(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 101711028 B
(45)授权公告日 2011.12.14

(21)申请号 200910234636.1

(22)申请日 2009.11.26

(73)专利权人 南京烽火星空通信发展有限公司
地址 210019 江苏省南京市建邺区云龙山路88号烽火大厦A座20层

(72)发明人 刘国俭 王娜

(74)专利代理机构 南京苏科专利代理有限责任公司 32102
代理人 何朝旭

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/02(2009.01)

(56)对比文件
EP 0725512 A2,1996.08.07,
US 7522723 B1,2009.04.21,
CN 101478595 A,2009.07.08,
CN 101340282 A,2009.01.07,

审查员 刘冬生

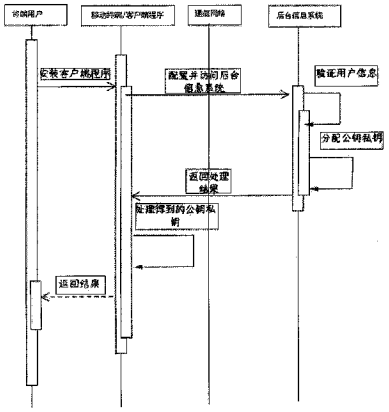
权利要求书 1 页 说明书 4 页 附图 2 页

(54)发明名称

一种移动终端设备上用户数据的自动保护方法

(57)摘要

本发明涉及一种移动终端设备上用户数据的自动保护方法，属于信息安全防护技术领域。该方法通过：加载通讯管理服务器后台访问程序；将用户输入的验证口令无线传输给通讯管理服务器后台；对传输来的验证口令进行验证并确认后分配特定的公钥私钥对；用公钥对存储数据进行加密；公钥被自动保存到移动终端的存储单元，私钥自动销毁；当用户需要访问存储的加密数据时，再次对验证口令进行验证并确认后分配特定的私钥；移动终端用传输来的私钥对用户需访问数据进行解密等步骤实现。本发明容易实施，能够方便地与其它信息化系统集成，可以切实保护移动终端的用户数据，有效防止泄密。



CN 101711028 B

1. 一种移动终端设备上用户数据的自动保护方法，包括以下基本步骤：

第一步、在移动终端加载通讯管理服务器后台访问程序；

第二步、通讯管理服务器后台访问程序在移动终端运行后，根据配置的后台地址将用户输入的验证口令无线传输给通讯管理服务器后台；

第三步、通讯管理服务器后台对传输来的验证口令进行验证并确认后，分配特定的公钥私钥对无线传输给该移动终端；

第四步、移动终端接收到发送来的公钥私钥对后，自动将公钥用于对用户需存储数据进行加密存储；

第五步、加密存储完成后，公钥被自动保存到移动终端的存储单元，用于后续需存储数据的加密，而私钥作为加密过程的临时变量被自动销毁；

第六步、当用户需要访问存储的加密数据时，移动终端再次运行通讯管理服务器后台访问程序，根据配置的后台地址将用户输入的验证口令再次无线传输给通讯管理服务器后台；

第七步、通讯管理服务器后台再次对传输来的验证口令进行验证并确认后，分配特定的私钥无线传输给该移动终端；

第八步、移动终端将传输来的私钥用于对用户需访问数据进行解密，解密之后私钥被再次自动销毁。

2. 根据权利要求 1 所述移动终端设备上用户数据的自动保护方法，其特征在于还包括：

第九步、当通讯管理服务器发现移动终端用户状态发生改变时，通讯管理服务器后台设置该用户状态为无法通过验证的非激活状态。

3. 根据权利要求 1 所述移动终端设备上用户数据的自动保护方法，其特征在于：所述第五步之后，移动终端可以随时使用存储单元中存储的公钥对数据加密，并发送给通讯管理服务器后台处理。

4. 根据权利要求 1 所述移动终端设备上用户数据的自动保护方法，其特征在于：所述第五步之后，移动终端可以随时接收通讯管理服务器后台使用特定公钥加密的数据，并保存在移动终端存储单元。

5. 根据权利要求 1 或 2 所述移动终端设备上用户数据的自动保护方法，其特征在于：所述第四步中，所述移动终端在退出加密存储程序之前，可以随时借助私钥解密数据。

