(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 103227789 B
(45)授权公告日 2015.09.16

(21)申请号 201310138434.3
(22)申请日 2013.04.19
(73)专利权人 武汉大学
地址 430072 湖北省武汉市武昌区珞珈山武汉大学
(72)发明人 彭智勇 程芳权 王书林 宋伟
(74)专利代理机构 武汉科皓知识产权代理事务所(特殊普通合伙) 42222
代理人 张火春
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

审查员 孟维志

(56)对比文件
CN 102739689 A,2012.10.17,
US 2013042106 A1,2013.02.14,
韩德志等.《一种在云计算下的细粒度数据访问控制算法》.《华中科技大学学报》.2012,第40卷1-4.

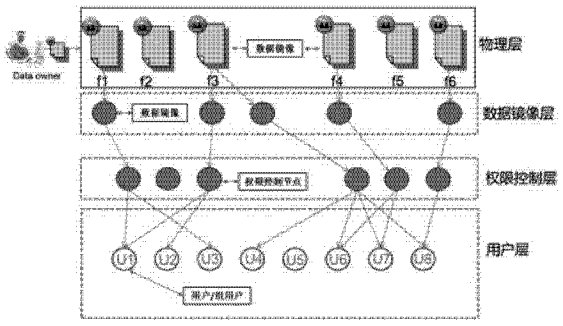
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种云环境下轻量级的细粒度访问控制方法

(57)摘要

本发明涉及云存储环境下一种轻量级的细粒度访问控制方法,属于安全云存储领域,包括以下步骤:1.数据上传;2.数据的授权;3.数据的访问;4.授权撤销;5.数据更新;本发明提供了一种轻量级、细粒度的访问控制方法,构建数据镜像和权限控制层,能够有效实现无副本数据共享以及细粒度的数据访问控制,并确保数据加密密钥的安全性。



CN 103227789 B

1. 一种云环境下轻量级的细粒度访问控制方法，其特征在于，包括以下步骤：

步骤 1：上传数据及初始化，其实现方式为：

一方面，数据拥有者通过自己的公钥本地加密所要上传的明文数据，得到密文数据；然后将所述的密文数据上传至云端；

另一方面，根据数据拥有者的访问控制需求，构造相应的权限控制节点层；

步骤 2：数据的授权，其实现方式包括如下步骤：

步骤 2.1：确定授权数据，针对每个所要授权的数据，生成一个对应的数据镜像，如果所述的数据需要被多次授权，则相应生成多个镜像，所述的数据拥有者为所述的每个镜像生成一个公私钥对；

步骤 2.2：计算所述的数据与其镜像之间的代理重加密密钥，存储在云端；

步骤 2.3：计算会话密钥，对于每一个被授权用户，所述的数据拥有者通过自己的私钥与所述的授权用户的公钥及公开参数构造出一个会话密钥，所述的用户指一个单用户或者一个用户群组；

步骤 2.4：通过所述的会话密钥对所述的镜像的私钥进行加密，将加密后的密文存储于所述的权限控制节点，同时更新所述的权限控制节点中所述的授权用户信息；

步骤 3：数据的读取：

所述的用户请求读取某个数据，系统首先根据所述的权限控制节点判断当前用户是否拥有该数据访问权限，如果有，则将所述的用户请求的数据经过镜像的重加密以及其权限控制节点中加密的镜像私钥发送给所述的用户，所述的用户在客户端则通过第一轮解密获得所述的镜像私钥，然后利用该私钥进行第二轮解密并最终获得所述的明文数据；否则，拒绝所述的用户请求；

步骤 4：授权撤销：

所述的被授权用户被请求撤销授权，系统判断所述的被授权用户与所述的数据之间是否存在访问路径，如果不存在，拒绝所述的请求；如果存在，系统判断所述的权限控制节点是否存在该用户信息，如果有：

如果所述的数据只对应一个镜像，则直接从云端删除该数据镜像，并清空其权限控制节点信息；

如果所述的数据只对应一个镜像，但是只针对部分用户执行授权撤销，则首先清空权限控制节点中的对应用户信息，其次对当前镜像重新生成公私钥对，并生成以该公私钥对为目标的重加密密钥，以及加密处理其私钥，最后更新权限控制节点中的用户授权信息为加密后的镜像私钥；

