(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101800738 A
(43)申请公布日 2010.08.11

(21)申请号 200910214601.1

(22)申请日 2009.12.31

(71)申请人 暨南大学
地址 510632 广东省广州市黄埔大道西 601 号

(72)发明人 姚国祥 罗伟其 官全龙 梁德恒 魏林锋 邱振谋

(74)专利代理机构 广州市华学知识产权代理有限公司 44245
代理人 陈燕娴

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 12/28(2006.01)

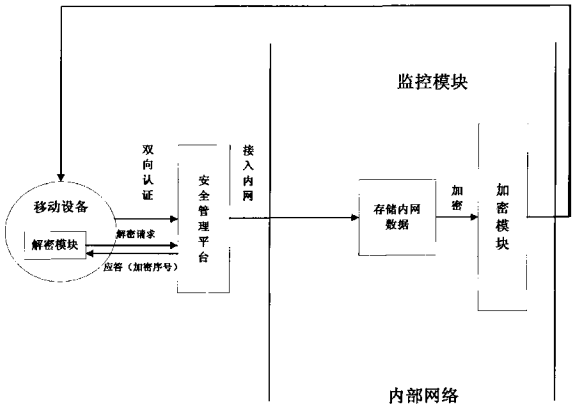
权利要求书 2 页 说明书 7 页 附图 3 页

(54)发明名称

一种移动设备安全访问与存储内网数据的实现系统及方法

(57)摘要

一种移动设备安全访问与存储内网数据的实现系统及方法，方法包括：安全管理平台判断移动设备是否已注册，对已注册的移动设备进行双向认证，认证成功后允许接入内网，拒绝没注册和认证失败的移动设备接入内网；监控模块在发现移动设备要将内网中的内网数据存储到自身上时，调用加密模块；加密模块在监控模块的监控下，根据内网数据的保密等级选择相应的加密方法，对要存储到移动设备的内网数据进行加密；当存储在移动设备中的加密数据需要解密时，解密模块向内网中的监控模块询问该加密数据是否是涉密数据，然后选择相应的解密方法对加密数据进行解密。本发明针对不同保密等级的数据实施不同的加解密方法，提高了加解密效率和数据保密性；综合运用双向认证方法和加解密方法，提高了内网数据的安全性。



CN 101800738 A

1. 一种移动设备安全访问与存储内网数据的实现系统，其特征在于，包括：

接入内网的安全管理平台，用于对要接入内网的移动设备进行注册和双向认证，对被允许访问内网的移动设备进行注册，对已注册的移动设备进行双向认证，允许双向认证成功后的移动设备接入内网，拒绝没有注册和双向认证失败的移动设备接入内网；

监控模块，其运行在内网，用于对接入内网的移动设备进行监控，保存移动设备访问内网和操作内网数据的监控记录，并在发现移动设备要存储内网数据时调用加密模块；

加密模块，其运行在内网，需要在监控模块的监控下运作，用于根据内网数据的保密等级选择相应的加密技术，对要存储到移动设备的内网数据进行加密；

解密模块，其运行在移动设备，用于对移动设备的加密数据采用与所使用的加密技术对应的解密方法进行解密。

2. 一种移动设备安全访问与存储内网数据的实现方法，其特征在于，首先，安全管理平台对移动设备进行注册，当移动设备请求接入内网时，进行如下操作：

(1) 安全管理平台判断该移动设备是否已注册，对已注册的移动设备进行双向认证，允许双向认证成功后的移动设备接入内网，拒绝没有注册和双向认证失败的移动设备接入内网；

(2) 监控模块在发现移动设备要将内网中的内网数据存储到自身上时，调用加密模块；

(3) 加密模块在监控模块的监控下，根据内网数据的保密等级选择相应的加密方法，对要存储到移动设备的内网数据进行加密；

(4) 当存储在移动设备中的加密数据需要解密时，解密模块采用与加密数据所使用的加密方法对应的解密方法对加密数据进行解密。

3. 根据权利要求 2 所述的一种移动设备安全访问与存储内网数据的实现方法，其特征在于：所述安全管理平台对移动设备进行注册，为预先进行注册，即由内部网络管理员操作安全管理平台对所有被允许接入内网的移动设备进行统一注册，该注册方法具体为：

安全管理平台获取移动设备的硬件信息，检测该获取的硬件信息是否有效，如无效则拒绝注册，如有效则生成该移动设备对应的网络标识和随机产生的加密序号，记录后发送给该移动设备进行存储。

4. 根据权利要求 3 所述的一种移动设备安全访问与存储内网数据的实现方法，其特征在于，步骤 1 所述安全管理平台判断该移动设备是否已注册，对已注册的移动设备进行双向认证，其方法具体为：

