(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 107370595 A
(43)申请公布日 2017.11.21

(21)申请号 201710417817.2

(22)申请日 2017.06.06

(71)申请人 福建中经汇通有限责任公司
地址 361000 福建省厦门市翔安区马巷镇莲亭路818号第一层

(72)发明人 郝波 柯炯亮

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/06(2006.01)
H04L 29/06(2006.01)

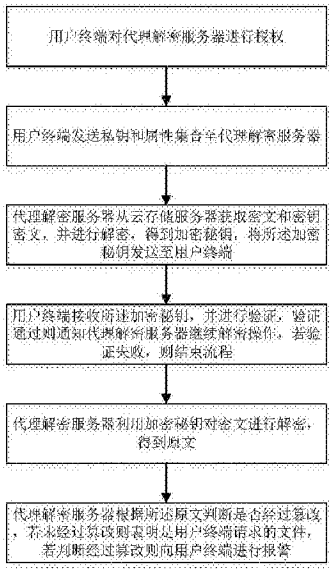
权利要求书2页 说明书8页 附图2页

(54)发明名称

一种基于细粒度的密文访问控制方法

(57)摘要

本发明涉及一种基于细粒度的密文访问控制方法，由代理解密服务器承担了解密计算，而用户终端则几乎没有解密方面的计算开销，可以为用户终端节省了大量的解密计算资源开销。尽管由于文件消息摘要的传输一定程度上增加了终端的网络流量，但是和现有技术相比较，本发明仅增加了较小的网络流量开销，实现了更安全的访问方案，所以本发明方案还是具有很大优势。此外，本发明方案还具有不可否认性和不可伪造性，同时可以保证共享文件的完整性。由代理解密服务器来执行满足访问控制权限的数据解密工作，有效减少了终端用户的解密计算开销，扩展了基于细粒度的密文的云存储访问控制机制的应用场景。



CN 107370595 A

1.一种基于细粒度的密文访问控制方法，其特征在于，包括步骤：

用户终端对代理解密服务器进行授权；

用户终端发送私钥和属性集合至代理解密服务器；

代理解密服务器从云存储服务器获取密文和密钥密文，并进行解密，得到加密秘钥，将所述加密秘钥发送至用户终端；

用户终端接收所述加密秘钥，并进行验证，验证通过则通知代理解密服务器继续解密操作，若验证失败，则结束流程；

代理解密服务器利用加密秘钥对密文进行解密，得到原文；

代理解密服务器根据所述原文判断是否经过篡改，若未经过篡改则表明是用户终端请求的文件，若判断经过篡改则向用户终端进行报警。

2.根据权利要求1所述的一种基于细粒度的密文访问控制方法，其特征在于，在所述用户终端对代理解密服务器进行授权之前，还包括：

第三方信任机构生成公开参数和主秘钥；

第三方信任机构通过用户属性和主秘钥生成用户私钥，分发至各个用户。

3.根据权利要求2所述的一种基于细粒度的密文访问控制方法，其特征在于，在所述第三方信任机构生成公开参数和主秘钥步骤之前，还包括：

数据上传端随机选择一个对称秘钥，对上传至云存储服务器的文件进行加密，得到密文；

所述数据上传端加密对称秘钥得到秘钥密文。

4.根据权利要求3所述的一种基于细粒度的密文访问控制方法，其特征在于，所述方法还包括：数据上传端生成数字签名的公私钥对；

数据上传端对上传至云存储服务器的文件进行哈希摘要算法，得到明文消息摘要，然后对加密文件的对称秘钥生成秘钥消息摘要；

上传所述数字签名、公私钥对、明文消息摘要、秘钥消息摘要一起发送至云存储服务器进行存储。

5.根据权利要求2所述的一种基于细粒度的密文访问控制方法，其特征在于，所述生成用户私钥具体为：

第三方信任机构通过用户属性集Λ和主私钥MK，为每个用户选取随机数$r \in \square_q^*$，为每个属性选取随机数$r_j \in \square_q^*$生成用户私钥，计算如下式：