6. 根据权利要求 5 所述移动终端设备上用户数据的自动保护方法，其特征在于：所述公钥私钥对以及加密、解密过程均对移动终端用户透明。

一种移动终端设备上用户数据的自动保护方法

技术领域

[0001] 本发明涉及一种终端设备的数据保护方法，尤其是一种移动终端设备上用户数据的自动保护方法，属于信息安全防护技术领域。

背景技术

[0002] 随着信息科技的发展，办公信息化软件、ERP 软件、CRM 软件等得到了广泛的应用。但随着信息化系统不断广泛应用并作为工作中的重要支撑平台，能够随时随地访问内部信息系统成了新的需求。而移动通信技术的飞速发展也使得将有线网络环境下的信息化系统扩展到无线网络中成为可能，借助移动通信网络的可移动性、快捷性的特点，可以把已有的信息系统延伸到无线网络环境中，并利用手机等移动终端来与现有的信息系统随时随地进行访问。

[0003] 在使用手机等终端设备访问信息系统时，用户可能会保存从后台信息平台得到的数据到本地，同时由于手机等移动终端的便携性，也造成此类终端易于丢失，与此情况，用户需要保护这些保存在终端上的数据。现在已有的方法有发送炸弹消息给终端，终端接收到炸弹消息后自动删除用户数据。但是该方法要求丢失后的终端能够顺利接收炸弹消息，生效的要求条件很高并易于失效。需要有更好的机制来保护用户数据。

[0004] 检索发现，申请号为 CN200610065011.3 的中国发明专利公开了一种实现移动终端数据保护的方法，采用该方法后，只要移动终端开机，无论其是否更换 SIM 卡，都可实现对该移动终端的锁止；避免了移动终端内容信息的泄漏；避免了移动终端和 / 或 SIM 卡被他人盗用。然而，该方法需要根据移动终端自动上报的 SIM 卡信息来要求网络侧服务器做对应的动作，例如发送锁定软件给所述终端，并让此移动终端自动运行此锁定软件来执行锁定移动终端的操作。如果移动终端处在一个没有移动信号的环境，不能够发送相关信息给网络侧服务器，该方法就无能为力了。

[0005] 此外，申请号为 CN200810198371.X 的中国专利申请公开了一种移动通信终端数据保护方法，其特征是采用配套的公钥、私钥、加密程序和解密程序，移动通信终端对录入的特定数据用公钥加密存储，读取特定数据时调用私钥解密；移动通信终端设有要求使用者输入口令的步骤，以口令通过验证作为可读取特定数据的必要条件；如果口令不通过验证，则向预设的关联终端报警；移动通信终端如果从关联终端收到特定指令，就销毁所述的特定数据，或向关联终端发送该特定数据。该方法要求保存私钥到通信用户识别模块或者移动通信终端存储卡，即私钥保存在移动终端本地，理论上仍存在验证口令被破解从而得到私钥来解密数据、甚至从用户识别模块直接得到私钥来解密数据的可能。因此，仍存在不安全因素。

发明内容

[0006] 本发明的首要目的在于：提供一种移动终端设备上用户数据的自动保护方法，该方法不仅便于实施，并且能够和其它信息化系统集成用于保护数据，实现在用户丢失移动

终端后切实有效防止数据泄密。

[0007] 本发明进一步的目的在于：当移动终端用户状态改变后，能够阻止用户访问已保存数据的移动终端设备上用户数据自动保护方法（例如用户从某个信息系统的合法用户变成非法用户后，阻止该用户访问已经保存好的数据）。

[0008] 为了达到以上首要目的，本发明移动终端设备上用户数据的自动保护方法在移动终端和通讯管理服务器构成的无线通讯系统中，通过以下基本步骤实现对数据的自动保护：

[0009] 第一步、在移动终端加载通讯管理服务器后台访问程序；

[0010] 第二步、通讯管理服务器后台访问程序在移动终端运行后，根据配置的后台地址将用户输入的验证口令无线传输给通讯管理服务器后台；

[0011] 第三步、通讯管理服务器后台对传输来的验证口令进行验证并确认后，分配特定的公钥私钥对无线传输给该移动终端；

[0012] 第四步、移动终端接收到发送来的公钥私钥对后，自动将公钥其用于对用户需存储数据进行加密存储；

[0013] 第五步、加密存储完成后，公钥被自动保存到移动终端的存储单元，用于后续需存储数据的加密，而私钥作为加密过程的临时变量被自动销毁；

[0014] 第六步、当用户需要访问存储的加密数据时，移动终端再次运行通讯管理服务器后台访问程序，根据配置的后台地址将用户输入的验证口令再次无线传输给通讯管理服务器后台；