(1.1) 安全管理平台读取该移动设备的硬件信息，以检验该设备是否已注册登记；如果没有注册则拒绝该移动设备接入内网，如果以注册，则安全管理平台向其发送所记录的，并与所读取的移动设备的硬件信息关联的网络标识；

(1.2) 移动设备接收到网络标识后，对比该网络标识与注册时所存储的网络标识是否相同，如果相同将向安全管理平台发送注册时所存储的加密序号，然后执行步骤 1.3 操作；否则，不发送加密序号，至此，双向认证失败，安全管理平台拒绝移动设备接入内网；

(1.3) 安全管理平台对比所接收到的加密序号是否与设备注册登记时所记录的该移动设备的加密序号相同；如果相同，则双向认证成功，允许移动设备接入内网；否则，拒绝移动设备接入内网。

5. 根据权利要求 2 至 4 任一项所述的一种移动设备安全访问与存储内网数据的实现方法，其特征在于：所述监控模块还对接入内网的移动设备进行监控，保存移动设备访问内网和操作内网数据的监控记录。

6. 根据权利要求 5 所述的一种移动设备安全访问与存储内网数据的实现方法，其特征在于：步骤 3 所述加密模块在监控模块的监控下，根据内网数据的保密等级选择相应的加密方法，对要存储到移动设备的内网数据进行加密，其方法具体为：监控模块判断该内网数据是否为涉密内网数据并告知加密模块，加密模块对非涉密内网数据采用对称加密方法，对涉密内网数据采用混合加密方法。

7. 根据权利要求 6 所述的一种移动设备安全访问与存储内网数据的实现方法，其特征在于：所述对称加密方法为：用户在移动设备设置密码，将该密码映射出密钥对，该密钥对包括一个公钥 PK 和一个为私钥 SK，并将该密钥对发送给内网中的加密模块进行存储；内网中的加密模块用公钥 PK 进行加密，最后将该已加密的非涉密内网数据发送到移动设备；

所述混合加密方法具体为：用户在移动设备设置密码，移动设备将该密码映射出一密钥对，该密钥对包括一个公钥 PK 和一个为私钥 SK，并将该密钥对发送给内网中的加密模块进行存储；加密模块首先生成对称密钥 K 对涉密内网数据进行对称加密，然后用所存储的公钥 PK 对对称密钥 K 进行非对称加密，最后将已加密的涉密内网数据和已加密的对称加密所使用的密钥 K 一起发送到移动设备；

步骤 4 所述解密模块对加密数据进行解密具体为：解密模块首先向内网中的监控模块询问该加密数据是否为涉密内网数据；如不是则采用私钥 SK 对该加密数据进行解密，如是则首先采用私钥 SK 对对称密钥 K 进行解密，然后采用解密出的对称密钥 K 对已加密的涉密内网数据进行解密。

8. 根据权利要求 7 所述的一种移动设备安全访问与存储内网数据的实现方法，其特征在于：所述对称加密方法具体采用 AES-256bit 加密方法，所述非对称加密方法具体采用 ECC 加密方法。

9. 根据权利要求 3 或 4 所述的一种移动设备安全访问与存储内网数据的实现方法，其特征在于：步骤 4 所述当存储在移动设备中的加密数据需要解密时，解密模块采用与加密数据所使用的加密方法对应的解密方法对加密数据进行解密，在进行解密之前，还包括以下操作：移动设备向安全管理平台发送解密请求，安全管理平台返回与该移动设备硬件信息关联的加密序号，移动设备将返回的加密序号与注册时所存储的加密序号进行对比；若两者相同，则认为已接入该内网，允许加密数据被解密，否则，认为没有接入该内网，不允许加密数据被解密。

一种移动设备安全访问与存储内网数据的实现系统及方法

技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种实现移动设备安全访问与存储内网数据的实现系统及方法，更具体的说是涉及了移动设备与内网之间的双向认证技术和数据加解密技术。

背景技术

[0002] 随着社会信息化的深入推进，以及移动设备和网络的不断发展，移动设备在社会各领域中日益普及。由于移动设备具有携带方便、使用灵活等优点，使其在信息化过程中得到了迅速发展。因此，移动设备在单位内部得到使用也成为一个趋势。与此同时，在内网中使用移动设备（如便携式电脑、手机和 PDA 等）也引发了一系列安全性问题。