$SK = (D = g^{(\partial+r)/\beta}, \forall \lambda_i \in \Lambda : D_i = g^r \square H_0(\lambda_i)^{r_i}, D_i' = g^{r_i}, D_i'' = H_0(\lambda_i)^{\beta})$。

6.根据权利要求3所述的一种基于细粒度的密文访问控制方法，其特征在于，所述数据上传端随机选择一个对称秘钥，对上传至云存储服务器的文件进行加密，得到密文，具体为：

步骤1，数据上传端随机选择一个对称密钥K_f，对需要存储的文件f进行对称加密，得到密文：

$C_f = E_{K_f}(f)$；

步骤2，使用访问结构参数Γ加密对称密钥K_f得到秘钥密文C_k，具体为：

$C_k=(\Gamma,C'=k_f\cdot e(g,g)^{\alpha s},C=h^s,\forall y\in Y:C_y=g^{q_x(0)},C_y'=H_0=(att(y))^{q_x(0)})$；

其中，随机数$s\in\mathbb{Z}_q^*$，Y表示访问结构树所有叶子节点的集合，att(y)表示返回叶子节点对应的属性信息，q_x为访问结构树中任意节点x的随机多项式，$q_x(0)$代表x节点的秘密信息。

7.根据权利要求4所述的一种基于细粒度的密文访问控制方法，其特征在于，所述数据上传端对上传至云存储服务器的文件进行哈希摘要算法，得到明文消息摘要，然后对加密文件的对称秘钥生成秘钥消息摘要；上传所述数字签名、公私钥对、明文消息摘要、秘钥消息摘要一起发送至云存储服务器进行存储步骤具体为：

步骤1：参数与秘钥的生成，数据上传端根据大素数q，选择q-1个大素数因子p，且$g^p\equiv 1 \bmod q$，数据上传端生成数字签名的公私钥对(sk,vk)，计算如下：

$sk=x,1<x<p$

$vk=y$ ；

$y\equiv g^x \bmod q$

步骤2，数据上传端对需要存储的文件f执行哈希摘要运算得到明文消息摘要m_f，然后对加密文件的对称秘钥K_f生成秘钥消息摘要m_K，具体计算如下：

$m_f=H_1(f)$，

$m_K=H_1(K_f)$；

数据上传端选取任意$k\in\mathbb{Z}_q^*$，且1＜k＜p，计算：

$r\equiv g^x \bmod q$，

$s\equiv (m_K-xr)k^{-1} \bmod p$。

则数字签名为：

$\delta=(r,s)$；

步骤3，将数字签名、秘钥消息摘要、验证公钥、明文消息摘要、密文、密钥密文信息一同发送至云存储服务器进行存储，云存储服务器针对每个文件建立对应的表项。

一种基于细粒度的密文访问控制方法

技术领域

[0001] 本申请涉及物联网云计算领域，具体的，涉及一种基于细粒度的密文访问控制方法。

背景技术

[0002] 云存储作为一种基本服务得到了业界的广泛认同，越来越多的企事业单位或个人通过云存储服务保留大量的各类数据信息。然而，网络时代的数据信息内涵更为丰富，往往涉及企业的商业秘密或个人隐私，例如企业销售记录信息、公文信息、个人健康信息等。而事实上，提供存储服务的第三方，即云存储服务提供者(Cloud Service Provider,CSP)往往是独立的运营管理机构或组织，并不完全值得信赖。因此，许多个人和企业还都不敢轻易地将自己的重要数据或私密数据存储到云存储服务器，因此，云存储环境下敏感数据的机密性尤为重要。

[0003] 云存储服务虽然带来了许多便利，但是也引起了用户对于其安全性的担忧。有数据显示，出于安全方面的考虑，仍有多达70％的企业用户不愿意将关键数据置于自己的控制区域之外。因此，云存储服务的广泛应用，还要依赖于云存储安全访问控制机制。与此同时，随着信息电子化的进一步发展及法制的进一步完善，企业及个人也会越来越多地将私密的信息存储于云中。现有的访问控制方案可以在云存储环境下有效实施密文共享的细粒度的存储访问控制，能够保证用户数据的机密性、完整性和真实性。但是，尽管一些方案较好地解决了访问策略变更、用户属性变更及访问控制粒度等问题，但这些方案的最终解密都需要共享密文访问的用户自身进行大量的解密计算。此外，多数方案是先下载密文，再检查访问控制权限，满足访问控制权限的，可以顺利解密；对于不满足访问权限的，不仅不能解密密文，可能还会白白花费了网络资源及计算资源。如何实现安全的细粒度访问是社交网络环境下的物联网系统所亟需解决的问题之一。