如果所述的数据对应于多个镜像，且需要对所有镜像执行授权撤销，则删除对应镜像，并更新权限控制节点中的被授权用户信息；

如果所述的数据对应于多个镜像，但是执行多镜像中部分用户的授权撤销，则针对相关的每一个镜像，首先清空权限控制节点中的对应用户信息，其次对当前镜像重新生成公私钥对，并生成以该公私钥对为目标的重加密密钥，以及加密处理其私钥，最后更新权限控制节点中的用户授权信息为加密后的镜像私钥；

否则，拒绝所述的请求；

步骤 5：数据更新，当对云端的某些所述的数据进行更新后，

如果是对其访问授权保持不变，则不执行任何操作；

如果需要撤销某些所述的授权，则按照所述的步骤 4 中的授权撤销执行；

如果需要新增访问授权，则按照所述的步骤 2 中的数据授权执行。

2. 根据权利要求 1 所述的云环境下轻量级的细粒度访问控制方法，其特征在于：步骤 1 中所述的构造相应的权限控制节点层，所述的每个节点被赋予被授权用户的相关信息。

3. 根据权利要求 1 所述的云环境下轻量级的细粒度访问控制方法，其特征在于：随着系统的运行，以及权限的变更，可以对所述的权限控制节点进行动态更新。

一种云环境下轻量级的细粒度访问控制方法

技术领域

[0001] 本发明属于安全云存储领域，特别是涉及到隐私数据轻量级、细粒度、灵活的数据访问控制方法。

背景技术

[0002] 云计算作为一种新的网络计算模型一经提出，便得到了学术界，工业界的极大关注。云存储服务以其特有的良好扩展性、便捷的部署以及低廉的成本迅速得到发展，无论学术界还是工业界都取得了显著的成果。

[0003] 尽管云存储服务在如此短的时间内取得如此多显著成果，但其在发展过程中所面临的问题依然制约着云存储的进一步发展，而目前公认的制约云存储服务发展的瓶颈便是数据安全问题，尽管目前有很多安全技术来保证数据安全，但大部分的技术更多关注的是来自外部的威胁，而针对云存储提供商的内部威胁并没有得到有效关注。

[0004] 目前的主要通过对数据的本地加解密技术来抵御来自云存储提供商的内部攻击。尽管目前的本地加解密技术有效的抵御了来自云服务提供商内部以及网络中的攻击，但却极大的影响了数据在不同用户之间的共享。尽管密钥协商机制可以解决密文数据的共享，但该机制会导致每次数据授权的高计算成本，以及无法有效的进行授权撤销或更新，而只能通过对数据重新加密的方式进行授权撤销或更新。

[0005] 针对当前的密文数据访问控制方法进行分析发现，当前的密文数据访问控制方法存在以下主要问题：

[0006] 1. 在保证数据安全的前提，没有一个有效的机制来解决无副本的密文数据共享。

[0007] 2. 目前的数据授权大部分都是基于静态的角色或者属性划分，无法针对数据进行灵活的，细粒度的数据授权。

[0008] 3. 一旦对密文进行数据授权后，尤其是针对同一数据进行多次授权后，不能有效的针对数据进行授权撤销，目前大部分采用对数据进行重加密机制，大大加重了计算代价并且会导致其他可访问用户的密钥更换。

发明内容

[0009] 为解决上述问题，本发明提供了一种云环境下轻量级的细粒度访问控制方法，包括以下步骤：

[0010] 步骤 1：上传数据及初始化，其实现方式为：

[0011] 一方面，数据拥有者通过自己的公钥本地加密所要上传的明文数据，得到密文数据；然后将所述的密文数据上传至云端；

[0012] 另一方面，根据数据拥有者的访问控制需求，构造相应的权限控制节点层；

[0013] 步骤 2：数据的授权，其实现方式包括如下步骤：

[0014] 步骤 2.1：确定授权数据，针对每个所要授权的数据，生成一个对应的数据镜像，如果所述的数据需要被多次授权，则相应生成多个镜像，所述的数据拥有者为所述的每个

镜像生成一个公私钥对；

[0015] 步骤 2.2：计算所述的数据与其镜像之间的代理重加密密钥，存储在云端；

[0016] 步骤 2.3：计算会话密钥，对于每一个被授权用户，所述的数据拥有者通过自己的私钥与所述的授权用户的公钥及公开参数构造出一个会话密钥，所述的用户指一个单用户或者一个用户群组；