[0003] 其中，常见的安全问题是：未经许可的移动设备连接到单位内网上，如果移动设备此时已感染了病毒，病毒就能轻易地绕过在单位内网的网关上已经部署的防病毒软件和防火墙，对单位内网进行攻击，甚至导致内网秘密数据的外泄。据蓝代斯克软件公司委托第三方调查机构进行的一项调查结果表明，60％的单位还没有有效的办法来扫描需要连接到单位网络的设备，也没有办法隔离未满足本单位安全要求的任何接入系统。此外，移动设备可能存储了单位内部的保密信息，而由于移动设备的丢失、失窃等原因使单位的保密信息和重要文件泄露，将会带来不可估量的损失和危害。

[0004] 目前，市场上的移动设备数据安全加密产品分为以下几类：一般资料加密产品（如：Word、WinZip 自带的设置密码）；安全文件夹类加密产品（如：安科 Strongbox）；“防火墙”类加密产品（通常我们称之为第一代权限控制产品）；格式转换类加密产品（通常我们称之为第二代权限控制产品）；安全域控制类加密产品（通常我们称之为第三代权限控制产品，如：安科 cofferdisk）。但这些产品中大多数都没有实现对移动设备的双向认证功能，而且也没有针对不同保密等级的数据采用不同的加解密技术，因此，在安全和效率方面还有待进一步改善。上述产品可能存在以下问题：

[0005] (1) 使用简单的单向认证，如仅仅通过内网对移动设备的单向认证，存在移动设备与外网设备通信的可能。因此，保存在移动设备的内网数据可能外泄，而且非常容易受到假冒攻击和中间人攻击。

[0006] (2) 使用双向认证，但移动设备必须通过可信任的第三方证明身份并获得与身份对应的私钥。此方法必须依赖于第三方认证中心，从而也导致内网数据的安全性存在隐患，而且认证效率不高。

[0007] (3) 对于保存到移动设备的内网数据没有进行保密等级分类，对所有数据的加密均使用同一种加密算法，可能造成对涉密数据使用了简单的加密算法，也可能对非涉密数据使用了复杂的加密算法。因此，存在加密效率低下和数据容易被解密的问题。

[0008] 因此，为了让移动设备在单位内网得到安全使用，人们急需一种更安全、更有效的移动设备与内网之间的双向认证技术，以确保连接到内网的移动设备是已被授权连接的，并且确保它满足内网安全要求和认证效率要求。同时，需要针对不同保密等级的数据采用

不同的加解密技术，确保从内网复制到移动设备的数据已进行高效加密。已加密数据只有在内网才能解密和查看，在外网无法解密，从而保证了移动设备中存储内网信息的安全性和保密性。

发明内容

[0009] 本发明的目的在于提供一种移动设备安全访问与存储内网数据的实现系统，本发明针对不同保密等级的数据实施不同的加解密方法，从而提高了数据加解密的效率和数据的保密性；通过综合运用本发明的双向认证方法和加解密方法，提高了内网数据的安全性。

[0010] 本发明的再一目的是提供一种移动设备安全访问与存储内网数据的实现方法。

[0011] 本发明目的通过下述技术方案实现：一种移动设备安全访问与存储内网数据的实现系统，包括：

[0012] 接入内网的安全管理平台，用于对要接入内网的移动设备进行注册和双向认证，对被允许访问内网的移动设备进行注册，对已注册的移动设备进行双向认证，允许双向认证成功后的移动设备接入内网，拒绝没有注册和双向认证失败的移动设备接入内网；

[0013] 监控模块，其运行在内网，用于对接入内网的移动设备进行监控，保存移动设备访问内网和操作内网数据的监控记录，并在发现移动设备要存储内网数据时调用加密模块；

[0014] 加密模块，其运行在内网，需要在监控模块的监控下运作，用于根据内网数据的保密等级选择相应的加密技术，对要存储到移动设备的内网数据进行加密；

[0015] 解密模块，其运行在移动设备，用于对移动设备的加密数据采用与所使用的加密技术对应的解密方法进行解密。

[0016] 一种移动设备安全访问与存储内网数据的实现方法，首先，安全管理平台对移动设备进行注册，该注册可以预先进行，也可以在移动设备请求接入内网时进行，当移动设备请求接入内网时，本发明进行如下操作：

[0017] 1. 安全管理平台判断该移动设备是否已注册，对已注册的移动设备进行双向认证，允许双向认证成功后的移动设备接入内网，拒绝没有注册和双向认证失败的移动设备接入内网；