发明内容

[0004] 本发明旨在至少解决现有技术中存在的技术问题之一。

[0005] 为此，本发明的目的在于，通过设计一种基于细粒度的密文访问控制方法，结合数字签名技术，由代理解密服务器执行满足访问控制权限的数据解密操作。本发明的技术方案不仅有效减少了用户终端的计算开销，而且又达到了共享密文访问控制的目的，安全性也大大提高。

[0006] 为实现上述目的，本发明提供一种基于细粒度的密文访问控制方法，包括步骤：

[0007] 用户终端对代理解密服务器进行授权；

[0008] 用户终端发送私钥和属性集合至代理解密服务器；

[0009] 代理解密服务器从云存储服务器获取密文和密钥密文，并进行解密，得到加密秘钥，将所述加密秘钥发送至用户终端；

[0010] 用户终端接收所述加密秘钥，并进行验证，验证通过则通知代理解密服务器继续

解密操作，若验证失败，则结束流程；

[0011] 代理解密服务器利用加密秘钥对密文进行解密，得到原文；

[0012] 代理解密服务器根据所述原文判断是否经过篡改，若未经过篡改则表明是用户终端请求的文件，若判断经过篡改则向用户终端进行报警。

[0013] 具体的，在所述用户终端对代理解密服务器进行授权之前，还包括：

[0014] 第三方信任机构生成公开参数和主秘钥；

[0015] 第三方信任机构通过用户属性和主秘钥生成用户私钥，分发至各个用户；

[0016] 具体的，在所述第三方信任机构生成公开参数和主秘钥步骤之前，还包括：

[0017] 数据上传端随机选择一个对称秘钥，对上传至云存储服务器的文件进行加密，得到密文；

[0018] 所述数据上传端加密对称秘钥得到秘钥密文；

[0019] 具体的，所述方法还包括：数据上传端生成数字签名的公私钥对；

[0020] 数据上传端对上传至云存储服务器的文件进行哈希摘要算法，得到明文消息摘要，然后对加密文件的对称秘钥生成秘钥消息摘要；

[0021] 上传所述数字签名、公私钥对、明文消息摘要、秘钥消息摘要一起发送至云存储服务器进行存储。

[0022] 更具体的，所述生成用户私钥具体为：

[0023] 第三方信任机构通过用户属性集Λ和主私钥MK，为每个用户选取随机数$r\in\mathbb{Z}_q^*$，为每个属性选取随机数$r_j\in\mathbb{Z}_q^*$生成用户私钥，计算如下式：

$$SK=(D=g^{(\partial+r)/\beta},\forall\lambda_i\in\Lambda:D_i=g^r\cdot H_0(\lambda_i)^{r_i},D_i'=g^{r_i},D_i''=H_0(\lambda_i)^{\beta})。$$

[0024] 更具体的，所述数据上传端随机选择一个对称秘钥，对上传至云存储服务器的文件进行加密，得到密文，具体为：

[0025] 步骤1，数据上传端随机选择一个对称密钥K_f，对需要存储的文件f进行对称加密，得到密文：

[0026] $C_f=E_{K_f}(f)$；

[0027] 步骤2，使用访问结构参数Γ加密对称密钥K_f得到秘钥密文C_k，具体为：

$$C_k=(\Gamma,C'=k_f\cdot e(g,g)^{\partial/s},C=h^s,\forall y\in Y:C_y=g^{q_x(0)},C_y'=H_0=(att(y))^{q_x(0)})；$$

[0028] 其中，随机数$s\in\mathbb{Z}_q^*$，Y表示访问结构树所有叶子节点的集合，att(y)表示返回叶子节点对应的属性信息，q_x为访问结构树中任意节点x的随机多项式，$q_x(0)$代表x节点的秘密信息。

