(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 104662870 B
(45)授权公告日 2019.02.05

(21)申请号 201380047198.2
(22)申请日 2013.09.10
(65)同一申请的已公布的文献号
申请公布号 CN 104662870 A
(43)申请公布日 2015.05.27
(30)优先权数据
61/699,274 2012.09.10 US
(85)PCT国际申请进入国家阶段日
2015.03.10
(86)PCT国际申请的申请数据
PCT/CN2013/083241 2013.09.10
(87)PCT国际申请的公布数据
WO2014/036977 EN 2014.03.13
(73)专利权人 云深系统有限公司
地址 中国香港新界沙田香港科学园科技大道西5号企业广场543室
(72)发明人 伍灿耀 严正山 朱成义 郑锦添 李廷谦 杨耀松
(74)专利代理机构 深圳市精英专利事务所 44242
代理人 刘贻盛
(51)Int.Cl.
H04L 29/08(2006.01)
(56)对比文件
CN 102281314 A,2011.12.14,
US 2002029340 A1,2002.03.07,
US 2002029340 A1,2002.03.07,
US 2009106550 A1,2009.04.23,
CN 101064598 A,2007.10.31,
审查员 樊星

权利要求书4页 说明书10页 附图4页

(54)发明名称

数据安全管理系统

(57)摘要

本专利申请涉及一种数据安全管理系统。该系统包括:安全服务器,配置为存储用于加密文件或任何数据的加密密钥和用于解密所述文件或数据的解密密钥;第一计算装置,配置为发送携带授权限制的访问授权列表到所述安全服务器、向所述安全服务器请求加密密钥、以及利用从所述安全服务器接收到的所述加密密钥加密所述文件或数据;第二计算装置,配置为向所述安全服务器请求解密密钥、并使用从所述安全服务器接收到的所述解密密钥对加密的文件进行解密;和云存储,配置为在使用所述第一计算装置的第一用户和使用所述第二计算装置的第二用户之间共享所述文件。

CN 104662870 B

1.一种数据安全管理系统,包括:

安全服务器,配置为存储用于加密文件或任何数据的加密密钥以及用于解密所述文件或数据的解密密钥;

第一计算装置,配置为发送携带授权限制的访问授权列表到所述安全服务器、向所述安全服务器请求加密密钥、以及利用从所述安全服务器接收到的所述加密密钥加密所述文件或数据;所述携带授权限制的每个访问授权列表绑定唯一的加密密钥;每个文件或数据采用唯一的加密密钥以及单独设置有一个所述访问授权列表;所述第一计算装置配置为随时随地改变所述访问授权列表;

第二计算装置,配置为向所述安全服务器请求解密密钥、并使用从所述安全服务器接收到的所述解密密钥对加密的文件或数据进行解密;和

存储器,配置为在使用所述第一计算装置的第一用户和使用所述第二计算装置的第二用户之间共享所述文件或数据;其中:

所述安全服务器配置为根据验证所述第二用户是否在所述访问授权列表及在所述授权限制内,来确定是否将所述解密密钥发送给所述第二计算装置;

当加密所述文件时,所述第一计算装置配置为给所述加密文件添加文件头,并生成所述文件头的报头哈希,所述文件头包括随机生成的唯一的文件标识以及所述密钥标识和头格式标识符;

所述安全服务器提供身份验证方法的多种选择,包括:1)用户标识+密码;2)用户标识+密码+登录图片;3)用户标识+密码+一次性密码;4)用户标识+密码+登录图片+一次性密码;

所述系统在加密密钥被删除后禁止打开加密文件但保留所述文件的日志,所述日志包括多个文件的事件,每个事件包括:1)每个日志事件的时间和日期;2)解密设备的标识和类型;3)位置;4)加密密钥的所有者;5)事件动作的用户标识;6)取决于事件动作的事件内容;

对于每个用户标识,存在用户操作日志,每个用户标识的用户操作日志包括所有与相应用户相关的操作事件;

所述头格式标识符用于识别头参数包括哪些参数和头参数如何排列,以及描述头参数是否被加密及其如何加密;所述头格式标识符分为与加密的文件在一起的部分1和被发送到所述安全服务器的部分2;所述头格式标识符的部分1用于识别所述密钥标识和所述安全服务器的互联网位置,所述头格式标识符的部分2用于生成原始报头;

所述安全服务器绑定如下参数以及密钥标识:1)创建时间;2)加密密钥的类型和大小;3)用户标识;4)具有每个授权用户的授权限制的访问授权列表;5)文件标识;6)头格式标识符的部分2;7)文件哈希和所使用的哈希算法;8)报头哈希值和所使用的哈希算法;9)文件安全日志所述授权限制包括:通过开始启动时间限制、通过结束时间限制以及所允许的解密数量。

2.根据权利要求1所述的数据安全管理系统,其特征在于,所述第一计算装置、所述第二计算装置、所述存储器和所述安全服务器都与互联网和/或局域网连接。

3.根据权利要求1所述的数据安全管理系统,其特征在于,所述第一计算装置和所述第二计算装置分别与所述安全服务器之间的通信是通过预定义的应用程序接口来实现的。

4.根据权利要求1的数据安全管理系统,其特征在于,当向所述安全服务器请求加密密钥时,所述第一计算装置配置为向所述安全服务器发送文件名和所述加密密钥的类型和大

小。

5.根据权利要求1的数据安全管理系统，其特征在于，所述安全服务器包括具有加密密钥数据库的密钥管理器，所述安全服务器配置为给所述加密密钥分配密钥标识，而所述加密密钥和密钥标识保存于所述加密密钥数据库。

6.如权利要求1所述的数据安全管理系统，其特征在于，在加密所述文件或数据后，所述第一计算装置配置为将所述密钥标识、所述访问授权列表和所述报头哈希发送到所述安全服务器。

7.如权利要求6所述的数据安全管理系统，其特征在于，所述安全服务器配置为将所述第一用户的用户标识、所述访问授权列表以及和所述报头哈希相关的信息与所述密钥标识绑定。

8.根据权利要求7的数据安全管理系统，其特征在于，当解密所述加密文件或数据时，所述第二计算装置配置为从所述文件头提取所述密钥标识。

9.根据权利要求8的数据安全管理系统，其特征在于，当向所述安全服务器请求所述解密密钥时，所述第二计算装置配置为将所述密钥标识作为参数发送给所述安全服务器。

10.根据权利要求9的数据安全管理系统，其特征在于，所述安全服务器配置为根据所述密钥标识在所述加密密钥数据库中查找对应的加密密钥记录，以验证所述第二用户是否处于绑定有所述密钥标识的访问授权列表，并基于有效的验证向所述第二计算装置发送所述加密密钥和相应的报头哈希信息。

11.根据权利要求10的数据安全管理系统，其特征在于，所述报头哈希信息包括报头哈希和哈希法，所述第二计算装置配置为利用所述哈希法生成新的报头哈希，并比较所述新的报头哈希和来自所述安全服务器的所述报头哈希信息中的报头哈希，以便验证所述文件的所述文件头的完整性。

12.根据权利要求5的数据安全管理系统，其特征在于，当加密所述文件或数据时，所述第一计算装置配置为发送参数给所述安全服务器，以便所述安全服务器为所述加密文件创建文件头。