[0018] 2. 监控模块在发现移动设备要将内网中的内网数据存储到自身上时，调用加密模块；

[0019] 3. 加密模块在监控模块的监控下，根据内网数据的保密等级选择相应的加密方法，对要存储到移动设备的内网数据进行加密；

[0020] 4. 当存储在移动设备中的加密数据需要解密时，解密模块采用与加密数据所使用的加密方法对应的解密方法对加密数据进行解密。

[0021] 上述方法中，所述安全管理平台对移动设备进行注册，优选为预先进行注册，即由内网管理员操作安全管理平台对所有被允许接入内网的移动设备进行统一注册。该注册方法具体为：

[0022] 安全管理平台获取移动设备的硬件信息，如设备序列号、型号和生产商等，检测该获取的硬件信息是否有效，如无效则拒绝注册，如有效则生成该移动设备对应的网络标识和随机产生的加密序号，记录后发送给该移动设备进行存储。所述网络标识是作为双向认证的私钥固化在移动设备中，而所述加密序号存储在移动设备的加密区，用于识别发送该

加密序号的具体内网。

[0023] 对应于上述注册的优选方法，步骤 1 所述安全管理平台判断该移动设备是否已注册，对已注册的移动设备进行双向认证，其方法具体为：

[0024] 1.1 安全管理平台读取该移动设备的硬件信息，如设备序列号、型号和生产商等，以检验该设备是否已注册登记；如果没有注册则拒绝该移动设备接入内网，如果已注册，则安全管理平台向其发送所记录的，并与所读取的移动设备的硬件信息关联的网络标识；

[0025] 1.2 移动设备接收到网络标识后，对比该网络标识与注册时所存储的网络标识是否相同，如果相同将向安全管理平台发送注册时所存储的加密序号，然后执行步骤 1.3 操作；否则，不发送加密序号，至此，双向认证失败，安全管理平台拒绝移动设备接入内网；

[0026] 1.3 安全管理平台对比所接收到的加密序号是否与设备注册登记时所记录的该移动设备的加密序号相同；如果相同，则双向认证成功，允许移动设备接入内网；否则，拒绝移动设备接入内网。

[0027] 上述方法中，所述监控模块还可以对接入内网的移动设备进行监控，保存移动设备访问内网和操作内网数据的监控记录，以便为以后的审计工作所使用。

[0028] 上述方法中，步骤 3 所述加密模块在监控模块的监控下，根据内网数据的保密等级选择相应的加密方法，对要存储到移动设备的内网数据进行加密，优选为：监控模块判断该内网数据是否为涉密内网数据并告知加密模块，加密模块对非涉密内网数据采用对称加密方法，对涉密内网数据采用混合加密方法。由于对称加密方法及其所对应的解密方法效率高，而混合加密方法及其所对应的解密方法又能保证涉密内网数据的安全性，从而从整体上实现了数据加解密效率和数据保密性的提高。

[0029] 所述对称加密方法优选为：用户在移动设备设置密码，将该密码映射出密钥对，该密钥对包括一个公钥 PK 和一个为私钥 SK，并将该密钥对发送给内网中的加密模块进行存储；内网中的加密模块用公钥 PK 进行加密，最后将该已加密的非涉密内网数据发送到移动设备。

[0030] 上述方法中，所述混合加密方法优选为：先对涉密内网数据采用对称加密方法进行加密，然后针对该对称加密所使用的密钥使用非对称加密方法进行加密，最后将已加密的涉密内网数据和已加密的对称加密所使用的密钥一起发送到移动设备。相应的，步骤 4 所述解密模块对已加密的涉密内网数据进行解密，首先采用非对称加密方法解密出对称加密所使用的密钥，然后采用该对称加密所使用的密钥对已加密的涉密内网数据进行解密。

[0031] 上述混合加密方法具体为：用户在移动设备设置密码，移动设备将该密码映射出一密钥对，该密钥对包括一个公钥 PK 和一个为私钥 SK，并将该密钥对发送给内网中的加密模块进行存储；加密模块首先生成对称密钥 K 对涉密内网数据进行对称加密，然后用所存储的公钥 PK 对对称密钥 K 进行非对称加密，最后将已加密的涉密内网数据和已加密的对称加密所使用的密钥 K 一起发送到移动设备。

[0032] 相对于上述加密方法的具体方法，步骤 4 所述解密模块对加密数据进行解密具体为：解密模块首先向内网中的监控模块询问该加密数据是否为涉密内网数据；如不是则采用私钥 SK 对该加密数据进行解密，如是则首先采用私钥 SK 对对称密钥 K 进行解密，然后采用解密出的对称密钥 K 对已加密的涉密内网数据进行解密。