[0017] 步骤 2.4：通过所述的会话密钥对所述的镜像的私钥进行加密，将加密后的密文存储于所述的权限控制节点，同时更新所述的权限控制节点中所述的授权用户信息；

[0018] 步骤 3：数据的读取：

[0019] 所述的用户请求读取所述的某个数据，系统首先根据所述的权限控制节点判断所述的当前用户是否拥有该数据访问权限，如果有，则将所述的用户请求的数据经过镜像的重加密以及其权限控制节点中加密的镜像私钥发送给所述的用户，所述的用户在客户端则通过第一轮解密获得所述的镜像私钥，然后利用该私钥进行第二轮解密并最终获得所述的明文数据；否则，拒绝所述的用户请求；

[0020] 步骤 4：授权撤销：

[0021] 所述的被授权用户被请求撤销授权，系统判断所述的被授权用户与所述的数据之间是否存在访问路径，如果不存在，拒绝所述的请求；如果存在，系统判断所述的权限控制节点是否存在该用户信息，如果有：

[0022] 如果所述的数据只对应一个镜像，则直接从云端删除该数据镜像，并清空其权限控制节点信息；

[0023] 如果所述的数据只对应一个镜像，但是只针对部分用户执行授权撤销，则首先清空权限控制节点中的对应用户信息，其次对当前镜像重新生成公私钥对，并生成以该公私钥对为目标的重加密密钥，以及加密处理其私钥，最后更新权限控制节点中的用户授权信息为加密后的镜像私钥；

[0024] 如果所述的数据对应于多个镜像，且需要对所有镜像执行授权撤销，则删除对应镜像，并更新权限控制节点中的被授权用户信息；

[0025] 如果所述的数据对应于多个镜像，但是执行多镜像中部分用户的授权撤销，则针对相关的每一个镜像，首先清空权限控制节点中的对应用户信息，其次对当前镜像重新生成公私钥对，并生成以该公私钥对为目标的重加密密钥，以及加密处理其私钥，最后更新权限控制节点中的用户授权信息为加密后的镜像私钥；

[0026] 否则，拒绝所述的请求；

[0027] 步骤 5：数据更新，当对云端的某些所述的数据进行更新后，

[0028] 如果是对其访问授权保持不变，则不执行任何操作；

[0029] 如果需要撤销某些所述的授权，则按照所述的步骤 4 中的授权撤销执行；

[0030] 如果需要新增访问授权，则按照所述的步骤 2 中的数据授权执行。

[0031] 作为优选，步骤 1 中所述的构造相应的权限控制节点层，所述的每个节点被赋予被授权用户的相关信息。

[0032] 作为优选，随着系统的运行，以及权限的变更，可以对所述的权限控制节点进行动态更新。

[0033] 本发明与现有的授权访问控制相比具有以下优点：

[0034] 1. 通过数据镜像实现无副本的数据多次授权，轻量级数据共享；

[0035] 2. 按照需求灵活数据授权。用户不但可以根据组划分，还可以根据组内不同的角色再次进行划分，并且可以针对临时用户进行短暂性授权；

[0036] 3. 便捷的授权撤销。根据需求，通过调整数据镜像以及权限控制节点值，来执行访问权限的回收。

附图说明

[0037] 图 1 ：本发明的支持轻量级、细粒度的数据访问控制层次结构图。

[0038] 图 2 ：本发明的数据上传及初始化流程图。

[0039] 图 3 ：本发明具体实施例的细粒度权限控制节点数据结构图。

[0040] 图 4 ：本发明的数据授权流程图。

[0041] 图 5 ：本发明的数据读取流程图。

[0042] 图 6 ：本发明的授权撤销流程图。

具体实施方式

[0043] 下面结合具体的实例和附图对本发明做进一步说明。

[0044] 本发明提供了一种云环境下轻量级的细粒度访问控制方法，包括以下步骤：

[0045] 步骤 1 ：上传数据及初始化，其实现方式为：

[0046] 一方面，数据拥有者通过自己的公钥本地加密所要上传的明文数据，得到密文数据；然后将密文数据上传至云端；

[0047] 另一方面，根据数据拥有者的访问控制需求，构造相应的权限控制节点层，每个节点被赋予被授权用户的相关信息，随着系统的运行，以及权限的变更，可以对权限控制节点进行动态更新；

