(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 107743133 A
(43)申请公布日 2018.02.27

(21)申请号 201711233877.5

(22)申请日 2017.11.30

(71)申请人 中国石油大学(北京)
地址 102249 北京市昌平区府学路18号

(72)发明人 范永开 刘声乐 林晓东 白建蓉 赵冠群

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 李辉 刘飞

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

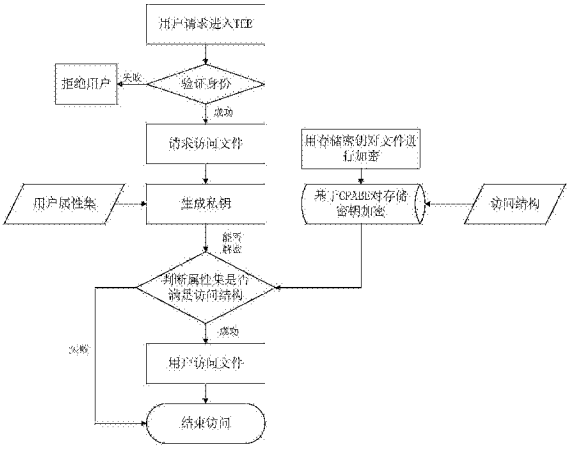
权利要求书3页 说明书10页 附图3页

(54)发明名称

移动终端及其基于可信安全环境的访问控制方法和系统

(57)摘要

本申请实施例提供了一种移动终端及其基于可信安全环境的访问控制方法和系统，该方法包括：预先在可信安全环境下，用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥；当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份；当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥；在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件；向所述客户端返回所述私密文件。本申请实施例可提高移动终端的信息安全。



CN 107743133 A

1.一种基于可信安全环境的访问控制方法,其特征在于,包括:

预先在可信安全环境下,用存储密钥加密私密文件,并用CPABE及所述私密文件的访问结构加密所述存储密钥;

当收到普通执行环境下的客户端发起的可信安全环境访问请求时,验证所述客户端的身份;

当收到所述客户端在通过身份验证后发起的文件访问请求时,根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥;

在所述客户端属性集满足对应文件密文的访问结构时,根据所述CPABE私钥获得对应私密文件;

向所述客户端返回所述私密文件。

2.如权利要求1所述的基于可信安全环境的访问控制方法,其特征在于,所述用存储密钥加密私密文件,并用CPABE及所述私密文件的访问结构加密所述存储密钥,包括:

在可信安全环境下生成存储密钥;

基于所述存储密钥加密私密文件,获得文件密文;

基于CPABE生成可信安全环境下的公钥及主密钥;

根据所述可信安全环境下的公钥和所述私密文件的访问结构,并利用CPABE的加密功能对所述存储密钥进行加密。

3.如权利要求1所述的基于可信安全环境的访问控制方法,其特征在于,所述当收到普通执行环境下的客户端发起的可信安全环境访问请求时,验证所述客户端的身份,包括:

在收到普通执行环境下的客户端发起的授权请求时,对所述授权请求进行PIN码认证;

接收所述客户端在通过PIN码认证后发送的随机密钥密文;

利用可信安全环境下的私钥解密所述随机密钥密文,获得带有RSA签名的随机密钥;所述带有RSA签名的随机密钥是由所述客户端,基于自身私钥对自身生成的随机密钥进行RSA签名而得到的;

利用所述客户端的公钥对所述带有RSA签名的随机密钥进行验证,获得所述客户端的随机密钥;

针对所述客户端生成一次性会话密钥,利用HMAC算法将所述客户端的随机密钥作为密钥,并将所述一次性会话密钥作为消息,生成消息摘要;

向所述客户端返回所述消息摘要,以便于所述客户端利用自身的随机密钥验证所述消息摘要中携带的一次性会话密钥的完整性,从而获得所述一次性会话密钥。

4.如权利要求1所述的基于可信安全环境的访问控制方法,其特征在于,所述当收到所述客户端在通过身份验证后发起的文件访问请求时,根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥,包括:

当收到所述客户端在通过身份验证后发起的文件访问请求时,对所述文件访问请求进行验证;

在确认所述文件访问请求通过验证后,根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥。

5.如权利要求4所述的基于可信安全环境的访问控制方法,其特征在于,所述对所述文件访问请求进行验证,包括:

根据所述文件访问请求中的一次性会话密钥所携带的ID，确认此前针对所述客户端生成的一次性会话密钥是否存在；

如果存在，则根据所述一次性会话密钥解析所述文件访问请求，并验证解析后的文件访问请求的合法性和完整性。

6.如权利要求1所述的基于可信安全环境的访问控制方法，其特征在于，所述在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件，包括：

在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥解密对应文件密文的存储密钥密文，获得存储秘钥；

利用获得的存储秘钥解密对应文件密文，获得对应私密文件。

7.一种基于可信安全环境的访问控制系统，其特征在于，所述基于可信安全环境的访问控制系统包括位于可信安全环境下的认证服务器及文件管理器；

所述认证服务器，用于当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份；

所述文件管理器，用于预先在可信安全环境下，用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥；当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥；在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件；并向所述客户端返回所述私密文件。