[0033] 上述方法中，步骤 4 所述当存储在移动设备中的加密数据需要解密时，解密模块

采用与加密数据所使用的加密方法对应的解密方法对加密数据进行解密，在进行解密之前，还可以包括以下操作：移动设备向安全管理平台发送解密请求，安全管理平台返回与该移动设备硬件信息关联的加密序号，移动设备将返回的加密序号与注册时所存储的加密序号进行对比；若两者相同，则认为已接入该内网，允许加密数据被解密，否则，认为没有接入该内网，不允许加密数据被解密。

[0034] 所述对称加密方法具体采用 AES-256bit 加密方法，即采用分组长度为 128bit，密钥长度为 256bit 的 AES 加密方法。

[0035] 所述非对称加密方法具体采用 ECC 加密方法。

[0036] 本发明相对于现有技术具有以下优点：

[0037] (1) 本发明所采用的双向认证技术，安全管理平台通过发送网络标识给移动设备以实现移动设备对内网的认证，移动设备再发送加密序号给安全管理平台以实现内网对移动设备的认证。这样做能够抵御假冒攻击和拒绝攻击，具有较高的安全性，此外，不需要依赖于第三方认证中心，具有较高的认证效率。

[0038] (2) 本发明中的加密模块对内网数据进行不同的加密处理，针对非涉密数据使用对称密钥加密方法，针对涉密数据使用混合加密方法，这样做能够有效地提高加解密效率。

[0039] (3) 本发明中的监控模块对接入内网的移动设备进行监控，并详细记录移动设备对内网数据的操作，以便为以后的审计工作提供数据，这有助于追踪内网数据泄露的源头。

[0040] (4) 移动设备在对加密数据进行解密之前，还可以包括以下操作：移动设备向安全管理平台发送解密请求，安全管理平台返回与该移动设备硬件信息关联的加密序号，移动设备将返回的加密序号与注册时所存储的加密序号进行对比；若两者相同，则认为已接入该内网，允许加密数据被解密，否则，认为没有接入该内网，不允许加密数据被解密。这样就使得已加密数据只能在执行加密的内网中才能解密，在其他网络中不能解密，从而提高了数据加解密的效率和数据的保密性。

附图说明

[0041] 图 1 为本发明一种移动设备安全访问与存储内网数据的实现系统的结构示意图；

[0042] 图 2 为本发明移动设备在内网注册的工作流程图；

[0043] 图 3 为本发明移动设备与内网之间双向认证的工作流程图；

[0044] 图 4 为本发明移动设备存储内网数据的工作流程图。

具体实施方式

[0045] 下面结合实施例及附图，对本发明作进一步详细说明，但本发明的实施方式不限于此。

[0046] 实施例

[0047] 如图 1 所示，一种移动设备安全访问与存储内网数据的实现系统，包括：

[0048] 接入内网的安全管理平台，用于对要接入内网的移动设备进行注册和双向认证，对被允许访问内网的移动设备进行注册，对已注册的移动设备进行双向认证，允许双向认证成功后的移动设备接入内网并受监控模块监控，拒绝没有注册和双向认证失败的移动设备接入内网，使得移动设备如果没有经过该平台认证处理将无法与内网和计算机设备进行

信息交换；

[0049] 监控模块，其运行在内网，用于对接入内网的移动设备进行监控，保存移动设备访问内网和操作内网数据的监控记录，并在发现移动设备要存储内网数据时调用加密模块；

[0050] 加密模块，其运行在内网，需要在监控模块的监控下运作，用于根据内网数据的保密等级选择相应的加密技术，对要存储到移动设备的内网数据进行加密；

[0051] 解密模块，其运行在移动设备，用于对移动设备的加密数据采用与所使用的加密技术对应的解密方法进行解密。

[0052] 所述安全管理平台将使用到移动设备序列号、保存于移动设备加密区的加密序号（该加密序号在移动设备注册成功时由安全管理平台随机生成并发送给移动设备）和网络标识（移动设备注册成功时由安全管理平台发送给移动设备）。所述加密模块包括两个子模块：对称密钥加密子模块和混合加密子模块。

[0053] 一种移动设备安全访问与存储内网数据的实现方法，首先，安全管理平台对移动设备进行注册，该注册可以预先进行，也可以在移动设备请求接入内网时进行，当移动设备请求接入内网时，本发明进行如下操作：

[0054] 1. 安全管理平台判断该移动设备是否已注册，对已注册的移动设备进行双向认证，允许双向认证成功后的移动设备接入内网，拒绝没有注册和双向认证失败的移动设备接入内网；