[0048] 步骤 2 ：数据的授权，其实现方式包括如下步骤：

[0049] 步骤 2.1 ：确定授权数据，针对每个所要授权的数据，生成一个对应的数据镜像，如果数据需要被多次授权，则相应生成多个镜像，数据拥有者为每个镜像生成一个公私钥对；

[0050] 步骤 2.2 ：计算数据与其镜像之间的代理重加密密钥，存储在云端；

[0051] 步骤 2.3 ：计算会话密钥，对于每一个被授权用户，数据拥有者通过自己的私钥与授权用户的公钥及公开参数构造出一个会话密钥，用户指一个单用户或者一个用户群组；

[0052] 步骤 2.4 ：通过会话密钥对镜像的私钥进行加密，将加密后的密文存储于权限控制节点，同时更新权限控制节点中授权用户信息；

[0053] 步骤 3 ：数据的读取：

[0054] 用户请求读取某个数据，系统首先根据权限控制节点判断当前用户是否拥有该数据访问权限，如果有，则将用户请求的数据经过镜像的重加密以及其权限控制节点中加密的镜像私钥发送给用户，用户在客户端则通过第一轮解密获得镜像私钥，然后利用该私钥进行第二轮解密并最终获得明文数据；否则，拒绝用户请求；

[0055] 步骤 4 ：授权撤销：

[0056] 被授权用户被请求撤销授权，系统判断被授权用户与数据之间是否存在访问路

径，如果不存在，拒绝请求；如果存在，系统判断权限控制节点是否存在该用户信息，如果有：

[0057] 如果数据只对应一个镜像，则直接从云端删除该数据镜像，并清空其权限控制节点信息；

[0058] 如果数据只对应一个镜像，但是只针对部分用户执行授权撤销，则首先清空权限控制节点中的对应用户信息，其次对当前镜像重新生成公私钥对，并生成以该公私钥对为目标的重加密密钥，以及加密处理其私钥，最后更新权限控制节点中的用户授权信息为加密后的镜像私钥；

[0059] 如果数据对应于多个镜像，且需要对所有镜像执行授权撤销，则删除对应镜像，并更新权限控制节点中的被授权用户信息；

[0060] 如果数据对应于多个镜像，但是执行多镜像中部分用户的授权撤销，则针对相关的每一个镜像，首先清空权限控制节点中的对应用户信息，其次对当前镜像重新生成公私钥对，并生成以该公私钥对为目标的重加密密钥，以及加密处理其私钥，最后更新权限控制节点中的用户授权信息为加密后的镜像私钥；

[0061] 否则，拒绝请求；

[0062] 步骤 5：数据更新，当对云端的某些数据进行更新后，

[0063] 如果是对其访问授权保持不变，则不执行任何操作；

[0064] 如果需要撤销某些授权，则按照步骤 4 中的授权撤销执行；

[0065] 如果需要新增访问授权，则按照步骤 2 中的数据授权执行。

[0066] 请见图 1，为本发明的支持轻量级、细粒度的数据访问控制层次结构图，包括物理层、数据镜像层、权限控制层、用户层。

[0067] 请见图2，为数据提交及初始化过程流程图，数据拥有者（data owner）首先在本地通过自己的公钥对数据 f1 ～ f6 进行加密，具体而言，这里采用非对称的 RSA 加密算法对数据进行加密。首先根据系统的安全性参数 λ 确定系统参数 SP:={p,q,n}，这里 n=pq，并且 p,q 是满足系统安全性参数 λ 的两个大素数。当用户注册时，系统为每个用户分配一对公私钥 (ek,dk)=(<e,n>,<d,n>)，这里 e 是$Z^*_{\emptyset(n)}$中随机选出，其中$\emptyset(n)=(p-1)(q-1)$，然后根据 e 计算相应的$d=e^{-1} mod\ \emptyset(n)$.其中 <e,n> 为公钥，<d,n> 为私钥。假设明文为 m，则加密后的密文为 c ＝ m^e • mod • n。

[0068] 然后将加密后的数据上传至云端。按照系统需求，对访问权限进行划分，即构造图 1 中的权限控制层中的权限控制节点。请见图 3，为权限控制节点具体数据结构图，记录相关用户授权信息。随着系统的运行，以及权限的变更等需求，可以对权限控制节点进行动态更新，借此实现细粒度的数据访问控制。