13.一种数据安全管理系统，包括：

第一计算装置；

第二计算装置；和

与所述第一计算装置和所述第二计算装置通信的安全服务器；其中：

所述第一计算装置配置为发送访问授权列表到所述安全服务器，并向所述安全服务器请求加密密钥；所述访问授权列表绑定唯一的加密密钥；每个文件或数据采用唯一的加密密钥以及单独设置有一个所述访问授权列表；

所述第一计算装置配置为随时随地改变所述访问授权列表；

所述安全服务器配置为发送所述加密密钥到所述第一计算装置；

所述第一计算装置配置为利用所述加密密钥加密文件或数据，并与所述第二计算装置共享加密文件或数据；

第二计算装置为配置向所述安全服务器请求解密密钥；

所述安全服务器配置为在验证所述第二计算装置正由所述访问授权列表上的用户正在使用之后，向所述第二计算装置发送所述解密密钥；和

所述第二计算装置配置为利用所述解密密钥对所述加密文件或数据进行解密；

当加密所述文件时，所述第一计算装置配置为给所述加密文件添加文件头，并生成所述文件头的报头哈希，所述文件头包括随机生成的唯一的文件标识以及所述密钥标识和头格式标识符；

所述安全服务器提供身份验证方法的多种选择，包括：1)用户标识+密码；2)用户标识+密码+登录图片；3)用户标识+密码+一次性密码；4)用户标识+密码+登录图片+一次性密码；

所述系统在加密密钥被删除后禁止打开加密文件但保留所述文件的日志，所述日志包括多个文件的事件，每个事件包括：1)每个日志事件的时间和日期；2)解密设备的标识和类型；3)位置；4)加密密钥的所有者；5)事件动作的用户标识；6)取决于事件动作的事件内容；

对于每个用户标识，存在用户操作日志，每个用户标识的用户操作日志包括所有与相应用户相关的操作事件；

所述头格式标识符用于识别头参数包括哪些参数和头参数如何排列，以及

描述头参数是否被加密及其如何加密；所述头格式标识符分为与加密的文件在一起的部分1和被发送到所述安全服务器的部分2；所述头格式标识符的部分1用于识别所述密钥标识和所述安全服务器的互联网位置，所述头格式标识符的部分2用于生成原始报头；

所述安全服务器绑定如下参数以及密钥标识：1)创建时间；2)加密密钥的类型和大小；3)用户标识；4)具有每个授权用户的授权限制的访问授权列表；5)文件标识；6)头格式标识符的部分2；7)文件哈希和所使用的哈希算法；8)报头哈希值和所使用的哈希算法；9)文件安全日志所述授权限制包括：通过开始启动时间限制、通过结束时间限制以及所允许的解密数量。

14.根据权利要求13的数据安全管理系统，其特征在于，所述第一计算装置配置为通过存储器将所述加密文件或数据共享给所述第二计算装置，所述安全服务器包括具有加密密钥数据库的密钥管理器，所述安全服务器配置为给所述加密密钥分配密钥标识，而所述加密密钥和所述密钥标识保存于所述加密密钥数据库。

15.一种数据安全管理方法，包括：

将来自第一计算装置的访问授权列表发送到安全服务器，通过所述第一计算装置向所述安全服务器请求加密密钥；所述访问授权列表绑定唯一的加密密钥；每个文件或数据采用唯一的加密密钥以及单独设置有一个所述访问授权列表；所述第一计算装置配置为随时随地改变所述访问授权列表；将来自所述安全服务器的所述加密密钥发送给所述第一计算装置；

通过所述第一计算装置利用所述加密密钥加密文件或数据，将加密文件或数据共享给第二计算装置；

通过所述第二计算装置向所述安全服务器请求解密密钥；

在通过所述安全服务器验证所述第二计算装置正由所述访问授权列表上的用户正在使用后，将所述解密密钥发送给所述第二计算装置；和

通过所述第二计算装置利用所述解密密钥对所述加密文件或数据进行解密；

当加密所述文件时，所述第一计算装置配置为给所述加密文件添加文件头，并生成所述文件头的报头哈希，所述文件头包括随机生成的唯一的文件标识以及所述密钥标识和头格式标识符；

所述安全服务器提供身份验证方法的多种选择，包括：1）用户标识+密码；2）用户标识+密码+登录图片；3）用户标识+密码+一次性密码；4）用户标识+密码+登录图片+一次性密码；

执行所述方法的数据安全管理系统在加密密钥被删除后禁止打开加密文件但保留所述文件的日志，所述日志包括多个文件的事件，每个事件包括：1）每个日志事件的时间和日期；2）解密设备的标识和类型；3）位置；4）加密密钥的所有者；5）事件动作的用户标识；6）取决于事件动作的事件内容；

对于每个用户标识，存在用户操作日志，每个用户标识的用户操作日志包括所有与相应用户相关的操作事件；

所述头格式标识符用于识别头参数包括哪些参数和头参数如何排列，以及描述头参数是否被加密及其如何加密；所述头格式标识符分为与加密的文件在一起的部分1和被发送到所述安全服务器的部分2；所述头格式标识符的部分1用于识别所述密钥标识和所述安全服务器的互联网位置，所述头格式标识符的部分2用于生成原始报头；

所述安全服务器绑定如下参数以及密钥标识：1）创建时间；2）加密密钥的类型和大小；3）用户标识；4）具有每个授权用户的授权限制的访问授权列表；5）文件标识；6）头格式标识符的部分2；7）文件哈希和所使用的哈希算法；8）报头哈希值和所使用的哈希算法；9）文件安全日志所述授权限制包括：通过开始启动时间限制、通过结束时间限制以及所允许的解密数量。

数据安全管理系统

[0001] 相关申请交叉引用

[0002] 本申请要求享有于2012年9月10日提交的序列号为61/699,274的美国临时专利申请的利益,其内容完全以引用方式并入本申请。

技术领域

[0003] 本专利申请一般涉及数据管理技术,更具体地涉及一种数据安全管理系统,该系统为云计算应用提供额外的安全,并允许用户在任何时间从任何地点控制存在于任何设备的数据的数据安全性。

背景技术

[0004] 世界上超过60%的公司首席信息官担心云计算的安全性,特别是云数据的安全性。关于云计算的数据安全的主要问题之一是,存在于云数据中心的数据可以通过云数据中心服务提供商的员工及第三方承包商访问。因此,希望允许用户在任何时间从任何地点控制存在于任何设备的数据的数据安全性,这些设备可包括云数据中心、终端设备、USB设备等。

发明内容

[0005] 本专利申请涉及一种数据安全管理系统。该系统包括:安全服务器,配置为存储一个或多个用于加密一个或多个文件或任何数据以及一个或多个解密密钥用于解密相应的加密文件或数据;一个或多个第一计算装置,配置为发送携带授权限制的访问授权列表到所述安全服务器、向所述安全服务器请求加密密钥、以及利用从所述安全服务器接收到的所述加密密钥加密一个或多个文件或数据;一个或多个第二计算装置,配置为向所述安全服务器请求解密密钥、并使用从所述安全服务器接收到的所述解密密钥解密一个或多个加密文件;和云存储或任何数据存储,配置为在使用所述第一计算装置的第一用户和使用所述第二计算装置的第二用户之间共享所述文件。所述安全服务器配置为根据验证所述第二用户是否在所述访问授权列表及在所述授权限制内来确定是否将所述解密密钥发送给所述第二计算装置。