[0029] 更具体的，所述数据上传端对上传至云存储服务器的文件进行哈希摘要算法，得到明文消息摘要，然后对加密文件的对称秘钥生成秘钥消息摘要；上传所述数字签名、公私钥对、明文消息摘要、秘钥消息摘要一起发送至云存储服务器进行存储步骤具体为：

[0030] 步骤1：参数与秘钥的生成，数据上传端根据大素数q，选择q-1个大素数因子p，且$g^p\equiv 1 \bmod q$，数据上传端生成数字签名的公私钥对(sk，vk)，计算如下：

[0031] sk＝x，1＜x＜p

[0032] vk＝y；

[0033] $y \equiv g^x \bmod q$

[0034] 步骤2，数据上传端对需要存储的文件f执行哈希摘要运算得到明文消息摘要m_f，然后对加密文件的对称秘钥K_f生成秘钥消息摘要m_K，具体计算如下：

[0035] $m_f = H_1(f)$，

[0036] $m_K = H_1(K_f)$；

[0037] 数据上传端选取任意$k \in \mathbb{Z}_q^*$，且1＜k＜p，计算：

[0038] $r \equiv g^x \bmod q$，

[0039] $s \equiv (m_K - xr)k^{-1} \bmod p$。

[0040] 则数字签名为：

[0041] $\delta = (r, s)$。

[0042] 步骤3，将数字签名、秘钥消息摘要、验证公钥、明文消息摘要、密文、密钥密文信息一同发送至云存储服务器进行存储，云存储服务器针对每个文件建立对应的表项。

[0043] 通过本发明的技术方案，可知本发明由代理解密服务器基本承担了解密计算，而用户终端则几乎没有解密方面的计算开销。因此，该方案非常适用于在一个内部可信网络环境下建立代理解密服务机制的情形，可以为用户终端节省了大量的解密计算资源开销。尽管由于文件消息摘要的传输一定程度上增加了终端的网络流量，但是和现有技术相比较，本发明仅增加了较小的网络流量开销，实现了更安全的访问方案，所以本发明方案还是具有很大优势。此外，本方案还具有不可否认性和不可伪造性，同时可以保证共享文件的完整性。由代理解密服务器来执行满足访问控制权限的数据解密工作，有效减少了终端用户的解密计算开销，扩展了基于密文的云存储访问控制机制的应用场景。