[0069] 请见图 4，为数据授权过程流程图，这里以将数据 f1 授权给 U1,U3 为例。首先数据拥有者确定将要授权的数据为 f1，系统为 f1 生成相应镜像，数据拥有者为每个镜像生成一个公私钥对 (ek1,dk1)，待生成完毕，图 1 中数据镜像层中对应 f1 的镜像生成完毕，然后计算 f1 到其对应镜像的代理重加密密钥，具体计算如下：这里设用户密钥对为 (eu_i, du_i) =(<eu_i, n>,<du_i,n>)，对应的镜像密钥对为 (eu_j, du_j) =(<eu_j,n>,<du_j,n>)，那么相应的重加密密钥为$rk_{i\to j}=e_j/e_i\ mod\ \emptyset(n)$。并将相应的重加密密钥 rk_{i-j} 上传至云端存储在镜像节

点中。然后分别根据授权用户 U1, U3 的公钥 eu_1, eu_2, 作为会话密钥, 利用会话密钥加密镜像私钥 du_j, 具体计算如下 : $c_{eu_1} = (du_j)^{eu_1} \bmod n$, $c_{eu_3} = (du_j)^{eu_3} \bmod n$. 并将加密后的私钥 c_{eu_1} , c_{eu_3} 存储在相应的权限控制节点中。

[0070] 请见图 5, 为数据读取过程流程图, 首先用户 U1 发出访问数据 f1 请求, 系统判断 U1 与 f1 之间是否存在访问路径, 如果存在, 则去查找当前路径上的权限控制节点, 判断 U1 是否具有 f1 的授权访问。如果具有, 则云端利用镜像中重加密密钥对数据 f1 进行重加密得到 F1, 连同权限控制节点中 U1 相应的加密后的私钥 c_{eu_1} 发送给用户 U1。用户 U1 利用自己的私钥首先解密 f1 镜像对应私钥的密文 c_{eu_1}, 然后利用解密出来的镜像私钥 du_j 解密数据 F1 得到数据明文 f1。否则, 拒绝访问。

[0071] 请见图 6, 为授权撤销具体过程流程图, 参照图 1 如果我们撤销 f1 对 U1 的授权, 我们首先清空路径 f1 到 U1 路径上的权限控制节点中 U1 的相关授权信息, 然后为 f1 的镜像生成新的公私钥对, 并以其计算新的代理重加密密钥, 最后将镜像的新私钥通过数据拥有者和授权用户计算的会话密钥加密, 更新权限控制节点中其他用户的信息。至此, 针对 U1 的授权撤销完毕, 并且对其他用户没有任何影响。如果撤销 f7 针对 U8 的授权, 我们将 f7 对应的镜像删除, 并清空该路径上权限控制节点中 U8 相应授权信息。

[0072] 以上内容是结合最佳实施方案对本发明所做的进一步详细说明, 不能认定本发明的具体实施只限于这些说明。本领域的技术人员应该理解, 在不脱离由所附权利要求书限定的情况下, 可以在细节上进行各种修改, 都应当视为属于本发明的保护范围。