附图说明

[0006] 图1示出了根据本专利申请一种实施例的作为数据安全管理系统的一部分的基于计算机的应用程序。

[0007] 图2示出了根据本专利申请一种实施例的数据安全管理系统的操作。

[0008] 图3示出了根据本专利申请一种实施例的数据安全管理系统的基础体系结构。

[0009] 图4示出了根据本专利申请一种实施例的在uSave App和安全服务器之间的通信处理以完成在数据安全管理系统中的文件加密。

[0010] 图5示出了根据本专利申请一种实施例的在uSave App和安全服务器之间的通信

处理以完成在数据安全管理系统中的文件解密。

[0011] 详细说明

[0012] 现在将参考本专利申请中披露的数据安全管理系统的优选实施方式进行详细说明，这些例子也将在随后的说明中给出。尽管为了清楚起见，某些对于理解数据安全管理系统来说并非特别重要的技术特征未呈现出来，但是对于相关领域技术人员而言，它们是显而易见的。

[0013] 此外，应当理解，本专利申请中披露的数据安全管理系统并不限于以下描述的具体实施例，本领域技术人员可以在不脱离本申请保护的实质或范围的情况下进行各种改变和修改。例如，不同的说明性实施例的元件和/或特征可以在本申请的范围内彼此结合和/或相互替换。

[0014] 图1示出了根据本专利申请一种实施例的作为数据安全管理系统的一部分的基于计算机的应用程序。参照图1，存在一个或多个用户，每个用户从应用程序商店(如谷歌市场、苹果商店和微软商店等)或网站(如图1所示的“nwStor Website”下载应用程序到一个或多个设备，该应用程序在下文中也称为uSav App，该设备为诸如智能电话、膝上型电脑、iPad、平板电脑等。在使用数据安全管理系统之前，每个用户都必须注册并新建账户。在本实施例中，所要求的来自用户的注册信息为如下：

[0015] 1.姓名(非验证，以保护隐私)

[0016] 2.电子邮件地址(也用于密码恢复)

[0017] 3.用户ID：在系统数据库中必须是唯一的(用户ID可以但不限于用户的电子邮件地址)。

[0018] 4.认证方法的选择(下文将更详细地描述认证方法)

[0019] a.收费帐户信息：该信息不是初始注册所必需的。只有在用户用完附加的免费使用量后才需要。该信息包括但不限于信用卡号、Paypal帐户号码、银行帐号等。

[0020] 5.用于密码恢复目的的个人问题和答案。

[0021] 为保护用户隐私，不对用户信息执行核实。在用户注册完成之后，向用户的电子邮箱地址发送由计算机生成的密码。该密码可以在登录到uSav App后更改。

[0022] 图2示出了根据本专利申请一种实施例的数据安全管理系统的操作。参照图2，发送方201和接收方203已经下载uSav App，并已在系统中注册。如图2所示，在步骤1中，作为文件所有者的发送方201在其设备上登录uSav App，并确定要保密的文件。发送方201还提供了系统的一些被授权打开并读取文件的注册者(也称为uSav注册者)的访问授权列表。发送方201的uSav App然后向安全服务器205(也称为uSav安全服务器)请求加密密钥。与此同时，该uSav App还向安全服务器205发送访问授权列表(作为参数)。安全服务器205保存用户的数据安全需求，并根据用户指令通过控制加密密钥来控制用户的数据信息。

[0023] 然后在步骤2中，uSav安全服务器205将随机生成的新的加密密钥的副本发送给uSav App(即发送方201)。访问授权列表附着于(或绑定着)加密密钥，而且两者都保存在安全服务器205。(之后在图4所示的加密过程中加密密钥绑定有更多信息。)在步骤3中，在uSav App已经加密文件后，文件所有者向其已注册于系统的朋友发送加密文件，以便与朋友共享文件。通常可以通过互联网、局域网、有线网、无线网或他们的网络服务的组合，通过将加密文件附着于电子邮件、消息、或将加密文件放到例如由谷歌硬盘、Dropbox、Sky

Drive等之一者提供的云驱动(或云存储)207来实现这一共享。该共享也可以通过物理存储设备,例如USB存储器、USB存储棒或能够存储数据的任何物理设备来实现。在步骤4中,接收方203通过互联网(或任何类型的网络)下载加密文件,或者通过物理存储设备接收加密文件。在步骤5中,接收方203之一者登录uSav App,并请求uSav App解密文件。接收方203的uSav App向uSav安全服务器205发送解密密钥请求,该请求携带有作为请求的参数的请求方(接收方203)的标识和密码。在步骤6中,云密钥管理器(在安全服务器205中)进行检查以确保请求者(接收方203)的ID在(如步骤1和2述及的)授权列表上,然后发送解密密钥给处于接收方203端的uSav App,并且uSav App使用该解密密钥来解密文件。

[0024] 上述实施例中可以有大量的uSav注册者。每个注册者201可以是一个或多个加密文件的发送方。任何uSav注册者可以加密文档的接收方203中的一个。因而可以在注册者间实现安全协作和文件共享。

[0025] 上述实施例提供了一种数据安全管理系统。数据安全管理系统包括:配置为存储用以加密大量文件的加密密钥和用以解密相应的加密文件的解密密钥的安全服务器;配置为向安全服务器发送访问授权列表、向安全服务器请求加密密钥、及利用从安全服务器接收的加密密钥加密文件的第一计算装置;

[0026] 配置为向安全服务器请求解密密钥、及使用从安全服务器接收到的解密密钥对加密文件进行解密的第二计算装置;和

[0027] 配置为在使用第一计算装置的第一用户和使用第二计算装置的第二用户之间共享文件的云存储或任何数据存储。安全服务器配置为在验证第二用户是否在访问授权列表之后,确定是否发送解密密钥到第二计算装置。通过随时随地控制加密密钥的访问权限列表,发送者控制谁可以随时随地打开相应的加密文件的访问权。

[0028] 图3示出了根据本专利申请一种实施例的数据安全管理系统的基础体系结构。参照图3,所有的便携式和台式设备301(也称为应用程序装置301)安装有通过互联网或局域网与uSav安全服务器303通信的uSav App。uSav安全服务器303可以位于任何数据中心,包括云计算数据中心、或任何只要uSav App可以与之通信的位置。该通信可以基于Wi-Fi、以太网、互联网、局域网等。uSav App和uSav安全服务器303之间的通信通过预定义的应用程序接口实现。

[0029] 每个uSav使得每个用户能够进行文件/数据加密、解密以及随时随地安全地管理他的/她的数据。uSav安全服务器303和App设备301受限于公司或组织;通信可以通过局域网实现。如果App设备301需要移动,并可以物理分布于世界上的任何地方,则安全服务器303必须通过互联网可访问。

[0030] 安全服务器303可以是从任何云计算服务提供商的数据中心或用户自己的位置(数据中心)操作的虚拟安全服务器。安全服务器303还可以是运行于用户自己的位置或任何其它位置的真实的专用服务器。安全服务器应当处于无单点故障的高可用模式或群集模式。

[0031] 用户可以选择不同的安全级别进行身份验证。在注册或更改用户配置文件设置期间提供选择。存在三种选择:

[0032] 1.用户ID+密码

[0033] 2.用户ID+密码+登录图片

[0034] 3.用户ID+密码+OTP(一次性密码)

[0035] 4.用户ID+密码+登录图片+OTP(一次性密码)

[0036] 用户ID和密码是最低要求的验证方法。用户选择密码。用户需要键入密码两次以核实密码。向用户的电子邮箱地址发送电子邮件。用户需要根据电子邮箱的指令来激活其账户。在用户选择他的/她的密码后,uSav App提供了密码的安全等级:

[0037] 1.低级(最少的密码要求):具有至少一个字母和一个数字的至少八个字符;

[0038] 2.中级:具有至少一个大写字母、一个小写字母和一个数字的至少八个字符;

[0039] 3.高级:具有至少一个大写字母、一个小写字母、一个数字和一个符号的至少八个字符。

[0040] 市面上的认证方法的其它选择可以集成到uSav安全管理系统。

[0041] 为恢复密码,在用户正确回答若干个用于核实的预设问题后,将新的计算机生成的密码发送到用户的电子邮箱地址。为进一步验证,可以使用由USB/智能电话或软件生成的OPT(一次性密码)。

[0042] 就像电子邮件地址列表一样,每个用户可以建立uSav联系人列表。对于每个联系人,所需要的信息为如下:

[0043] 1.联系人的姓名(可选);

[0044] 2.联系人ID:该项必须有联系人或用户的朋友(在本实施例中,使用朋友的电子邮件地址作为ID)提供;

[0045] 3.联系人的备注/评论区(并非用户必须输入项);

[0046] 4.联系人的电子邮件地址(并非用户必须输入项)。

[0047] 虽然可以增加新的联系人,但也可以编辑或删除已有的联系人。可以将一个或多个联系人作为一组,放在一个组名下。可以对组进行编辑。对于一个组,

[0048] 1.可以修改、添加或删除该组中的联系人成员;

[0049] 2.可以修改组名;

[0050] 3.可以删除该组;

[0051] 4.可以添加新的组。

[0052] 允许用户创建没有注册于uSav的联系人。在显示联系人列表期间,未注册的联系人将显示为不同的阴影或颜色。在本实施例中,当文件所有者使用uSav App加密文件时,他/她可以指定授权解密该加密文件的联系人列表。授权的联系人列表为AAL(访问授权列表)。AAL可以包括联系人的姓名和/或联系组的名称。如果AAL为空,则只有文件所有者有权进行解密。可以将一个或多个未注册联系人添加到AAL。在此情况下,向该未注册联系人发送电子邮件,以通知他/她向系统注册。

[0053] 每个AAL绑定相应的唯一加密密钥。应当指出的是,可以通过相同的加密密钥加密一个或多个文件。多个文件使用一个密钥具有好处,例如子目录使用一个密钥。在这种情况下,对于AAL中的联系人,所有的文件具有相同的访问权限。

[0054] 本实施例中存在三种类型的授权:文件所有者授权、非所有者的读取授权和分级多层授权。在文件所有者授权中,当AAL为空时,文件所有者是唯一授权的人。文件所有者可以读取(实际上是解密)并授予读取权限给其它联系人。文件所有者可以永久删除该文件,这将在下文进行更详细的描述。文件所有者可以查看文件的历史日志。用户可以查看他/她

自己的操作日志，也将在下文进行更详细的描述。文件所有者可以更改文件的AAL。在本实施例中，uSav App的内部时区被设置为标准的UTC 0。所有日志将按UTC 0时区示出。

[0055] 特定的加密密钥的访问授权列表中的每个非所有者(或接收方)的解密(或读取)授权还具有定义为如下的授权限制：

[0056] 1.通过开始启动时间限制；当开始时间为0，授权立即启动。在开始时间之前，加密密钥不会被发送到接收方。

[0057] 2.通过结束时间限制；在通过结束时间之后，加密密钥不会被发送到接收方。结束时间可以是永恒。

[0058] 3.所允许的解密(或读取)数量，其范围可以从1到n，其中n>1。

[0059] 当发送到接收方的加密密钥的次数已达到n，则安全服务器将不批准来自接收方的更多的密钥请求。

[0060] 在用于组织或机构的分级多层授权中，可以设置策略，使得组的管理者或主管可以具有访问和解密所有由他/她监督的成员和组创建的加密文件或数据的权限，而不论其是否被该文件或数据的所有者授予访问权限。根据组织的策略，主管可以具有和文件所有者相同或受限的权利。还可以设置可以解密组织中所有加密文件的“超级用户”。

[0061] 设置文件所有者或某人只能加密而不能做其它操作，这也是可取的。这种情况适合于那些只收集信息、加密和保存信息的调查工作者。

[0062] 加密文件的所有者可以显示AAL和加密文件的每个授权用户(AAL+AL)的授权限制。列表上的非注册联系人将显示为不同的阴影或颜色。为安全起见，加密文件的任何接收方不能看到加密文件的AAL+AL。换言之，在本实施例中，第二计算装置即文件接收方受到限制，无法接收访问授权列表。

[0063] 文件所有者可以随时更改任何加密文件的AAL+AL。因为AAL+AL对应于具有唯一密钥ID的唯一的加密密钥，这将在下文进行更详细的描述，所以改变文件的AAL+AL实际上是改变对应于加密密钥的AAL+AL。由于多个文件可能已被一个密钥加密，因此改变单一文件的AAL+AL有效地改变的由同一密钥加密的多个文件的AAL+AL。

[0064] 每个文件由256位CBC加密算法及初始化变量值加密。可以使用其它加密算法，例如3DES等。也可以使用不同加密算法开发具有多个密钥的多重加密。在本实施例中，uSav加密文件的文件类型扩展名是“.usav”，其被添加到原始文件的名称。加密文件的文件图标也很独特。系统能够加密所支持的系统中的任何选定的文件。该选定的文件可以是单个文件、多个文件或文件夹/子目录。如果文件所有者没有成功登录，则选择过程会自动调用登录过程。

[0065] 当选择一个以上的文件进行加密时，文件所有者可以为所有文件选择单个密钥，或者每个文件采用一个唯一的密钥。当选择单个加密密钥，该密钥的AAL+AL将管理所有这些加密文件的访问控制。当选择一个文件对应一个唯一密钥时，该多个文件的每一者将由唯一的密钥进行加密。换言之，文件所有者可以选择是否待加密的所有文件具有一个AAL+AL或者为每个文件单独设置一个AAL+AL。

[0066] 文件所有者可以指定用于存储新加密文件或文件夹/子目录的路径位置。默认路径位置与所选择的原始(未加密的)的明文文件或子目录的位置相同。对于非文件夹加密，每个加密文件出现在(未加密的)明文文件的旁边(默认位置)。

[0067] 在本实施例中，解密将使加密文件恢复到其原始的明文文件，而文件“.usav”将从解密文件中删除。选择文件来解密的过程非常简单、透明且用户友好。用户可以选择单个文件、多个文件或文件夹/子目录来解密。如果用户没有成功登录，该选择过程将自动调用登录过程。文件所有者可以指定存储新解密文件的路径位置。默认路径位置与原始选择的加密文件或子目录的位置相同。对于非文件夹解密，每个解密文件将出现在加密文件的旁边。

[0068] 文件所有者可以永久删除加密文件。任何加密文件的现有副本将永远不会被任何人再次打开，即使是文件所有者。系统通过删除文件的加密密钥来实现这一点。由于多个文件可能已被相同的密钥加密，所以如果密钥被删除，所有这些文件将不能被打开。应当注意的是，即使加密密钥已被删除，与密钥相关的其它信息如作为密钥(或文件)的日志仍然存在。

[0069] 加密文件的所有者可以显示加密文件的历史日志(也称为文件安全登录日志)。历史日志实际上是由uSav安全服务器205(参照图2)的密钥管理者(参照图3的304)所维护的相应加密密钥的日志解释。密钥可以由一个以上的文件使用。在这种情况下，日志包括多个文件的事件。每个日志事件可以包括以下信息：

