(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106980580 B
(45)授权公告日 2018.08.03

(21)申请号 201710194677.7
(22)申请日 2017.03.29
(65)同一申请的已公布的文献号
申请公布号 CN 106980580 A
(43)申请公布日 2017.07.25
(73)专利权人 宁夏凯速德科技有限公司
地址 750004 宁夏回族自治区银川市金凤区高新区标准厂房1号楼5层515室
(72)发明人 王以哲
(74)专利代理机构 北京和信华成知识产权代理事务所(普通合伙) 11390
代理人 胡剑辉
(51)Int.Cl.
G06F 12/14(2006.01)
G06F 21/32(2013.01)

审查员 刘芳

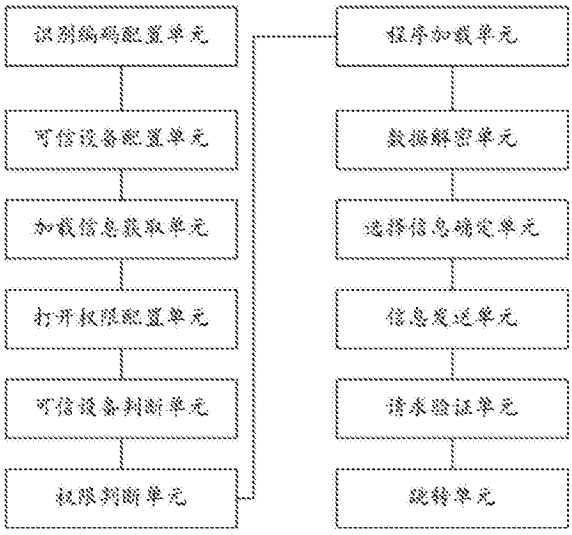
权利要求书2页 说明书6页 附图1页

(54)发明名称

去中心化的移动硬盘加解密方法及系统

(57)摘要

一种去中心化的移动硬盘加解密方法，其包括如下步骤：S1、在远程服务器配置存储移动硬盘对应的唯一识别编码，并在远程服务器中配置多套移动硬盘权限驱动加载程序以及硬盘运行基本驱动加载程序，配置每套权限驱动加载程序对应的文件打开权限；S2、在远程服务器中配置移动硬盘可信设备名单；S3、获取移动硬盘加载信息，将移动硬盘加载信息以及加载对应的设备信息发送到远程服务器；S4、远程服务器配置移动硬盘中合法用户对应的文件打开权限；S5、远程服务器根据设备信息判断是否处于配置的移动硬盘可信设备名单中。



CN 106980580 B

1.一种去中心化的移动硬盘加解密方法，其特征在于，其包括如下步骤：

S1、在远程服务器配置存储移动硬盘对应的唯一识别编码，并在远程服务器中配置多套移动硬盘权限驱动加载程序以及硬盘运行基本驱动加载程序，配置每套权限驱动加载程序对应的文件打开权限；硬盘运行基本驱动加载程序只用于获取用户的验证信息；移动硬盘权限驱动加载程序用于在运行后对硬盘内数据进行恢复和加载，并在每次使用完之后自动销毁；

S2、在远程服务器中配置移动硬盘可信设备名单；

S3、获取移动硬盘加载信息，将移动硬盘加载信息以及加载对应的设备信息发送到远程服务器；

S4、远程服务器配置移动硬盘中合法用户对应的文件打开权限；

S5、远程服务器根据设备信息判断是否处于配置的移动硬盘可信设备名单中，不在可信设备名单中时，跳转到步骤S6；在可信设备名单中时，跳转到步骤S9；

S6、远程服务器向设备下发硬盘运行基本驱动加载程序，设备加载硬盘运行基本驱动加载程序后弹出硬盘运行基本驱动加载程序内置身份验证请求信息，获取用户输入的验证信息并发送给远程服务器，远程服务器对用户输入的验证信息进行验证，根据验证结果判断合法用户对应的文件打开权限，并跳转到步骤S7；