[0055] 2. 监控模块在发现移动设备要将内网中的内网数据存储到自身上时，调用加密模块；

[0056] 3. 加密模块在监控模块的监控下，根据内网数据的保密等级选择相应的加密方法，对要存储到移动设备的内网数据进行加密；

[0057] 4. 当存储在移动设备中的加密数据需要解密时，解密模块采用与加密数据所使用的加密方法对应的解密方法对加密数据进行解密。

[0058] 上述方法中，所述安全管理平台对移动设备进行注册，优选为预先进行注册，即由内网管理员操作安全管理平台对所有被允许接入内网的移动设备进行统一注册。如图 2 所示，该注册方法具体为：

[0059] 安全管理平台获取移动设备的硬件信息，如设备序列号、型号和生产商等，检测该获取的硬件信息是否有效，如无效则拒绝注册，如有效则生成该移动设备对应的网络标识和随机产生的加密序号，记录后发送给该移动设备进行存储。所述网络标识是作为双向认证的私钥固化在移动设备中，而所述加密序号存储在移动设备的加密区，用于识别发送该加密序号的具体内网。

[0060] 对应于上述注册的优选方法，步骤 1 所述安全管理平台判断该移动设备是否已注册，对已注册的移动设备进行双向认证，如图 3 所示，其方法具体为：

[0061] 1.1 安全管理平台读取该移动设备的硬件信息，如设备序列号、型号和生产商等，以检验该设备是否已注册登记；如果没有注册则拒绝该移动设备接入内网，如果以注册，则安全管理平台向其发送所记录的，并与所读取的移动设备的硬件信息关联的网络标识；

[0062] 1.2 移动设备接收到网络标识后，对比该网络标识与注册时所存储的网络标识是否相同，如果相同将向安全管理平台发送注册时所存储的加密序号，然后执行步骤 1.3 操作；否则，不发送加密序号，至此，双向认证失败，安全管理平台拒绝移动设备接入内网；

[0063] 1.3 安全管理平台对比所接收到的加密序号是否与设备注册登记时所记录的该移动设备的加密序号相同；如果相同，则双向认证成功，允许移动设备接入内网；否则，拒绝移动设备接入内网。

[0064] 上述方法中，所述监控模块还可以对接入内网的移动设备进行监控，保存移动设备访问内网和操作内网数据的监控记录，以便为以后的审计工作所使用。

[0065] 上述方法中，步骤 3 所述加密模块在监控模块的监控下，根据内网数据的保密等级选择相应的加密方法，对要存储到移动设备的内网数据进行加密，如图 4 所示，优选为：监控模块判断该内网数据是否为涉密内网数据并告知加密模块，加密模块对非涉密内网数据采用对称加密方法，对涉密内网数据采用混合加密方法。由于对称加密方法及其所对应的解密方法效率高，而混合加密方法及其所对应的解密方法又能保证涉密内网数据的安全性，从而从整体上实现了数据加解密效率和数据保密性的提高。

[0066] 所述对称加密方法，主要是针对存储量和处理的数据量较大的非涉密内网数据。具体采用 AES-256bit 加密方法，即采用分组长度为 128bit，密钥长度为 256bit 的 AES 加密方法。具体是：用户在移动设备设置密码，将该密码通过特殊处理映射出 256bit 的密钥对，该密钥对包括一个公钥 PK 和一个为私钥 SK，并将该密钥对发送给内网中的加密模块进行存储；以供加解密操作。内网中的加密模块用公钥 PK 进行加密，最后将该已加密的非涉密内网数据发送到移动设备。

[0067] 采用上述 AES-256bit 加密方法作为对称加密方法，主要优点是加解密效率高，应用实现简单，而且 256bit 的密钥长度使其安全性相对较高，非常适合容量较大的数据加密。

[0068] 上述方法中，所述混合加密方法优选为：先对涉密内网数据采用对称加密方法进行加密，然后针对该对称加密所使用的密钥使用非对称加密方法进行加密，最后将已加密的涉密内网数据和已加密的对称加密所使用的密钥一起发送到移动设备。相应的，步骤 4 所述解密模块对已加密的涉密内网数据进行解密，首先采用非对称加密方法解密出对称加密所使用的密钥，然后采用该对称加密所使用的密钥对已加密的涉密内网数据进行解密。

[0069] 上述混合加密方法具体为：用户在移动设备设置密码，移动设备将该密码映射出一密钥对，该密钥对包括一个公钥 PK 和一个为私钥 SK，并将该密钥对发送给内网中的加密模块进行存储；加密模块首先生成对称密钥 K 对涉密内网数据进行对称加密，然后用所存储的公钥 PK 对对称密钥 K 进行非对称加密，最后将已加密的涉密内网数据和已加密的对称加密所使用的密钥 K 一起发送到移动设备。