[0070] 1.每个日志事件的时间和日期(例如，第一个事件为密钥创建)。

[0071] 2.解密设备的ID和类型：

[0072] a.智能设备类型和型号、ID、序列号、电话号码。SIM ID、设备所有者等。

[0073] 3.位置，例如通过GPS获得。

[0074] 4.加密密钥的所有者，以及已采用这个加密密钥加密的文件。

[0075] 5.事件动作的用户ID:这可能是所有人或任何用户。

[0076] 6.事件动作。

[0077] a.密钥创建:在本实施例中，由于密钥是用来做文件加密的，所以这被解释为文件加密。

[0078] b.AAL+AL设置:这是设置允许访问文件密钥和授权限制其每一者的用户列表。

[0079] c.AAL+AL的改变。

[0080] d.用于文件解密的密钥请求，结果可以是成功或带错误代码的失败:由于当已准备好执行文件解密时，用户设备中的APP仅在其已准备好执行文件解密时请求密钥，所以这可以解释为文件解密的动作。

[0081] e.完全成功或带有错误原因的失败的解密。

[0082] f.文件加密的密钥请求:结果是成功或带有原因的失败。

[0083] g.完全成功或带有错误代码的失败的加密。

[0084] h.文件永久删除(这是删除加密密钥):结果是成功或者带有错误代码的失败。

[0085] i.显示文件的历史日志:将替代显示的是加密密钥历史日志。

[0086] 7.事件内容:取决于事件动作。

[0087] a.文件、文件夹或子目录的名称:这是用于加密或解密事件。

[0088] i.如果每个密钥加密单个文件，则文件的名称将被加密。

[0089] ii.如果通过单个密钥加密一组文件，则是第一个文件的名称加上多个文件的指示。

[0090] iii.如果通过单个密钥加密文件夹或子目录，则是该文件夹或子目录的名称加上

文件夹或子目录的指示。

[0091] b.加密密钥大小与加密和算法的类型。

[0092] i.在本实施例中，密钥大小可以是用于对称密钥加密类型的64位、96位、128位和256位；以及用于公钥加密类型的1024位和2048位。

[0093] c.文件和密钥ID。

[0094] d.初始AAL+AL。

[0095] e.新的AAL+AL或对AAL+AL的改变。

[0096] 对于本实施例中的系统的每个用户ID，存在用户操作日志(也称为用户ID安全登录)。用户ID操作日志包括所有与该特定用户相关的操作事件。每个用户ID的操作日志事件可以包括如下信息：

[0097] 1.每个日志事件的时间和日期(例如，第一个事件为用户注册)。

[0098] 2.解密设备的ID和类型：

[0099] a.智能设备类型和型号、ID、序列号、电话号码。SIM ID、设备所有者等。

[0100] 3.通过GPS定位。

[0101] 4.事件动作的用户ID。

[0102] 5.事件动作。

[0103] a.用户成功注册或带错误原因的失败的用户注册。

[0104] b.用户成功登录或带错误原因的失败的用户登录。

[0105] c.用户成功注销或者带错误原因的失败的用户注销。

[0106] d.因超时而强制注销用户。

[0107] e.显示用户的带有成功或失败状态的历史日志。

[0108] 6.事件内容：取决于事件动作。

[0109] 参照图3，uSav App(下文也称为uApp)和uSav安全服务器303(下文也称为SecServer)之间的通信通过预定义API实现。图4示出了用于实现文件加密的uApp和SecServer之间的通信过程。实际的加密过程在用户设备例如PC、智能电话、平板电脑等上实现。假设已成功完成用户认证。文件历史日志记录如前所述也将被更新。

[0110] 参照图4，在步骤1中，用户设备如IPhone中的uApp通过网络(其可以是互联网、局域网等)连接向SecServer请求随机生成的加密密钥。被发送到SecServer的参数包括文件或文件夹或子目录的名称、用户设备类型、型号和ID、位置(GPS)和加密密钥的类型(对称加密或公钥加密)、算法(AES、3DES、Twofish等)以及大小。

[0111] 在步骤2中，在接收到对加密密钥的请求后，SecServer产生随机生成的加密密钥，并为该加密密钥分配密钥ID。加密密钥、密钥ID、用户ID(从通信协议识别)以及日期和时间保存于数据存储器，例如SecServer(图3的303)的密钥管理器(图3的304)中的加密密钥数据库(参照图3的305)。更具体地，SecServer响应步骤1中uApp的请求：

[0112] 1.加密类型、加密算法、加密密钥及其大小；

[0113] 2.唯一的密钥ID，用于识别加密密钥；

[0114] 3.加密密钥生成的日期和时间；

[0115] 4.可以找到加密密钥数据库的互联网位置地址，在本实施例中其为SecServer的互联网位置地址。互联网位置地址可以是IP地址、域名或任何使得SecServer可以通过网络

定位的形式。例如SecServer可以位于公共云。

[0116] 在步骤3中，uApp在加密前为文件生成哈希。哈希算法可以是MD5、SHA-1等。这是为了在未来验证解密文件的完整性。在接收来自SecServer的响应后，uApp加密由用户指定的文件。加密方法由uApp的类型确定，并且也可以由用户预先配置。

[0117] 在步骤4中，在将加密算法应用于文件数据以生成加密数据的末尾，通过uSav App将文件头添加到加密文件数据。文件头包括如下信息：

[0118] 1.步骤2中的来自SecServer的日期和时间；

[0119] 2.文件ID：该文件的随机生成的唯一的ID。为避免文件ID的重复，本实施例中使用随机生成的32字节的ID；

[0120] 3.步骤2中的来自SecServer的密钥ID，用于识别未来的加密密钥；

[0121] 4.所使用的加密/解密算法，如AES256、3DES等；

[0122] 5.步骤2中的来自SecServer的互联网位置地址，用于在将来与SecServer通信；

[0123] 6.头格式标识符，用于识别头参数包括的哪些参数比如上面列出的参数以及头参数如何排列。

[0124] a.头格式标识符事实上描述了头信息是如何隐藏于加密文件中。头格式标识符还描述了头参数是否被加密及其如何加密。头格式ID被分成HFID 1和HFID 2两部分。HFID 1与加密文件在一起，而HFID 2将被发送到安全服务器，如步骤6所述。HFID 1应该能够识别如上第3项和第5项所述的密钥ID和SecServer的互联网位置。

[0125] 通过uSav App利用哈希算法生成具有上述参数的文件头的报头哈希。哈希算法可以是MD5、SHA-1等。这是用于检测报头的完整性。新加密的文件将具有“.usav”作为新的文件扩展名。