S7、根据合法用户对应的文件打开权限，远程服务器中搜索对应的移动硬盘权限驱动加载程序，并将移动硬盘权限驱动加载程序下发到设备；

S8、设备加载移动硬盘权限驱动加载程序后，根据移动硬盘权限驱动加载程序从移动硬盘中解密移动硬盘权限对应的数据，并且赋予用户相应的权限并结束；

S9、远程服务器在设备上显示设备对应的用户名单，获取用户的对于用户名单的选择信息；

S10、远程服务器根据用户选择的用户名单，将验证信息发送到用户选择的用户对应的移动终端上；

S11、移动终端对用户的请求进行验证，在验证通过后向远程服务器反馈验证通过信息；

S12、远程服务器判断合法用户对应的文件打开权限，并跳转到步骤S7。

2.如权利要求1所述的去中心化的移动硬盘加解密方法，其特征在于，

预先将移动硬盘内数据进行置乱并加密，并配置不同情况下数据恢复规则；

所述步骤S1还包括：

根据每套权限驱动加载程序对应的文件打开权限配置移动硬盘中相对应的数据的恢复规则；

所述步骤S8还包括：

根据文件打开权限配置移动硬盘中相对应的数据的恢复规则对相应数据进行解密并恢复。

3.如权利要求2所述的去中心化的移动硬盘加解密方法，其特征在于，

所述步骤S11中根据移动终端内置指纹验证功能对用户的请求进行验证。

4.一种去中心化的移动硬盘加解密系统，其特征在于，其包括如下单元：

识别编码配置单元，用于在远程服务器配置存储移动硬盘对应的唯一识别编码，并在

远程服务器中配置多套移动硬盘权限驱动加载程序以及硬盘运行基本驱动加载程序，配置每套权限驱动加载程序对应的文件打开权限；硬盘运行基本驱动加载程序只用于获取用户的验证信息；移动硬盘权限驱动加载程序用于在运行后对硬盘内数据进行恢复和加载，并在每次使用完之后自动销毁；

可信设备配置单元，用于在远程服务器中配置移动硬盘可信设备名单；

加载信息获取单元，用于获取移动硬盘加载信息，将移动硬盘加载信息以及加载对应的设备信息发送到远程服务器；

打开权限配置单元，用于通过远程服务器配置移动硬盘中合法用户对应的文件打开权限；

可信设备判断单元，用于通过远程服务器根据设备信息判断是否处于配置的移动硬盘可信设备名单中，不在可信设备名单中时，跳转到步骤S6；在可信设备名单中时，跳转到选择信息确定单元；

权限判断单元，用于通过远程服务器向设备下发硬盘运行基本驱动加载程序，设备加载硬盘运行基本驱动加载程序后弹出硬盘运行基本驱动加载程序内置身份验证请求信息，获取用户输入的验证信息并发送给远程服务器，远程服务器对用户输入的验证信息进行验证，根据验证结果判断合法用户对应的文件打开权限，并跳转到程序加载单元；