附图说明

[0044] 图1示出了本发明一种基于细粒度的密文访问控制方法的流程图；

[0045] 图2示出了本发明的一实施例的系统结构框图。

具体实施方式

[0046] 为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

[0047] 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

[0048] 图1示出了本发明一种基于细粒度的密文访问控制方法的流程图。

[0049] 如图1所示，一种基于细粒度的密文访问控制方法，包括步骤：

[0050] 用户终端对代理解密服务器进行授权；

[0051] 用户终端发送私钥和属性集合至代理解密服务器；

[0052] 代理解密服务器从云存储服务器获取密文和密钥密文，并进行解密，得到加密秘钥，将所述加密秘钥发送至用户终端；

[0053] 用户终端接收所述加密秘钥，并进行验证，验证通过则通知代理解密服务器继续

解密操作，若验证失败，则结束流程；

[0054] 代理解密服务器利用加密秘钥对密文进行解密，得到原文；

[0055] 代理解密服务器根据所述原文判断是否经过篡改，若未经过篡改则表明是用户终端请求的文件，若判断经过篡改则向用户终端进行报警。

[0056] 具体的，在所述用户终端对代理解密服务器进行授权之前，还包括：

[0057] 第三方信任机构生成公开参数和主秘钥；

[0058] 第三方信任机构通过用户属性和主秘钥生成用户私钥，分发至各个用户；

[0059] 具体的，在所述第三方信任机构生成公开参数和主秘钥步骤之前，还包括：

[0060] 数据上传端随机选择一个对称秘钥，对上传至云存储服务器的文件进行加密，得到密文；

[0061] 所述数据上传端加密对称秘钥得到秘钥密文；

[0062] 具体的，所述方法还包括：数据上传端生成数字签名的公私钥对；

[0063] 数据上传端对上传至云存储服务器的文件进行哈希摘要算法，得到明文消息摘要，然后对加密文件的对称秘钥生成秘钥消息摘要；

[0064] 上传所述数字签名、公私钥对、明文消息摘要、秘钥消息摘要一起发送至云存储服务器进行存储。

[0065] 更具体的，所述生成用户私钥具体为：

[0066] 第三方信任机构通过用户属性集Λ和主私钥MK，为每个用户选取随机数$r\in\mathbb{Z}_q^*$，为每个属性选取随机数$r_j\in\mathbb{Z}_q^*$生成用户私钥，计算如下式：

$$SK=(D=g^{(\partial+r)/\beta},\forall\lambda_i\in\Lambda:D_i=g^r\cdot H_0(\lambda_i)^{r_i},D_i'=g^{r_i},D_i''=H_0(\lambda_i)^{\beta})。$$

[0067] 更具体的，所述数据上传端随机选择一个对称秘钥，对上传至云存储服务器的文件进行加密，得到密文，具体为：

[0068] 步骤1，数据上传端随机选择一个对称密钥K_f，对需要存储的文件f进行对称加密，得到密文：

[0069] $C_f=E_{K_f}(f)$；

[0070] 步骤2，使用访问结构参数Γ加密对称密钥K_f得到秘钥密文C_k，具体为：

$$C_k=(\Gamma,C'=k_f\cdot e(g,g)^{\partial\cdot k},C=h^s,\forall y\in Y:C_y=g^{q_x(0)},C_y'=H_0=(att(y))^{q_x(0)})；$$

[0071] 其中，随机数$s\in\mathbb{Z}_q^*$，Y表示访问结构树所有叶子节点的集合，att(y)表示返回叶子节点对应的属性信息，q_x为访问结构树中任意节点x的随机多项式，$q_x(0)$代表x节点的秘密信息。

[0072] 更具体的，所述数据上传端对上传至云存储服务器的文件进行哈希摘要算法，得到明文消息摘要，然后对加密文件的对称秘钥生成秘钥消息摘要；上传所述数字签名、公私钥对、明文消息摘要、秘钥消息摘要一起发送至云存储服务器进行存储步骤具体为：

[0073] 步骤1：参数与秘钥的生成，数据上传端根据大素数q，选择q-1个大素数因子p，且$g^p\equiv 1 \bmod q$，数据上传端生成数字签名的公私钥对(sk，vk)，计算如下：

[0074] sk＝x，1＜x＜p

[0075] vk＝y；

[0076] $y \equiv g^x \bmod q$

[0077] 步骤2，数据上传端对需要存储的文件f执行哈希摘要运算得到明文消息摘要m_f，然后对加密文件的对称秘钥K_f生成秘钥消息摘要m_K，具体计算如下：

[0078] $m_f = H_1(f)$，

[0079] $m_K = H_1(K_f)$；

[0080] 数据上传端选取任意$k \in \mathbb{Z}_q^*$，且1＜k＜p，计算：

[0081] $r \equiv g^x \bmod q$，

[0082] $s \equiv (m_K - xr)k^{-1} \bmod p$。

[0083] 则数字签名为：

[0084] $\delta = (r, s)$；

[0085] 步骤3，将数字签名、秘钥消息摘要、验证公钥、明文消息摘要、密文、密钥密文信息一同发送至云存储服务器进行存储，云存储服务器针对每个文件建立对应的表项。

[0086] $\delta, m_K, vk, m_f, C_f, C_k$分别为数字签名、秘钥消息摘要、验证公钥、明文消息摘要、密文、密钥密文。

[0087] 图2示出了本发明的一实施例的系统结构框图。

[0088] 如图2所示，本访问系统包括：

[0089] 第三方信任机构：用于方案中系统初始化，即生成系统公开参数和主密钥并且需要维护一个数据上传端共享密文的摘要列表。

[0090] 数据上传端：表示方案中提供共享信息或文件的用户所在的终端，所述用户是原始明文的拥有者。

[0091] 云存储服务器：为用户提供数据存储服务。

[0092] 本地代理解密服务器：为用户提供代理解密服务。是在安全内网环境下可信的代理服务器。用户可以通过授权为自己解密云中的文件，同时保证对于解密文件的不可抵赖性，确认共享文件的完整性。