[0070] 相对于上述加密方法的具体方法，步骤 4 所述解密模块对加密数据进行解密具体为：解密模块首先向内网中的监控模块询问该加密数据是否为涉密内网数据；如不是则采用私钥 SK 对该加密数据进行解密，如是则首先采用私钥 SK 对对称密钥 K 进行解密，然后采用解密出的对称密钥 K 对已加密的涉密内网数据进行解密。

[0071] 上述方法中，步骤 4 所述当存储在移动设备中的加密数据需要解密时，解密模块采用与加密数据所使用的加密方法对应的解密方法对加密数据进行解密，在进行解密之前，还可以包括以下操作：移动设备向安全管理平台发送解密请求，安全管理平台返回与该移动设备硬件信息关联的加密序号，移动设备将返回的加密序号与注册时所存储的加密序号进行对比；若两者相同，则认为已接入该内网，允许加密数据被解密，否则，认为没有接入

该内网，不允许加密数据被解密。

[0072] 所述非对称加密方法具体采用ECC加密方法。非对称密码体制的安全性仅依赖于所依据的数学问题计算的复杂性，主要有基于大整数因子分解困难问题（如RSA、Rabin密码体制）和基于离散对数困难问题（如基于ECC的Diffle-Hellman、ElGamal密码体制）。

[0073] 所述混合加密方法具体可以使用ECC和AES相结合的混合加密方法，在目前技术下，使用160bit模长的ECC加密体制即可保证加密信息的安全。

[0074] 上述实施例为本发明典型的实施方式，但本发明的实施方式并不受所述实施例的限制，其他的任何未背离本发明的精神实质与原理下所作的改变、修饰、替代、组合、简化，均应为等效的置换方式，都包含在本发明的保护范围之内。