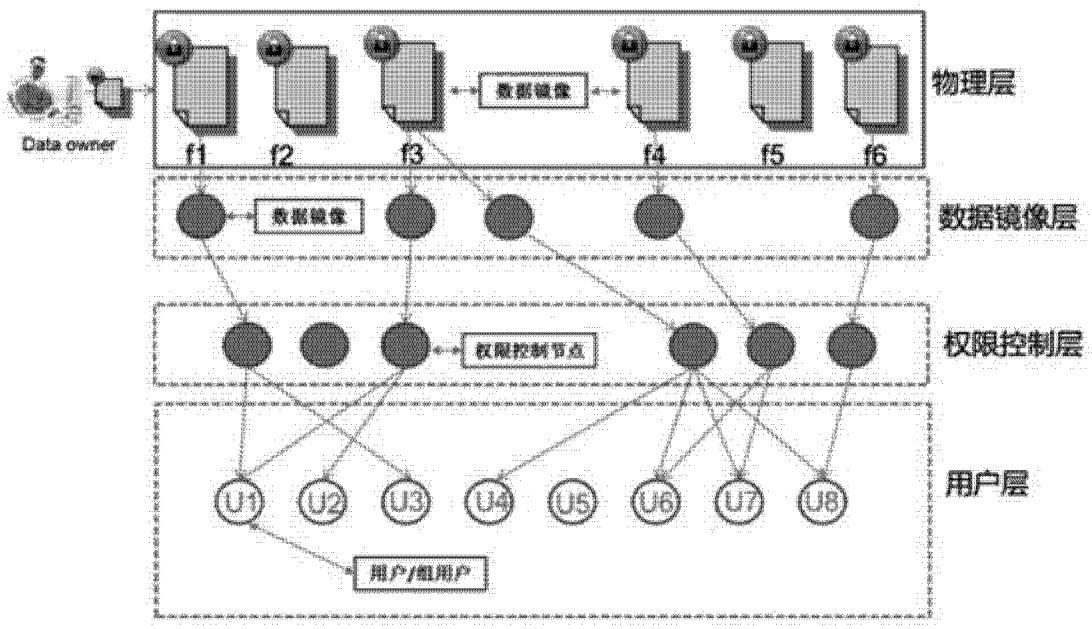

Data owner
f1
f2
f3
数据镜像
f4
f5
f6
物理层
数据镜像
数据镜像层
权限控制节点
权限控制层
U1
U2
U3
U4
U5
U6
U7
U8
用户/组用户
用户层