程序加载单元，用于根据合法用户对应的文件打开权限，远程服务器中搜索对应的移动硬盘权限驱动加载程序，并将移动硬盘权限驱动加载程序下发到设备；

数据解密单元，用于在设备加载移动硬盘权限驱动加载程序后，根据移动硬盘权限驱动加载程序从移动硬盘中解密移动硬盘权限对应的数据，并且赋予用户相应的权限并结束；

选择信息确定单元，用于通过远程服务器在设备上显示设备对应的用户名单，获取用户的对于用户名单的选择信息；

信息发送单元，用于通过远程服务器根据用户选择的用户名单，将验证信息发送到用户选择的用户对应的移动终端上；

请求验证单元，用于通过移动终端对用户的请求进行验证，在验证通过后向远程服务器反馈验证通过信息；

跳转单元，用于通过远程服务器判断合法用户对应的文件打开权限，并跳转到程序加载单元。

5.如权利要求4所述的去中心化的移动硬盘加解密系统，其特征在于，

预先将移动硬盘内数据进行置乱并加密，并配置不同情况下数据恢复规则；

所述识别编码配置单元还包括：

根据每套权限驱动加载程序对应的文件打开权限配置移动硬盘中相对应的数据的恢复规则；

所述数据解密单元还包括：

根据文件打开权限配置移动硬盘中相对应的数据的恢复规则对相应数据进行解密并恢复。

6.如权利要求5所述的去中心化的移动硬盘加解密系统，其特征在于，

所述请求验证单元中根据移动终端内置指纹验证功能对用户的请求进行验证。

去中心化的移动硬盘加解密方法及系统

技术领域

[0001] 本发明涉及磁盘加解密技术领域，特别涉及一种去中心化的移动硬盘加解密方法及系统。

背景技术

[0002] 在计算机技术迅速发展的今天，硬盘数据的保护变得尤为重要。因此硬盘加密技术也成为了众多技术人员所研究的方向。硬盘加密技术是指将用户数据通过某些可逆的加密算法生成新的加密后数据后，保存到硬盘上的技术。该技术对客户资料，商业机密等重要数据信息进行的高安全性保护，防止了未授权的数据访问。即时硬盘被窃取，也很难读取到硬盘上的重要数据。

[0003] 现有硬盘加密技术方法、装置及系统主要有如下三类：

[0004] 1)在主机端使用加密软件，对用户写入硬盘的数据进行加密和用户认证；

[0005] 2)占用硬盘的空间，增加额外的隐藏分区，将认证系统放入隐藏分区，通过从隐藏分区作为系统启动引导，来完成认证和加密；

[0006] 3)使用硬件加解密数据，但是密钥和密码也存放于磁盘上；

[0007] 但是现有的磁盘安全加密系统存在如下缺陷：第一，若通过纯软件加密，势必降低了系统的性能；第二，密钥和密码存放于磁盘上，增加了破解磁盘数据的可能性；第三，额外增加磁盘加密认证分区，降低了磁盘的利用率；第四，密钥具有唯一性，不利于授权多用户使用；第五，对主机系统存在一定的依赖性，只能支持某些特定架构或者操作系统的主机，如x86(微处理器)或者IA64(处理器)系统；第六，若需要自带操作系统及文件系统，涉及版权问题和兼容性问题。

[0008] 综上可知，现有硬盘加密技术在实际使用上，显然存在不便与缺陷，所以有必要加以改进。

发明内容

[0009] 有鉴于此，本发明提出一种去中心化的移动硬盘加解密方法及系统。

[0010] 一种去中心化的移动硬盘加解密方法，其包括如下步骤：

[0011] S1、在远程服务器配置存储移动硬盘对应的唯一识别编码，并在远程服务器中配置多套移动硬盘权限驱动加载程序以及硬盘运行基本驱动加载程序，配置每套权限驱动加载程序对应的文件打开权限；

[0012] S2、在远程服务器中配置移动硬盘可信设备名单；

[0013] S3、获取移动硬盘加载信息，将移动硬盘加载信息以及加载对应的设备信息发送到远程服务器；

[0014] S4、远程服务器配置移动硬盘中合法用户对应的文件打开权限；

[0015] S5、远程服务器根据设备信息判断是否处于配置的移动硬盘可信设备名单中，不在可信设备名单中时，跳转到步骤S6；在可信设备名单中时，跳转到步骤S9；

[0016] S6、远程服务器向设备下发硬盘运行基本驱动加载程序，设备加载硬盘运行基本驱动加载程序后弹出硬盘运行基本驱动加载程序内置身份验证请求信息，获取用户输入的验证信息并发送给远程服务器，远程服务器对用户验证的验证信息进行验证，根据验证结果判断合法用户对应的文件打开权限，并跳转到步骤S7；