[0015] 第七步、通讯管理服务器后台再次对传输来的验证口令进行验证并确认后，分配特定的私钥无线传输给该移动终端；

[0016] 第八步、移动终端将传输来的私钥用于对用户需访问数据进行解密，解密之后私钥被再次自动销毁。

[0017] 为了达到进一步的目的，本发明移动终端设备上用户数据的自动保护方法还包括：

[0018] 第九步、当通讯管理服务器发现移动终端用户状态发生改变时（例如，用户从合法用户变为非法用户），通讯管理服务器后台将设置该用户状态为无法通过验证的非激活状态。这样使得该用户无法再次与通讯管理服务器后台成功通信获取私钥，也就使该用户无法访问已经保存到终端本地的数据。

[0019] 本发明虽然与某些现有技术一样，使用公钥对用户数据加密，使用私钥对加密数据解密。但通讯管理服务器后台分配的私钥只能作为临时变量，不能保存在移动终端。因此，用户需要访问存储的加密数据时，需要与通讯管理服务器后台通讯，并通过验证，才能再次得到私钥进行解密处理。如果移动终端丢失，很容易在知悉后将通讯管理服务器后台设置为不允许此移动终端访问，因此即使该移动终端的验证口令被破解，用户保存的加密数据依然无法解密。显然，该方法不仅容易实施，而且能够方便地与其它信息化系统集成，从而可以切实保护移动终端的用户数据，有效防止泄密。在此基础上，本发明还可以在移动终端的用户状态发生改变后，阻止移动终端的原有用户数据再次被访问，从而杜绝诸如用户从某个信息系统的合法用户变成非法用户后再次访问已经保存的数据，进一步有效防止数据泄密。

附图说明

[0020] 下面结合附图对本发明作进一步的说明。

[0021] 图 1 为本发明一个实施例移动终端与后台第一次交互示意图。

[0022] 图 2 为图 1 实施例移动终端与后台再次交互示意图。

具体实施方式

[0023] 实施例一

[0024] 本实施例移动终端设备上用户数据的自动保护方法在移动终端和通讯管理服务器构成的无线通讯系统中，第一次移动终端与通讯管理服务器后台的交互过程如图 1 所示，包括：

[0025] 1) 安装客户端程序——即在移动终端加载通讯管理服务器后台访问程序；

[0026] 2) 配置并访问后台信息系统——即通讯管理服务器后台访问程序在移动终端运行后，根据配置的后台地址将用户输入的验证口令无线传输给通讯管理服务器后台；

[0027] 3) 验证用户信息分配公钥私钥对——即通讯管理服务器后台对传输来的验证口令进行验证并确认后，分配特定的公钥私钥对无线传输给该移动终端；

[0028] 4) 处理得到的公钥私钥——即移动终端接收到发送来的公钥私钥对后，自动将公钥其用于对用户需存储数据进行加密存储，并且在退出加密存储程序之前，可以随时借助留驻于内存的私钥解密数据；

[0029] 5) 返回结果——即加密存储完成退出后，公钥被自动保存到移动终端的存储单元，用于后续需存储数据的加密，而私钥作为加密过程的临时变量被自动销毁。

[0030] 当用户需要访问存储的加密数据时，第一次之后移动终端与通讯管理服务器后台的交互过程如图 2 所示，包括

[0031] 6) 访问后台系统得到私钥——即移动终端再次运行通讯管理服务器后台访问程序，根据配置的后台地址将用户输入的验证口令再次无线传输给通讯管理服务器后台；

[0032] 7) 返回结果成功就返回私钥——即通讯管理服务器后台再次对传输来的验证口令进行验证并确认后，分配特定的私钥无线传输给该移动终端；

[0033] 8) 处理本地数据使用得到的私钥解密——即移动终端将传输来的私钥用于对用户需访问数据进行解密，解密之后私钥被再次自动销毁。

[0034] 以上的公钥私钥对以及加密、解密过程均对移动终端用户透明，因此具有足够的安全性。此外，在第一次访问之后，移动终端可以随时和后台系统交互，使用公钥加密数据——即可以随时使用存储单元中存储的公钥对数据加密，并发送给通讯管理服务器后台自动使用私钥解密处理，也可以接收通讯管理服务器后台使用相应公钥加密的数据，，并保存在移动终端存储单元实现加密数据的交互。