图 1

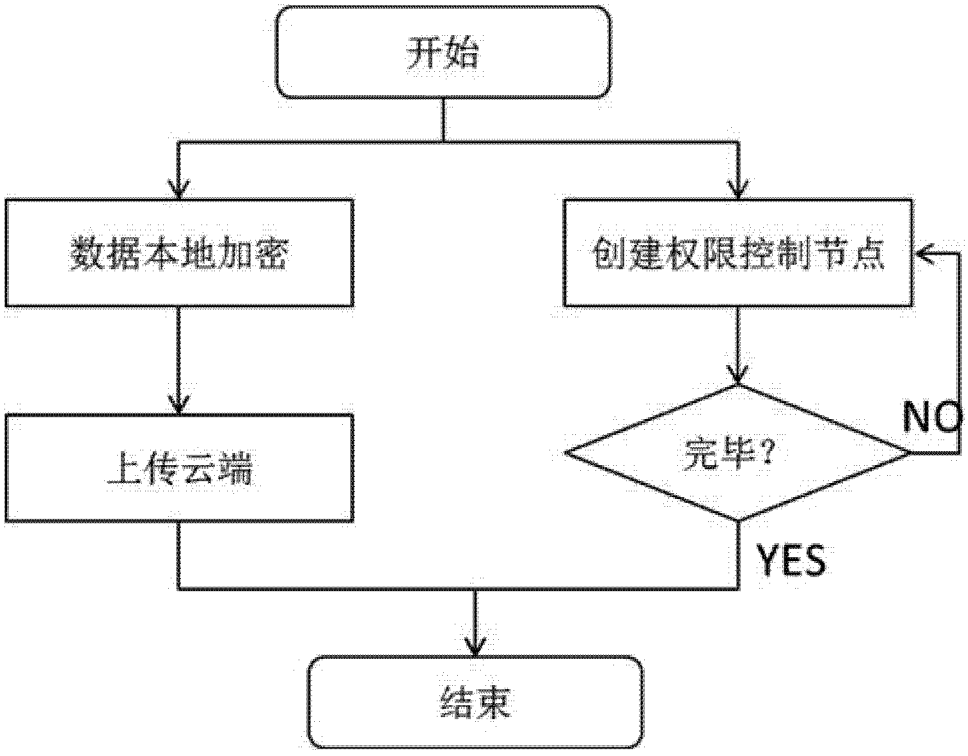

开始
数据本地加密
创建权限控制节点
上传云端
完毕?
NO
YES
结束

图 2

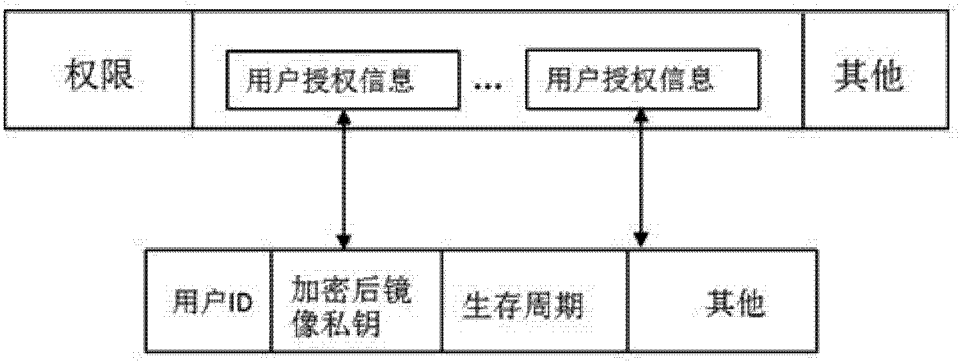

权限
用户授权信息
...
用户授权信息
其他
用户ID
加密后镜像私钥
生存周期
其他

图 3

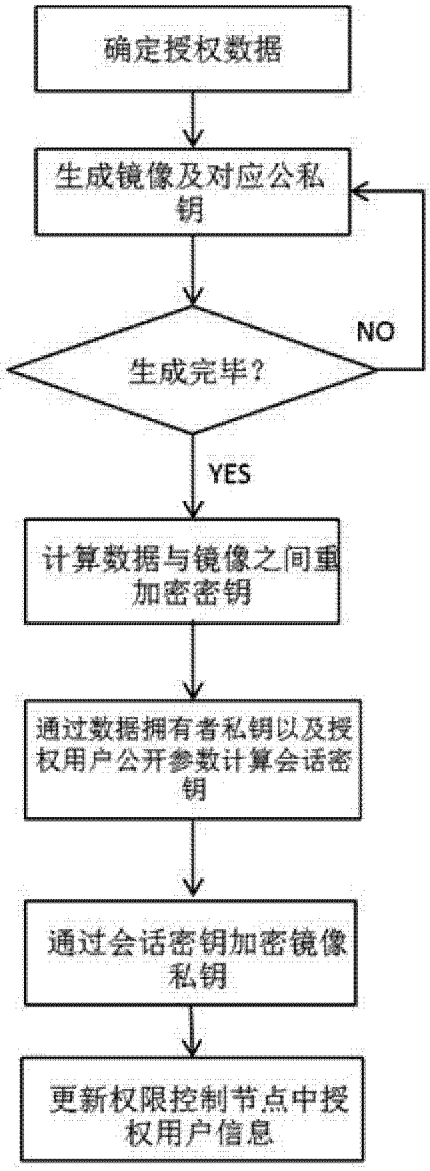

确定授权数据
生成镜像及对应公私钥
生成完毕?
NO
YES
计算数据与镜像之间重加密密钥
通过数据拥有者私钥以及授权用户公开参数计算会话密钥
通过会话密钥加密镜像私钥
更新权限控制节点中授权用户信息

图 4

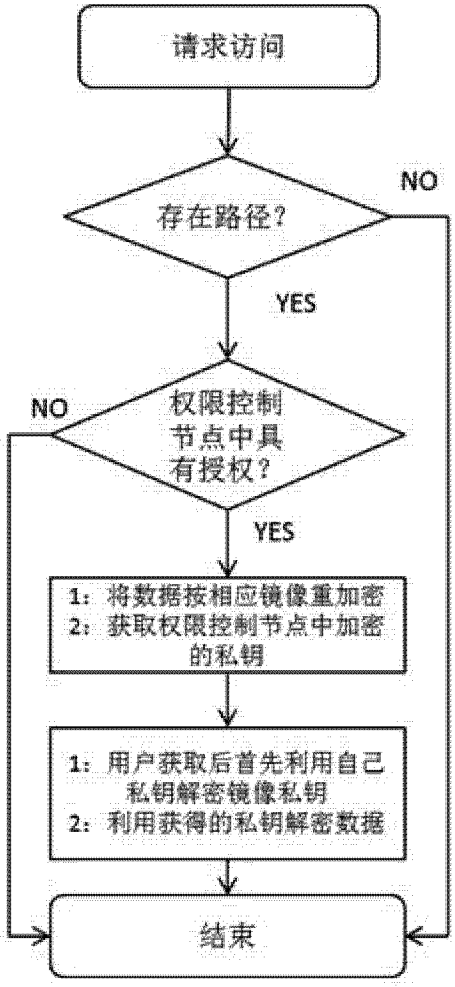

请求访问
存在路径?
NO
YES
权限控制节点中具有授权?
NO
YES
1：将数据按相应镜像重加密
2：获取权限控制节点中加密的私钥
1：用户获取后首先利用自己私钥解密镜像私钥
2：利用获得的私钥解密数据
结束