[0017] S7、根据合法用户对应的文件打开权限，远程服务器中搜索对应的移动硬盘权限驱动加载程序，并将移动硬盘权限驱动加载程序下发到设备；

[0018] S8、设备加载移动硬盘权限驱动加载程序后，根据移动硬盘权限驱动加载程序从移动硬盘中解密移动硬盘权限对应的数据，并且赋予用户相应的权限并结束；

[0019] S9、远程服务器在设备上显示设备对应的使用者名单，获取用户的对于使用者名单的选择信息；

[0020] S10、远程服务器根据用户选择的使用者名单，将验证信息发送到用户选择的使用者对应的移动终端上；

[0021] S11、移动终端对用户的请求进行验证，在验证通过后向远程服务器反馈验证通过信息；

[0022] S12、远程服务器根据判断合法用户对应的文件打开权限，并跳转到步骤S7。

[0023] 在本发明所述的去中心化的移动硬盘加解密方法中，

[0024] 预先将移动硬盘内数据进行置乱并加密，并配置不同情况下数据恢复规则；

[0025] 所述步骤S1还包括：

[0026] 根据配置每套权限驱动加载程序对应的文件打开权限，根据文件打开权限配置移动硬盘中相对应的数据的恢复规则；

[0027] 所述步骤S8还包括：

[0028] 根据文件打开权限配置移动硬盘中相对应的数据的恢复规则对相应数据进行解密并恢复。

[0029] 在本发明所述的去中心化的移动硬盘加解密方法中，

[0030] 所述步骤S11中根据移动终端内置指纹验证功能对用户的请求进行验证。

[0031] 一种去中心化的移动硬盘加解密系统，其包括如下单元：

[0032] 识别编码配置单元，用于在远程服务器配置存储移动硬盘对应的唯一识别编码，并在远程服务器中配置多套移动硬盘权限驱动加载程序以及硬盘运行基本驱动加载程序，配置每套权限驱动加载程序对应的文件打开权限；

[0033] 可信设备配置单元，用于在远程服务器中配置移动硬盘可信设备名单；

[0034] 加载信息获取单元，用于获取移动硬盘加载信息，将移动硬盘加载信息以及加载对应的设备信息发送到远程服务器；

[0035] 打开权限配置单元，用于通过远程服务器配置移动硬盘中合法用户对应的文件打开权限；

[0036] 可信设备判断单元，用于通过远程服务器根据设备信息判断是否处于配置的移动硬盘可信设备名单中，不在可信设备名单中时，跳转到步骤S6；在可信设备名单中时，跳转到选择信息确定单元；

[0037] 权限判断单元，用于通过远程服务器向设备下发硬盘运行基本驱动加载程序，设备加载硬盘运行基本驱动加载程序后弹出硬盘运行基本驱动加载程序内置身份验证请求

信息，获取用户输入的验证信息并发送给远程服务器，远程服务器对用户验证的验证信息进行验证，根据验证结果判断合法用户对应的文件打开权限，并跳转到程序加载单元；

[0038] 程序加载单元，用于根据合法用户对应的文件打开权限，远程服务器中搜索对应的移动硬盘权限驱动加载程序，并将移动硬盘权限驱动加载程序下发到设备；

[0039] 数据解密单元，用于在设备加载移动硬盘权限驱动加载程序后，根据移动硬盘权限驱动加载程序从移动硬盘中解密移动硬盘权限对应的数据，并且赋予用户相应的权限并结束；

