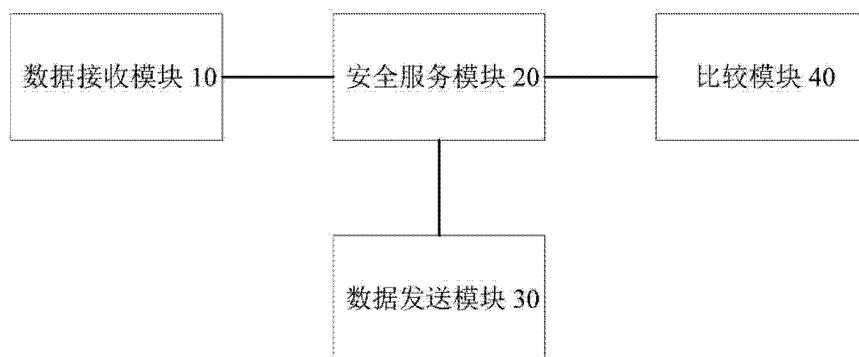


图 3

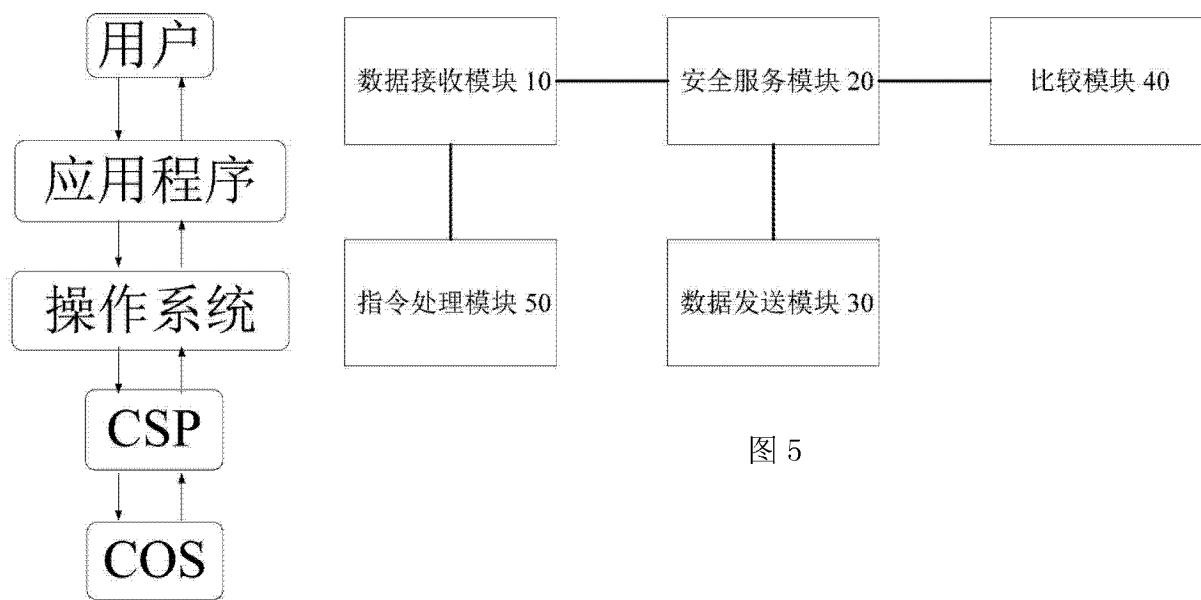


图 4

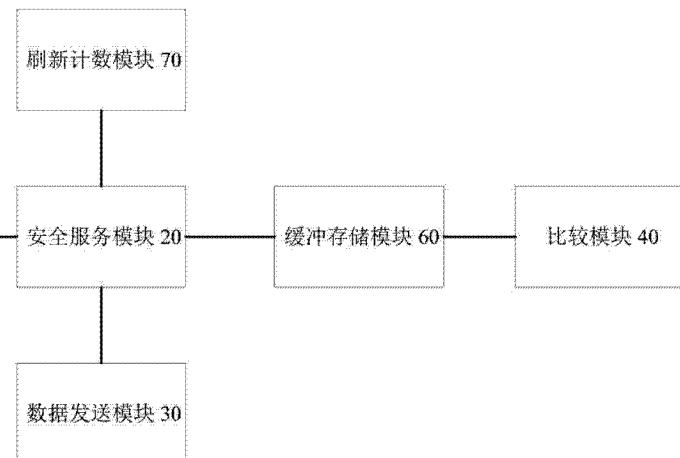


图 5