[0093] 用户终端：用户终端通过代理服务器进行密文访问的终端用户，可以是企事业单位内部的普通PC终端，移动终端等用户，也可以是开放环境下的普通用户。

[0094] 本系统的具体过程如下：

[0095] (1) 系统初始化过程

[0096] 设一个双线性映射$e: G_1 \times G_1 \rightarrow G_2$，$G_1, G_2$都是q阶的循环群，其中q为任意选取的一个大素数。设g，h_1为群G_1的生成元。α，β为两个随机数。输出公开参数PK和主秘钥MK如下：

[0097] $PK = \{q, g, h_1, e(g,g)^{\partial}\}$

[0098] $h_1 = g^{\beta}$

[0099] $MK = \{\beta, g^{\alpha}\}$

[0100] (2) 秘钥生成

[0101] 第三方信任机构通过用户属性集Λ和主私钥MK，为每个用户选取随机数$r \in \mathbb{Z}_q^*$，为每个属性选取随机数$r_j \in \mathbb{Z}_q^*$生成用户私钥：

[0102] $SK = (D = g^{(\partial + r)/\beta}, \forall \lambda_i \in \Lambda : D_i = g^r \cdot H_0(\lambda_i)^{r_i}, D_i' = g^{r_i}, D_i'' = H_0(\lambda_i)^{\beta})$

[0103] 通过安全通道分发给各个用户。

[0104] (3)加密过程

[0105] 为了提高加解密效率，先采用对称密钥加密明文，得到数据密文C_f；再对对称密钥k_f得到密钥密文；同时，为了代理解密时确认信息的完整性及不可否认性，还要将不同文件的数字签名及验证公钥一同存储在云存储服务器，即云存储服务器需要维护所有数据上传端的共享密文文件及其数字签名、公钥等信息的列表。具体的步骤如下：

[0106] 步骤1：数据上传端随机选择一个对称密钥K_f，对需要存储的文件f进行对称加密，得到密文：

[0107] $C_f = E_{K_f}(f)$；

[0108] 步骤2：使用访问结构参数Γ加密对称密钥K_f得到秘钥密文C_k，具体为：

$$C_k = (\Gamma, C' = k_f \cdot e(g,g)^{\partial s}, C = h^s, \forall y \in Y : C_y = g^{q_x(0)}, C_y' = H_0 = (att(y))^{q_x(0)})。$$

[0109] 其中，随机数$s \in \mathbb{Z}_q^*$，Y表示访问结构树所有叶子节点的集合，att(y)表示返回叶子节点对应的属性信息，q_x为访问结构树中任意节点x的随机多项式，$q_x(0)$代表x节点的秘密信息。对于访问树根节点R，$q_R(0)=s$。

[0110] (4)数字签名

[0111] 具体步骤为：

[0112] 步骤1：参数与秘钥的生成。数据上传端根据大素数q，选择q-1个大素数因子p，且$g^p \equiv 1 \bmod q$，数据上传端生成数字签名的公私钥对(sk,vk)如下：