[0040] 选择信息确定单元，用于通过远程服务器在设备上显示设备对应的使用者名单，获取用户的对于使用者名单的选择信息；

[0041] 信息发送单元，用于通过远程服务器根据用户选择的使用者名单，将验证信息发送到用户选择的使用者对应的移动终端上；

[0042] 请求验证单元，用于通过移动终端对用户的请求进行验证，在验证通过后向远程服务器反馈验证通过信息；

[0043] 跳转单元，用于通过远程服务器根据判断合法用户对应的文件打开权限，并跳转到程序加载单元。

[0044] 在本发明所述的去中心化的移动硬盘加解密系统中，

[0045] 预先将移动硬盘内数据进行置乱并加密，并配置不同情况下数据恢复规则；

[0046] 所述识别编码配置单元还包括：

[0047] 根据配置每套权限驱动加载程序对应的文件打开权限，根据文件打开权限配置移动硬盘中相对应的数据的恢复规则；

[0048] 所述数据解密单元还包括：

[0049] 根据文件打开权限配置移动硬盘中相对应的数据的恢复规则对相应数据进行解密并恢复。

[0050] 在本发明所述的去中心化的移动硬盘加解密系统中，

[0051] 所述请求验证单元中根据移动终端内置指纹验证功能对用户的请求进行验证。

[0052] 本发明提供的去中心化的移动硬盘加解密方法及系统，相对于现有技术，能够实现将硬盘的验证放到可信的远端，避免了本地设备被破解后造成的硬盘数据泄密。

附图说明

[0053] 图1是本发明实施例的去中心化的移动硬盘加解密系统结构框图。

具体实施方式

[0054] 如图1所示，本发明实施例一种去中心化的移动硬盘加解密方法，其包括如下步骤：

[0055] S1、在远程服务器配置存储移动硬盘对应的唯一识别编码，并在远程服务器中配置多套移动硬盘权限驱动加载程序以及硬盘运行基本驱动加载程序，配置每套权限驱动加载程序对应的文件打开权限；

[0056] 硬盘运行基本驱动加载程序只用于获取用户的验证信息；移动硬盘权限驱动加载程序用于在运行后对硬盘内数据进行恢复和加载。并在每次使用完之后自动销毁，通过移

动硬盘权限驱动加载程序内置的定期器实现。由于将移动硬盘权限驱动加载程序放在云端，不在移动硬盘内部，也避免了移动硬盘本身被破解造成的数据泄密的风险。

[0057] S2、在远程服务器中配置移动硬盘可信设备名单；

[0058] S3、获取移动硬盘加载信息，将移动硬盘加载信息以及加载对应的设备信息发送到远程服务器；

[0059] S4、远程服务器配置移动硬盘中合法用户对应的文件打开权限；

[0060] S5、远程服务器根据设备信息判断是否处于配置的移动硬盘可信设备名单中，不在可信设备名单中时，跳转到步骤S6；在可信设备名单中时，跳转到步骤S9；

[0061] S6、远程服务器向设备下发硬盘运行基本驱动加载程序，设备加载硬盘运行基本驱动加载程序后弹出硬盘运行基本驱动加载程序内置身份验证请求信息，获取用户输入的验证信息并发送给远程服务器，远程服务器对用户验证的验证信息进行验证，根据验证结果判断合法用户对应的文件打开权限，并跳转到步骤S7；