图 5

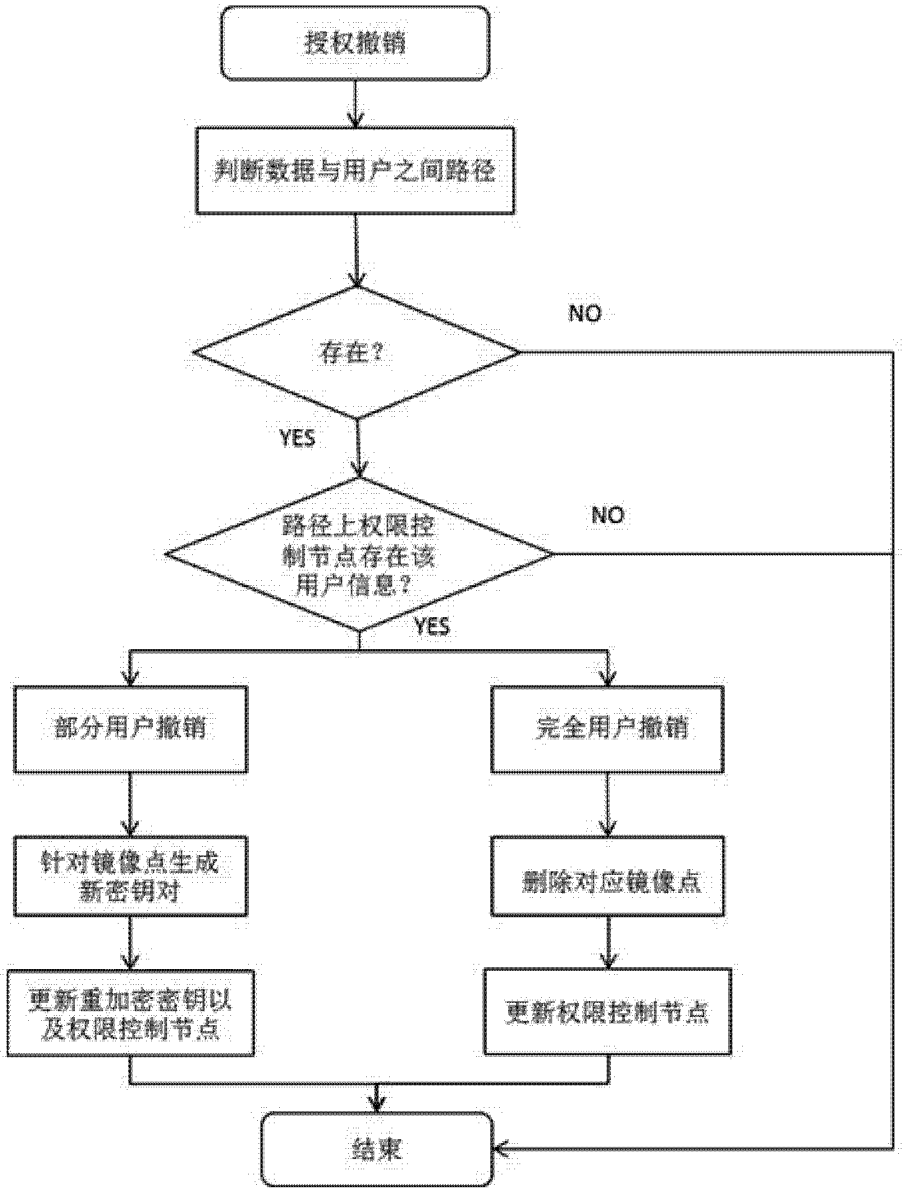

授权撤销
判断数据与用户之间路径
存在？
NO
YES
路径上权限控制节点存在该用户信息？
NO
YES
部分用户撤销
完全用户撤销
针对镜像点生成新密钥对
删除对应镜像点
更新重加密密钥以及权限控制节点
更新权限控制节点
结束

图 6