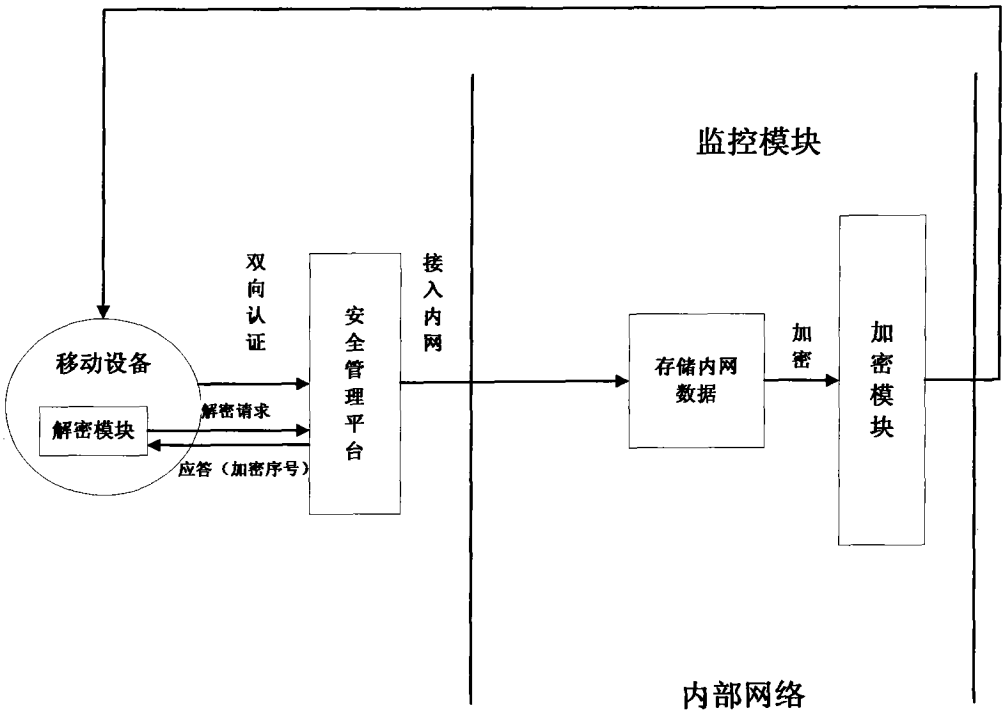

监控模块
双向认证
接入内网
安全管理平台
移动设备
解密模块
解密请求
应答（加密序号）
存储内网数据
加密
加密模块
内部网络

图 1

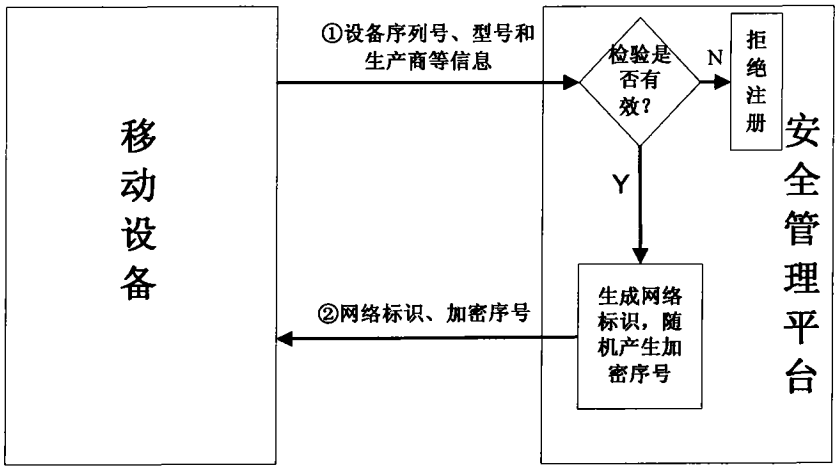

移动设备
①设备序列号、型号和生产商等信息
检验是否有效?
N
拒绝注册
Y
安全管理平台
②网络标识、加密序号
生成网络标识，随机产生加密序号

图 2

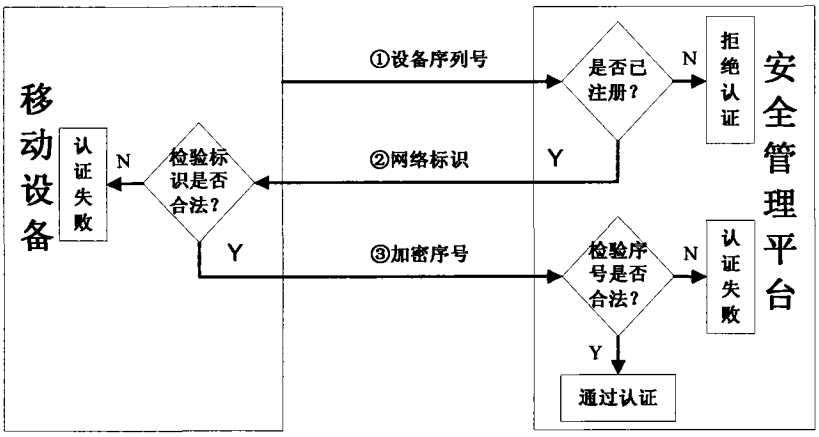

移动设备
认证失败
N
检验标识是否合法？
Y
①设备序列号
②网络标识
③加密序号
是否已注册？
N
拒绝认证
Y
检验序号是否合法？
N
认证失败
Y
通过认证
安全管理平台

图 3

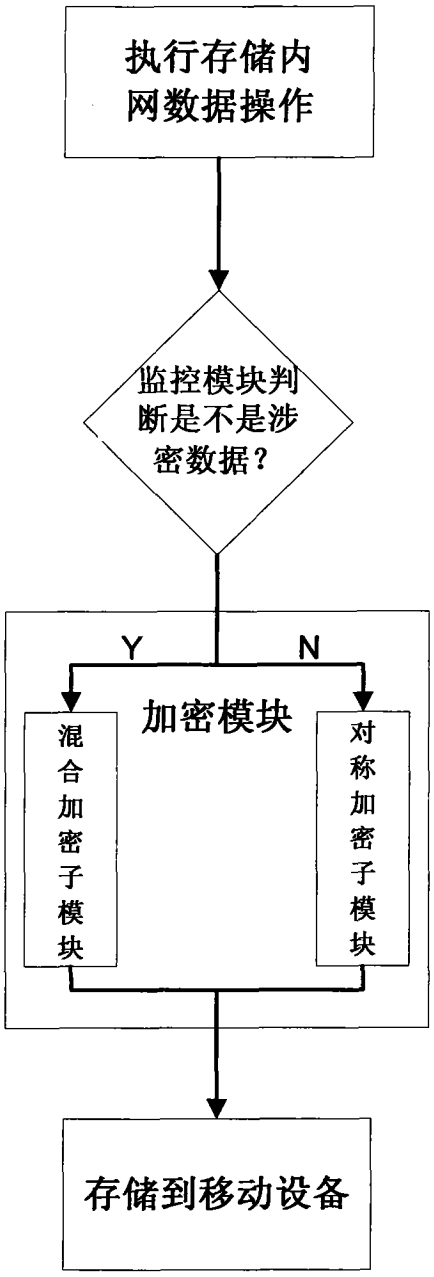

执行存储内网数据操作
监控模块判断是不是涉密数据？
Y
N
加密模块
混合加密子模块
对称加密子模块
存储到移动设备

图 4