[0035] 当通讯管理服务器发现移动终端用户状态发生改变时（例如，用户从合法用户变为非法用户），本实施例的通讯管理服务器后台将设置该用户状态为无法通过验证的非激活状态，从而使其无法再次与通讯管理服务器后台成功通信获取私钥，彻底杜绝该用户访问已经保存到终端本地的数据。

[0036] 通过以上步骤的完成，达到了对用户保存的数据自动进行加密保护的目的。与

现有技术相比，本实施例通过自动分配公钥私钥对来加密解密信息，同时对于用户获取私钥设定一个前提，即必须和通讯管理服务器后台的信息平台进行一次成功通信验证用户信息，而后台信息平台可以设置用户状态，从而可以控制移动终端能否和后台信息平台成功通信，从而达到了保护用户数据的目的。

[0037] 上述实施例并非限制性的，例如通讯管理服务器后台访问程序是广义的，并不限于指某一个程序，而是指能够完成用户和后台信息平台交互的各种程序媒介，但能够提供一个界面给用户用于和后台交互的程序都包括在内。此外，用户数据可以任意，包括但不限于通讯录信息等。凡采用等同替换或等效变换形成的技术方案，均落在本发明要求的保护范围。

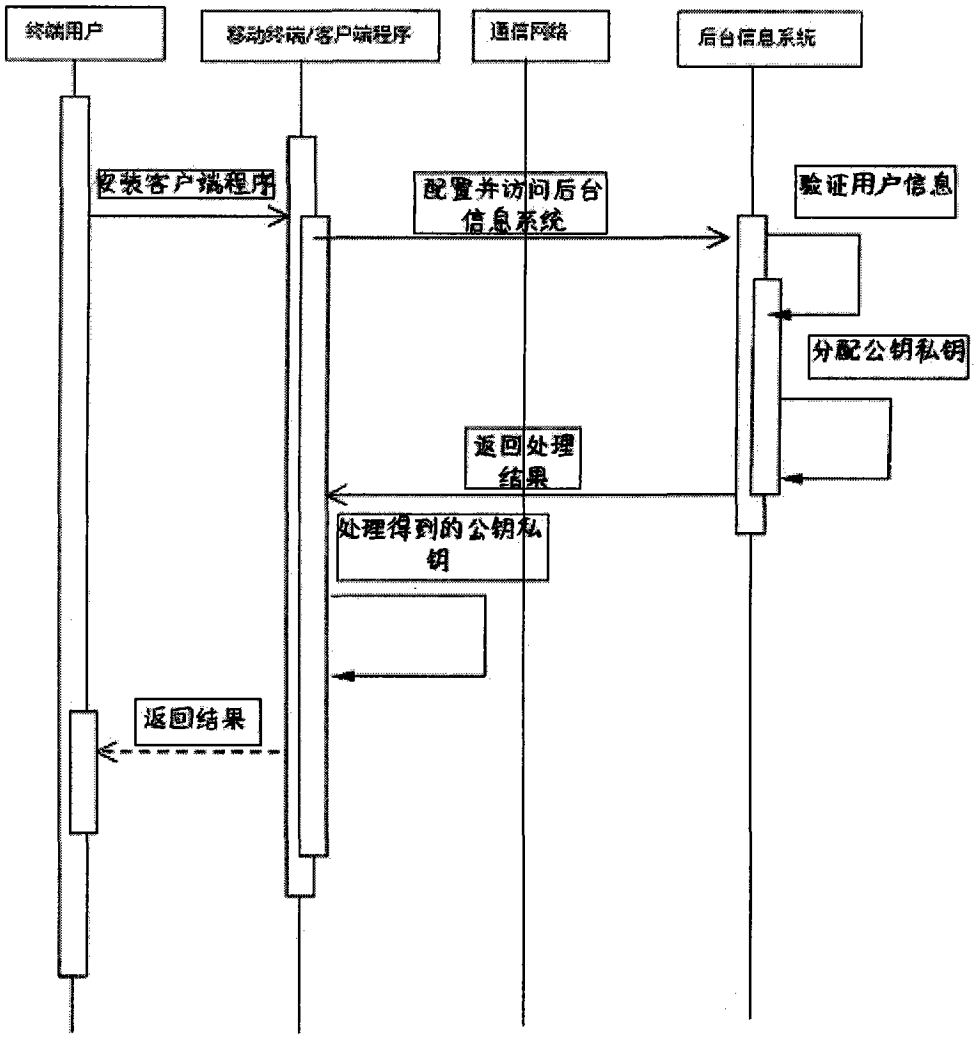

终端用户
移动终端/客户端程序
通信网络
后台信息系统
安装客户端程序
配置并访问后台信息系统
验证用户信息
分配公钥私钥
返回处理结果
处理得到的公钥私钥
返回结果

图 1

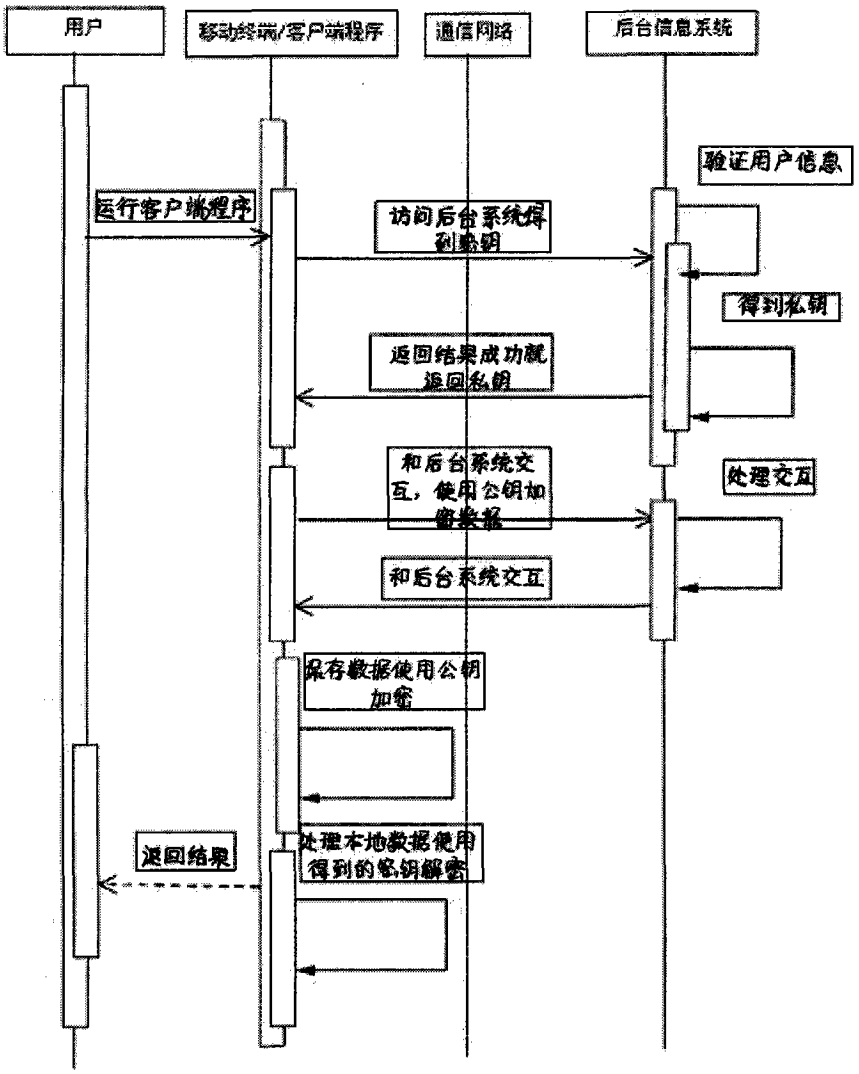

用户
移动终端/客户端程序
通信网络
后台信息系统
验证用户信息
运行客户端程序
访问后台系统得到密钥
得到私钥
返回结果成功就返回私钥
和后台系统交互，使用公钥加密数据
处理交互
和后台系统交互
保存数据使用公钥加密
处理本地数据使用得到的密钥解密
返回结果

图 2