[0126] 在步骤5中，在将报头添加到加密文件后，该uApp请求用户提供授权打开和读取该文件的朋友ID的列表。这个列表为如前所述的访问权限列表(AAL)。

[0127] 在步骤6中，uApp发送以下参数给SecServer：

[0128] 1.来自步骤2的密钥ID，其将被用作在将来连接的通信ID；

[0129] 2.AAL+AL；

[0130] 3.如步骤4中所描述的文件ID。

[0131] 4.HDF2，如步骤4中所描述的头格式标志的部分2。

[0132] 5.步骤3中生成的文件哈希(和哈希算法)。

[0133] 6.步骤4中生成的报头哈希(和哈希算法)。

[0134] 在第7步中，SecServer绑定如下参数以及密钥ID：

[0135] 1.创建时间；

[0136] 2.加密密钥、类型和大小；

[0137] 3.从用户通信协议确定的用户ID；

[0138] 4.具有每个授权用户的授权限制的AAL；

[0139] 5.文件ID；

[0140] 6.文件HDF2，即步骤4中描述的头格式标识符的部分2；

[0141] 7.文件哈希和所使用的哈希算法

[0142] 8.例如来自步骤6的报头哈希值和所使用的哈希算法，例如MD5；

[0143] 9.如上所述的文件安全日志。

[0144] 图5示出了根据本专利申请一种实施例的数据安全管理系统中在uApp和SecServer之间的通信过程以实现头文件h解密。在该过程中，文件安全日志也将被更新。参考图5，在步骤1中，用户确定哪些文件解密之后，uApp通过使用上述的HDF1即头格式标识符的部分1从文件头提取密钥ID和互联网位置地址。

[0145] 在步骤2中，uApp通过将密钥ID和互联网位置地址作为参数发送到SecServer以从SecServer请求加密密钥。在步骤3中，SecServer使用密钥ID来查找加密密钥数据库中对应的加密密钥记录。SecServer检查绑定有密钥ID的AAL+AL，以查看请求者是否被授权打开和查看文件。如果不是，则SecServer将拒绝该请求。

[0146] 如果是，SecServer将响应如下参数给请求者：

[0147] 1.加密密钥

[0148] 2.HFID2，即头格式ID的部分2

[0149] 3.文件ID

[0150] 4.文件哈希和所使用的哈希算法

[0151] 5.报头哈希和所使用的哈希算法

[0152] 在从步骤3接收参数后，在步骤4中，uApp根据HFID 2生成原始报头，并利用(步骤3中接收的)哈希方法生成新的报头哈希。uApp将新的报头哈希与步骤3中从SecServer接收的报头哈希进行比较，从而验证待解密的文件的文件头的完整性。如果它们相同，则意味着文件头没有被改变，然后uApp将继续执行步骤5。

[0153] 如果报头哈希不相同，则意味着文件头和以前不一样，不能被可靠使用，从而其结果是来自用户的解密请求将被拒绝。在这种情况下，比较所生成的报头的文件ID和从SecServer接收的文件ID。如果它们不同，很可能是从SecServer接收的密钥错误。如果它们相同，最可能的是加密数据和/或其文件头信息已被改变。

[0154] 在步骤5中，uApp使用SecServer提供的加密密钥来解密使用如前述的文件头确定出的解密方法的文件。uApp将生成解密文件的新的文件哈希(以及步骤3中接收的哈希方法)。uApp比较新的文件哈希和步骤3中的接收自SecServer的文件哈希，从而验证解密文件的完整性。如果它们相同，则意味着该文件没有发生改变，且uApp将继续执行步骤5。如果报头哈希不相同，则意味着文件已发生改变且解密失败。

[0155] 在本实施例中，文件头是由在用户自己的设备中的uApp所创建。更安全的方法是通过SecServer创建文件头。在这种情况下，在加密处理期间，SecServer创建加密文件的完整的文件头，并将其发送给uApp。uApp需要将必要参数发送给SecServer以创建文件头。uApp不知道文件头中数据和参数的格式。为解密文件，uApp需要发送完整的文件头给SecServer。SecServer将对报头哈希进行完整性检查。如果报头哈希通过完整性检查，则SecServer发送加密密钥(对应为解密密钥)和加密方法(对应为解密方法)给uApp以进行解密。

[0156] 文件所有者可以随时随地通过互联网改变AAL+AL，所以只要终端设备通过网络访问SecServer，通过移动设备可以随时随地在AAL+AL中添加、删除或修改任何人的访问权限。

[0157] 通过本实施例提供的系统，不同用户直接的协作也可以实现为如下。用户可以向

uSav App指出多个文件夹为“合作文件夹”。每个合作文件夹可以是普通文件系统或云存储中的文件夹，例如谷歌驱动器中的文件夹。每个“合作文件夹”下的所有文件和子文件夹可以具有相同的预设置的AAL+AL。合作文件夹中的所有当前文件和新文件通过uSav App保护及加密，并被AAL中的用户所共享。对于用户，保存在合作文件夹中的所有纯文本文件将不需直接从用户请求而被uSav透明地自动加密。合作文件夹中的所有由用户打开的加密文件将不许直接从用户请求而由uSav自动且透明地进行解密。

[0158] 在另一实施方式中，数据安全管理系统包括：第一计算装置；第二计算装置；和与第一计算装置和第二计算装置通信的安全服务器。第一计算装置配置成将具有授权限制的访问授权列表发送到安全服务器，以及向安全服务器请求加密密钥。

[0159] 安全服务器配置为发送加密密钥到第一计算装置。第一计算装置配置为使用加密密钥加密文件，并将加密文件共享给第二计算装置。第二计算装置配置为向安全服务器请求解密密钥。安全服务器配置为在验证第二计算装置正由授权访问列表上的用户在授权范围内使用之后，将解密密钥发送到第二计算装置。第二计算装置配置为利用解密密钥对加密文件进行解密。

[0160] 另一种实施方式提供了一种数据安全管理方法。该方法包括：从第一计算装置发送访问授权列表到安全服务器，并通过第一计算装置接收来自安全服务器的加密密钥；从安全服务器发送加密密钥到第一计算装置；通过第一计算装置利用加密密钥加密文件，并将加密文件共享给第二计算装置；从第二计算装置向安全服务器请求解密密钥；通过安全服务器在验证第二计算装置正由访问授权列表上的用户在授权范围内使用之后，将解密密钥发送到第二计算装置；和通过第二计算装置利用解密密钥对加密文件进行解密。

[0161] 在上述实施例提供的系统和方法中，uSav App位于终端设备、智能电话、PC、平板电脑、服务器等。在文件已被加密后，其可以根据用户的选择保存或发送到任何地方，包括任何云数据中心，即公共云或私有云；任何终端设备例如智能电话、平板电脑、PC等；个人PC或任何存储设备，其不存在共享而只是给用户自己保存文件；通过接收带有加密文件作为附件的电子邮件或消息的其他人；或任何服务器、NAS、USB、SD卡或存储设备。由于加密数据可以保存在云数据中心，所以可以实现云数据的安全。系统可以让用户控制他/她的云数据安全，从而即使云数据中心的IT管理员都不能访问加密密钥。此外，SecServer最有可能不位于同一数据中心。如前述，由于数据保留在终端节点、智能电话、平板电脑、PC、USB设备等，也可以实现终端节点的数据安全。uSav App允许文件所有者随时随地改变访问授权列表，即使是在加密文件已发送除去之后。

[0162] 由系统保护的文件的安全级别非常高，原因如下。文件所有者保存明文和加密数据，但加密密钥由uSav安全服务器单独保存。这使得加密数据和加密密钥的物理地址和逻辑地址得以分开。对于任何黑客或组织，从单个物理地址或逻辑地址访问数据是困难的。已知的加密数据存储的位置并不准确。用户可以自由地在任何地方存储加密数据或随时改变位置。uSav安全服务器包含加密密钥，但没有包含数据。黑客、任何人或任何组织将不能单独从系统访问该数据。即使是uSav安全服务器及其管理员都无法访问用户的文件数据。该加密是由用户的本地设备通过uSav App实现。