[0113] $sk = x, 1 < x < p$

[0114] $vk = y$

[0115] $y \equiv g^x \bmod q$

[0116] 步骤2：数据上传端对需要存储的文件f执行哈希摘要运算得到明文消息摘要m_f，然后对加密文件的对称秘钥K_f生成秘钥消息摘要m_K：

[0117] $m_f = H_1(f)$，

[0118] $m_K = H_1(K_f)$。

[0119] 数据上传端选取任意$k \in \mathbb{Z}_q^*$，且$1 < k < p$，计算：

[0120] $r \equiv g^x \bmod q$，

[0121] $s \equiv (m_K - xr)k^{-1} \bmod p$。

[0122] 则数字签名为：

[0123] $\delta = (r,s)$。

[0124] 步骤3：将上面所有的信息，数字签名、消息摘要等信息和秘钥密文、文件密文，一同发送至云存储服务器进行存储，云存储服务器针对每个文件建立对应的表项：

[0125] $C = \{\delta, m_K, vk, m_f, C_f, C_k\}$。

[0126] (5)解密过程

[0127] 当终端用户在用户终端请求解密服务时，首先要由用户端对代理解密服务器进行授权，然后将自己的私钥SK及属性集传送至代理解密服务器。代理解密服务器得到用户私钥SK后从云存储服务器获取$C = \{\delta, m_K, vk, m_f, C_f, C_k\}$。具体如下：

[0128] 步骤1：用户终端向代理解密服务器授权，

[0129] 步骤2：终端用户通过用户终端发送请求至代理解密服务器时，代理解密服务器从

云存储服务器处获取对应的δ,m_K,vk,m_f,C_f,C_k信息；

[0130] 步骤3：代理解密服务器根据获得的密文C_f,C_k，进行解密，得到加密秘钥K'_f，并将得到的K'_f发送至用户终端；

[0131] 步骤4：用户终端进行验证。若用户终端验证通过，则通知代理解密服务器，继续解密操作，即代理解密服务器利用加密秘钥K'_f解密C_f，得到原文f'。

[0132] 步骤5：用户终端验证原文件是否被篡改，具体如下：

[0133] $m'_f=H_1(f')$

[0134] 若$m'_f=m_f$成立，则用户终端验证为原文f'是要获取的文件，即该文件是未经篡改的。

[0135] 对称密钥是随机选取的，可以采用一次一密的对称加密算法，保证了信息明文的安全性。终端用户在发送私钥组件以及接收明文时，对外部而言是安全的。

[0136] 为了进一步验证文件信息是否在外部已被修改，由于文件摘要的生成采用了哈希函数，哈希函数的雪崩效应保证了密文数据一旦被更改，终端用户一旦验证就会及时发现，也确认了信息的完整性。

[0137] 由代理解密服务器基本承担了解密计算，而用户终端则几乎没有解密方面的计算开销。因此，该方案非常适用于在一个内部可信网络环境下建立代理解密服务机制的情形，可以为用户终端节省了大量的解密计算资源开销。尽管由于文件消息摘要的传输一定程度上增加了终端的网络流量，但是和现有技术相比较，本发明仅增加了较小的网络流量开销，实现了更安全的访问方案，所以本发明方案还是具有很大优势。此外，本方案还具有不可否认性和不可伪造性，同时可以保证共享文件的完整性。由代理解密服务器来执行满足访问控制权限的数据解密工作，有效减少了终端用户的解密计算开销，扩展了基于密文的云存储访问控制机制的应用场景。

[0138] 应理解，说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本发明的至少一个实施例中。因此，在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。应理解，在本发明的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0139] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0140] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合

或通信连接，可以是电性的、机械的或其它形式的。

[0141] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元；既可以位于一个地方，也可以分布到多个网络单元上；可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0142] 另外，在本发明各实施例中的各功能单元可以全部集成在一个处理单元中，也可以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0143] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：移动存储设备、只读存储器(Read Only Memory，ROM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0144] 或者，本发明上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机、服务器、或者网络设备等)执行本发明各个实施例所述方法的全部或部分。而前述的存储介质包括：移动存储设备、ROM、磁碟或者光盘等各种可以存储程序代码的介质。