[0062] S7、根据合法用户对应的文件打开权限，远程服务器中搜索对应的移动硬盘权限驱动加载程序，并将移动硬盘权限驱动加载程序下发到设备；

[0063] S8、设备加载移动硬盘权限驱动加载程序后，根据移动硬盘权限驱动加载程序从移动硬盘中解密移动硬盘权限对应的数据，并且赋予用户相应的权限并结束；

[0064] S9、远程服务器在设备上显示设备对应的使用者名单，获取用户的对于使用者名单的选择信息；

[0065] S10、远程服务器根据用户选择的使用者名单，将验证信息发送到用户选择的使用者对应的移动终端上；

[0066] S11、移动终端对用户的请求进行验证，在验证通过后向远程服务器反馈验证通过信息；

[0067] S12、远程服务器根据判断合法用户对应的文件打开权限，并跳转到步骤S7。

[0068] 在本发明所述的去中心化的移动硬盘加解密方法中，

[0069] 预先将移动硬盘内数据进行置乱并加密，并配置不同情况下数据恢复规则；

[0070] 通过对移动硬盘内数据进行置乱并加密，避免了数据的丢失风险。

[0071] 所述步骤S1还包括：

[0072] 根据配置每套权限驱动加载程序对应的文件打开权限，根据文件打开权限配置移动硬盘中相对应的数据的恢复规则；

[0073] 所述步骤S8还包括：

[0074] 根据文件打开权限配置移动硬盘中相对应的数据的恢复规则对相应数据进行解密并恢复。

[0075] 在本发明所述的去中心化的移动硬盘加解密方法中，

[0076] 所述步骤S11中根据移动终端内置指纹验证功能对用户的请求进行验证。

[0077] 一种去中心化的移动硬盘加解密系统，其包括如下单元：

[0078] 识别编码配置单元，用于在远程服务器配置存储移动硬盘对应的唯一识别编码，并在远程服务器中配置多套移动硬盘权限驱动加载程序以及硬盘运行基本驱动加载程序，配置每套权限驱动加载程序对应的文件打开权限；

[0079] 可信设备配置单元，用于在远程服务器中配置移动硬盘可信设备名单；

[0080] 加载信息获取单元，用于获取移动硬盘加载信息，将移动硬盘加载信息以及加载对应的设备信息发送到远程服务器；

[0081] 打开权限配置单元，用于通过远程服务器配置移动硬盘中合法用户对应的文件打开权限；

[0082] 可信设备判断单元，用于通过远程服务器根据设备信息判断是否处于配置的移动硬盘可信设备名单中，不在可信设备名单中时，跳转到步骤S6；在可信设备名单中时，跳转到选择信息确定单元；

[0083] 权限判断单元，用于通过远程服务器向设备下发硬盘运行基本驱动加载程序，设备加载硬盘运行基本驱动加载程序后弹出硬盘运行基本驱动加载程序内置身份验证请求信息，获取用户输入的验证信息并发送给远程服务器，远程服务器对用户验证的验证信息进行验证，根据验证结果判断合法用户对应的文件打开权限，并跳转到程序加载单元；

[0084] 程序加载单元，用于根据合法用户对应的文件打开权限，远程服务器中搜索对应的移动硬盘权限驱动加载程序，并将移动硬盘权限驱动加载程序下发到设备；

[0085] 数据解密单元，用于在设备加载移动硬盘权限驱动加载程序后，根据移动硬盘权限驱动加载程序从移动硬盘中解密移动硬盘权限对应的数据，并且赋予用户相应的权限并结束：

[0086] 选择信息确定单元，用于通过远程服务器在设备上显示设备对应的使用者名单，获取用户的对于使用者名单的选择信息；

[0087] 信息发送单元，用于通过远程服务器根据用户选择的使用者名单，将验证信息发送到用户选择的使用者对应的移动终端上；

[0088] 请求验证单元，用于通过移动终端对用户的请求进行验证，在验证通过后向远程服务器反馈验证通过信息；

[0089] 跳转单元，用于通过远程服务器根据判断合法用户对应的文件打开权限，并跳转到程序加载单元。

[0090] 在本发明所述的去中心化的移动硬盘加解密系统中，

[0091] 预先将移动硬盘内数据进行置乱并加密，并配置不同情况下数据恢复规则；

[0092] 所述识别编码配置单元还包括：

[0093] 根据配置每套权限驱动加载程序对应的文件打开权限，根据文件打开权限配置移动硬盘中相对应的数据的恢复规则；

[0094] 所述数据解密单元还包括：

[0095] 根据文件打开权限配置移动硬盘中相对应的数据的恢复规则对相应数据进行解密并恢复。

[0096] 在本发明所述的去中心化的移动硬盘加解密系统中，

[0097] 所述请求验证单元中根据移动终端内置指纹验证功能对用户的请求进行验证。

[0098] 本发明提供的去中心化的移动硬盘加解密方法及系统，相对于现有技术，能够实现将硬盘的验证放到可信的远端，避免了本地设备被破解后造成的硬盘数据泄密。

[0099] 结合本文中所公开的实施例描述的方法或算法的可以直接用硬件、处理器执行的软件模块，或者二者的结合来实施。软件模块可以置于随机储存器、内存、只读存储器、电可编程ROM、电可擦除可编程ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的