[0163] 虽然已经通过参考特定的多个实施方式示出及描述了本专利申请，但应当注意的是，可以不脱离本发明的范围而对其进行各种其它改变或修改。

图1

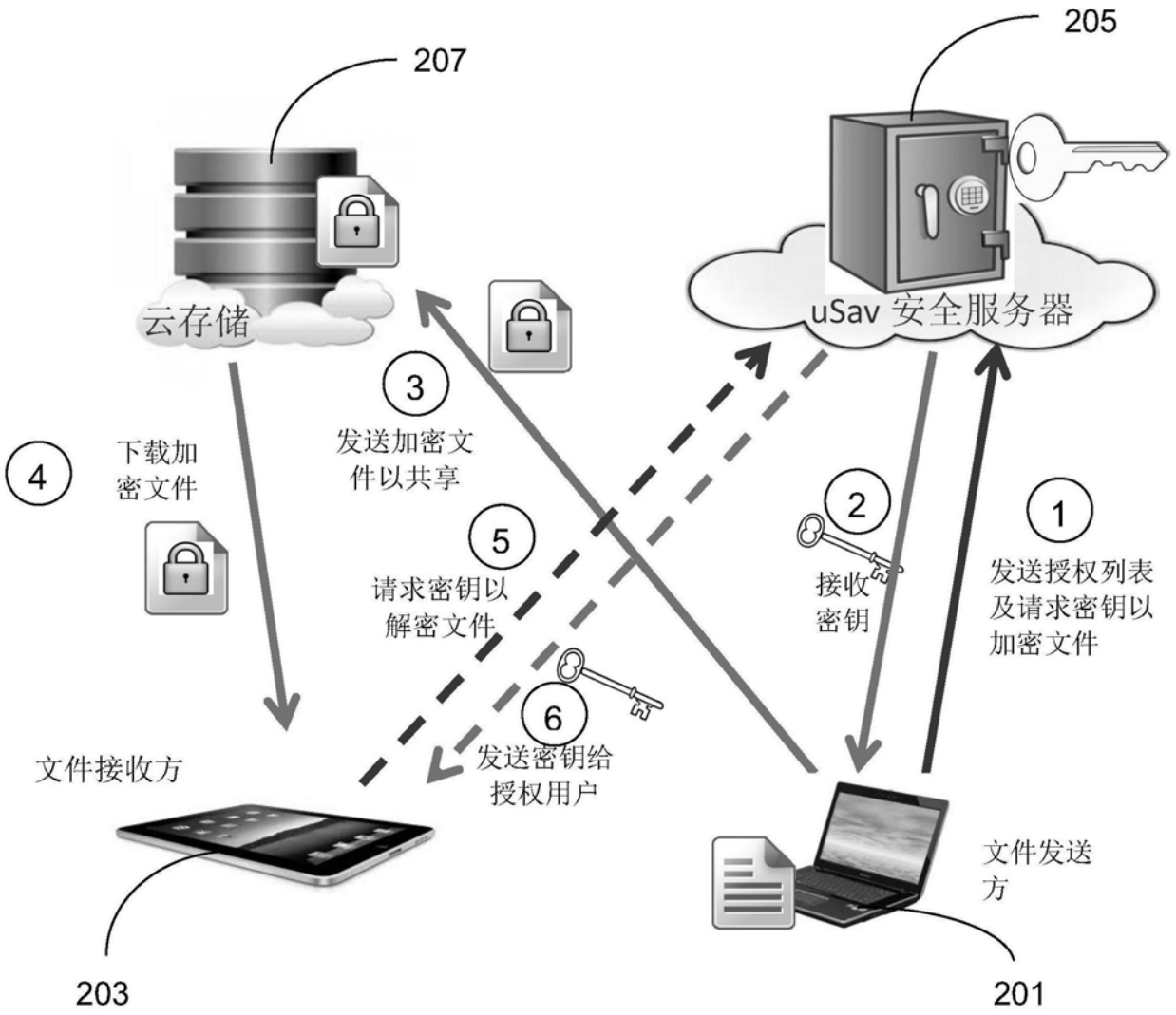
205
207
uSav 安全服务器
云存储
3
发送加密文
件以共享
4
下载加
密文件
5
请求密钥以
解密文件
2
接收
密钥
1
发送授权列表
及请求密钥以
加密文件
6
发送密钥给
授权用户
文件接收方
文件发送
方
203
201

图2

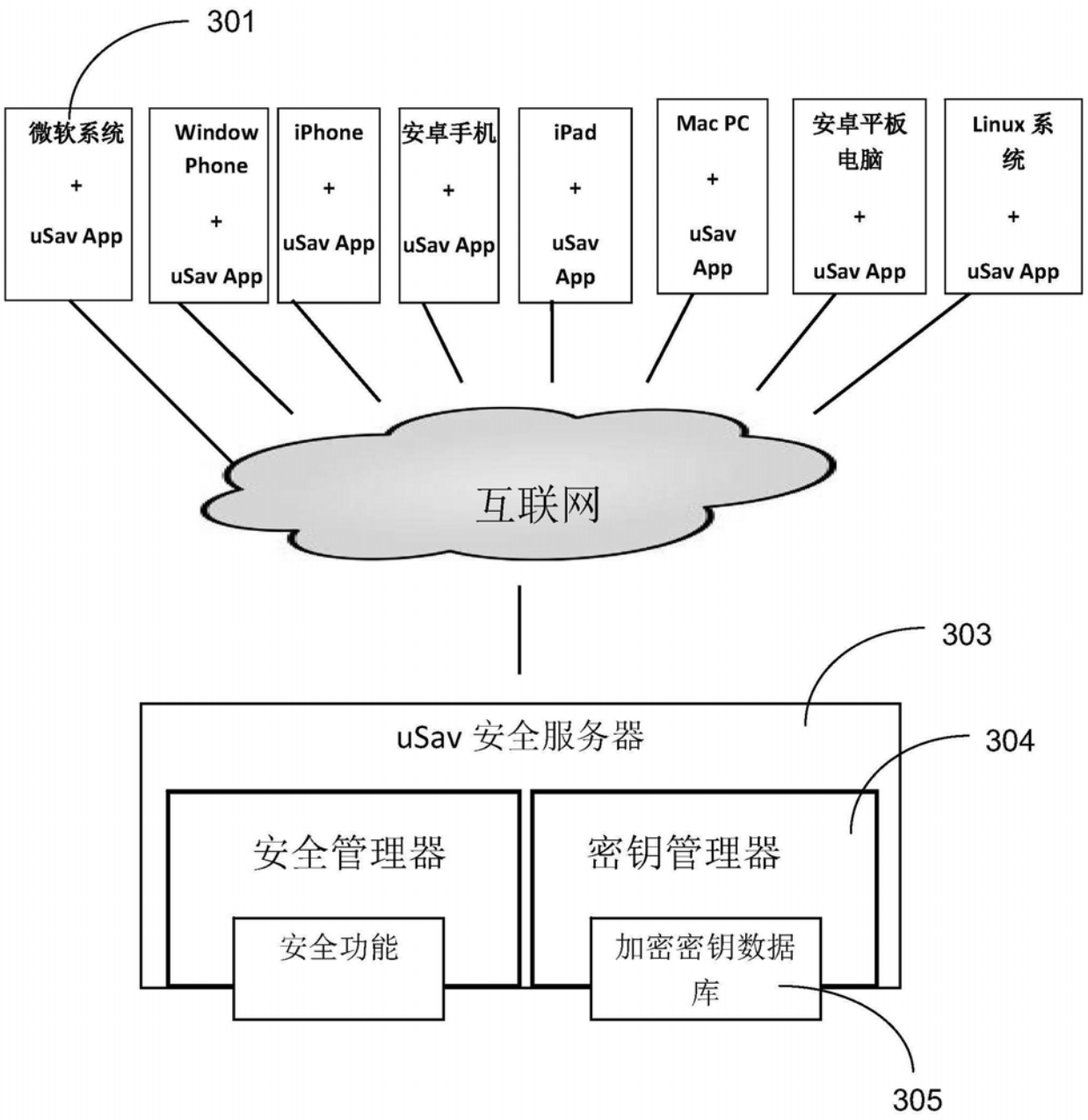
301
微软系统 + uSav App
Window Phone + uSav App
iPhone + uSav App
安卓手机 + uSav App
iPad + uSav App
Mac PC + uSav App
安卓平板电脑 + uSav App
Linux 系统 + uSav App
互联网
303
uSav 安全服务器
304
安全管理器
密钥管理器
安全功能
加密密钥数据库
305