[0145] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

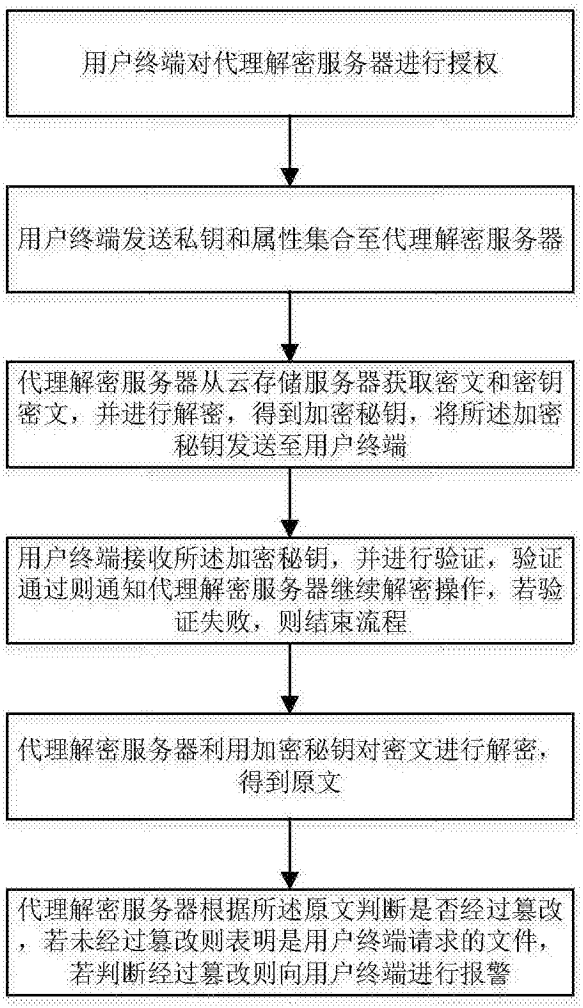

用户终端对代理解密服务器进行授权
用户终端发送私钥和属性集合至代理解密服务器
代理解密服务器从云存储服务器获取密文和密钥密文，并进行解密，得到加密秘钥，将所述加密秘钥发送至用户终端
用户终端接收所述加密秘钥，并进行验证，验证通过则通知代理解密服务器继续解密操作，若验证失败，则结束流程
代理解密服务器利用加密秘钥对密文进行解密，得到原文
代理解密服务器根据所述原文判断是否经过篡改，若未经过篡改则表明是用户终端请求的文件，若判断经过篡改则向用户终端进行报警

图1

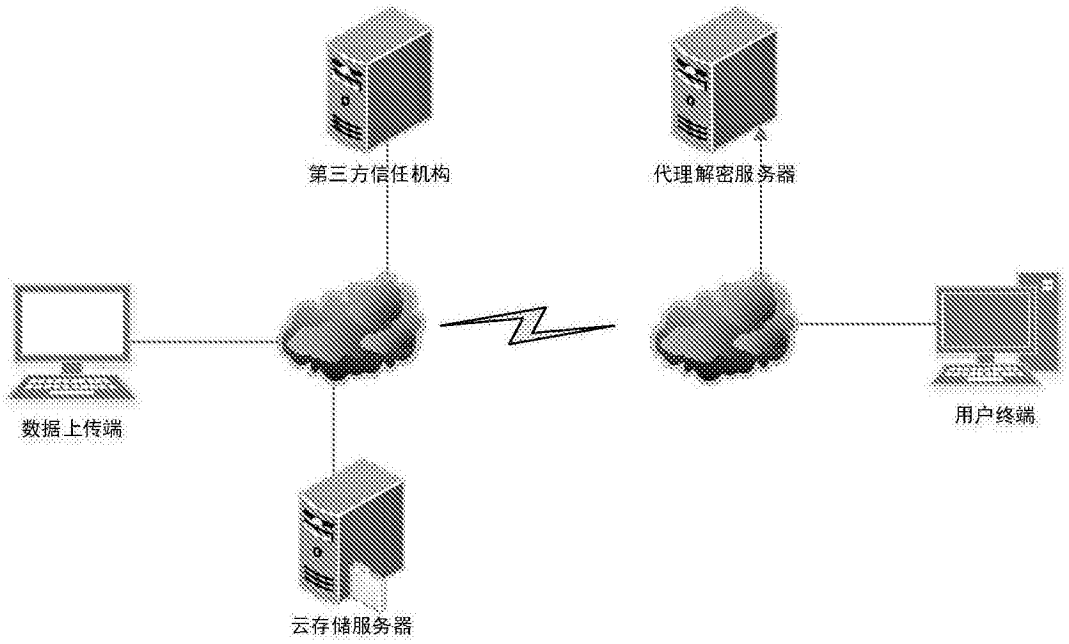


图2