任意其他形式的存储介质中。

[0100] 可以理解的是，对于本领域的普通技术人员来说，可以根据本发明的技术构思做出其它各种相应的改变与变形，而所有这些改变与变形都应属于本发明权利要求的保护范围。

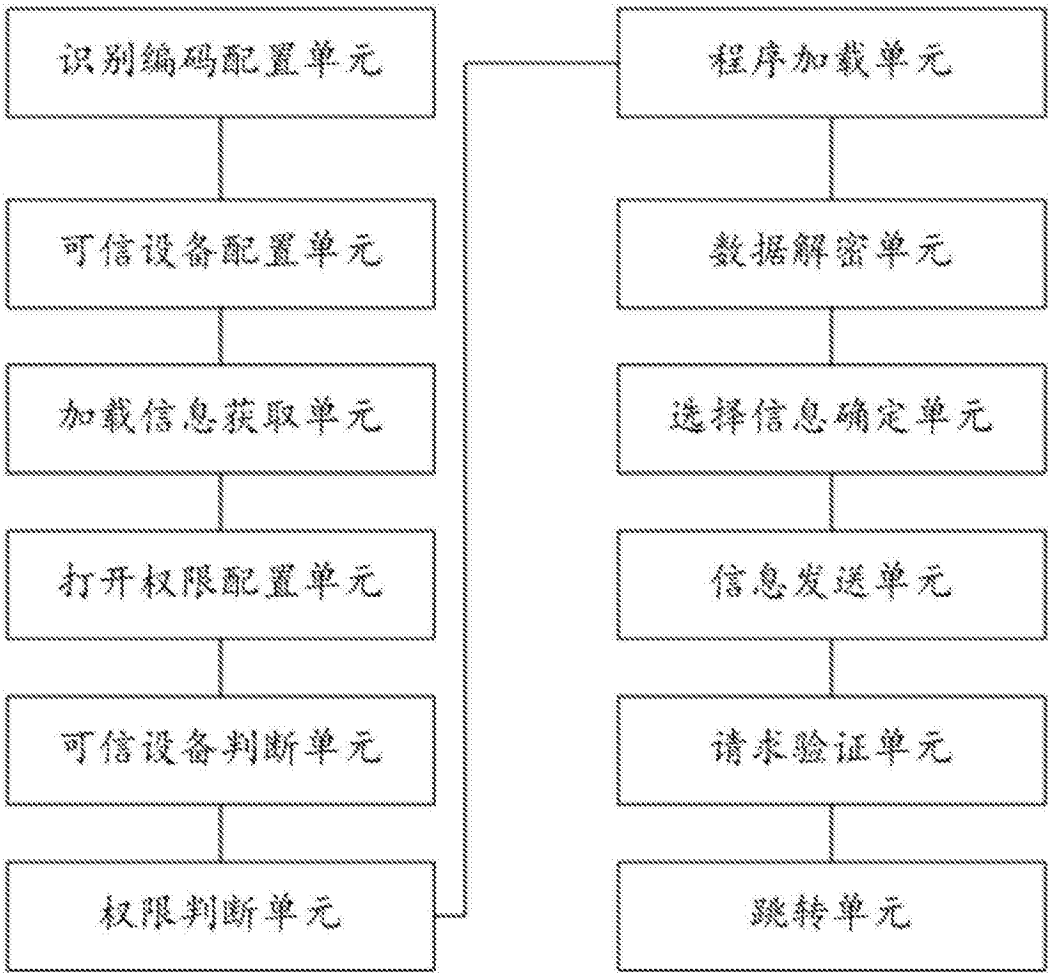

识别编码配置单元
可信设备配置单元
加载信息获取单元
打开权限配置单元
可信设备判断单元
权限判断单元
程序加载单元
数据解密单元
选择信息确定单元
信息发送单元
请求验证单元
跳转单元

图1