图3

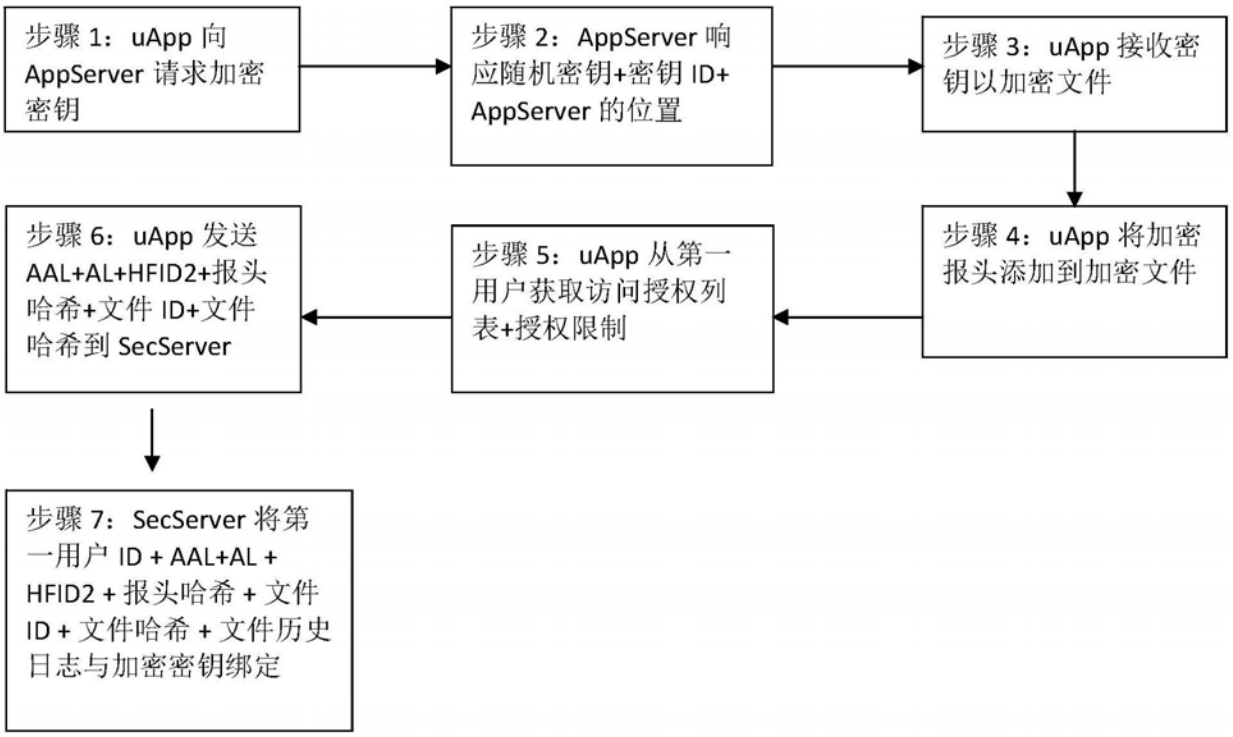
步骤 1：uApp 向 AppServer 请求加密密钥
步骤 2：AppServer 响应随机密钥+密钥 ID+AppServer 的位置
步骤 3：uApp 接收密钥以加密文件
步骤 4：uApp 将加密报头添加到加密文件
步骤 5：uApp 从第一用户获取访问授权列表+授权限制
步骤 6：uApp 发送 AAL+AL+HFID2+报头哈希+文件 ID+文件哈希到 SecServer
步骤 7：SecServer 将第一用户 ID + AAL+AL + HFID2 + 报头哈希 + 文件 ID + 文件哈希 + 文件历史日志与加密密钥绑定

图4

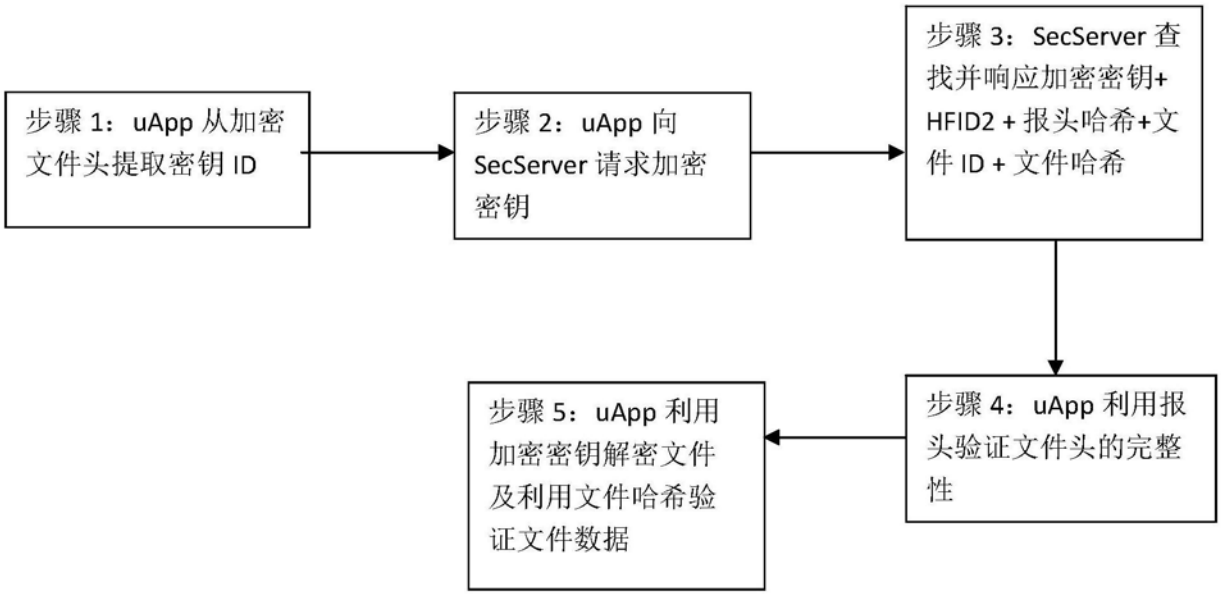
步骤 1：uApp 从加密文件头提取密钥 ID
步骤 2：uApp 向 SecServer 请求加密密钥
步骤 3：SecServer 查找并响应加密密钥+HFID2 + 报头哈希+文件 ID + 文件哈希
步骤 4：uApp 利用报头验证文件头的完整性
步骤 5：uApp 利用加密密钥解密文件及利用文件哈希验证文件数据

图5