8.如权利要求7所述的基于可信安全环境的访问控制系统，其特征在于，所述用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥，包括：

在可信安全环境下生成存储密钥；

基于所述存储密钥加密私密文件，获得文件密文；

基于CPABE生成可信安全环境下的公钥及主密钥；

根据所述可信安全环境下的公钥和所述私密文件的访问结构，并利用CPABE的加密功能对所述存储密钥进行加密。

9.如权利要求7所述的基于可信安全环境的访问控制系统，其特征在于，所述当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份，包括：

在收到普通执行环境下的客户端发起的授权请求时，对所述授权请求进行PIN码认证；

接收所述客户端在通过PIN码认证后发送的随机密钥密文；

利用可信安全环境下的私钥解密所述随机密钥密文，获得带有RSA签名的随机密钥；所述带有RSA签名的随机密钥是由所述客户端，基于自身私钥对自身生成的随机密钥进行RSA签名而得到的；

利用所述客户端的公钥对所述带有RSA签名的随机密钥进行验证，获得所述客户端的随机密钥；

针对所述客户端生成一次性会话密钥，利用HMAC算法将所述客户端的随机密钥作为密钥，并将所述一次性会话密钥作为消息，生成消息摘要；

向所述客户端返回所述消息摘要，以便于所述客户端利用自身的随机密钥验证所述消息摘要中携带的一次性会话密钥的完整性，从而获得所述一次性会话密钥。

10.如权利要求7所述的基于可信安全环境的访问控制系统，其特征在于，所述当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥，包括：

当收到所述客户端在通过身份验证后发起的文件访问请求时，对所述文件访问请求进行验证；

在确认所述文件访问请求通过验证后，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥。

11.如权利要求10所述的基于可信安全环境的访问控制系统，其特征在于，所述对所述文件访问请求进行验证，包括：

根据所述文件访问请求中的一次性会话密钥所携带的ID，确认此前针对所述客户端生成的一次性会话密钥是否存在；

如果存在，则根据所述一次性会话密钥解析所述文件访问请求，并验证解析后的文件访问请求的合法性和完整性。

12.如权利要求7所述的基于可信安全环境的访问控制系统，其特征在于，所述在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件，包括：

在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥解密对应文件密文的存储密钥密文，获得存储秘钥；

利用获得的存储秘钥解密对应文件密文，获得对应私密文件。

13.一种移动终端，其特征在于，所述移动终端配置有基于可信安全环境的访问控制系统，所述基于可信安全环境的访问控制系统包括位于可信安全环境下的认证服务器及文件管理器；

所述认证服务器，用于当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份；

所述文件管理器，用于预先在可信安全环境下，用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥；当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥；在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件；并向所述客户端返回所述私密文件。

移动终端及其基于可信安全环境的访问控制方法和系统

技术领域

[0001] 本申请涉及移动终端的访问控制技术领域，尤其是涉及一种移动终端及其基于可信安全环境的访问控制方法和系统。

背景技术

[0002] 随着互联网和移动通信技术的快速发展，诸如智能手机等移动终端的应用越来越普及。以智能手机为例，目前的智能手机不仅可以通话，拍照、听音乐、玩游戏、网购、电子支付，而且可以实现包括导航定位、信息处理、指纹扫描、身份证扫描、二维码扫描等丰富的功能。相应的，随着移动终端的功能及应用越来越多，其面临的信息安全也越来越受到人们的广泛关注。

[0003] 针对移动终端所面临的信息安全问题，目前已经出现一种TrustZone技术，其旨在提供安全框架，以使移动终端能够抵御众多特定威胁。TrustZone技术提供了两个相互物理隔离的环境：普通环境(NW，Normal World)和安全环境(SW，Secure World)。NW致力于满足普通应用的需求，在普通执行环境(REE，Rich Execution Environment)中运行；而SW则用于提供安全服务及执行安全的操作，在可信执行环境(TEE，Trusted Execution Environment)中运行。

[0004] 然而，在NW下客户端访问私密文件仍会存在安全隐患，例如非安全客户端窃取信息，黑客攻击，文件篡改等等。因此，在TrustZone提供的安全框架下，目前亟需一种新的访问控制机制来应对NW下存在的安全隐患问题。

发明内容

[0005] 本申请实施例的目的在于提供一种移动终端及其基于可信安全环境的访问控制方法和系统，以提高移动终端的信息安全。

[0006] 为达到上述目的，一方面，本申请实施例提供了一种基于可信安全环境的访问控制方法，包括：

[0007] 预先在可信安全环境下，用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥；

[0008] 当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份；

[0009] 当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥；

[0010] 在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件；

[0011] 向所述客户端返回所述私密文件。

[0012] 优选的，所述用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥，包括：

[0013] 在可信安全环境下生成存储密钥；

[0014] 基于所述存储密钥加密私密文件，获得文件密文；

[0015] 基于CPABE生成可信安全环境下的公钥及主密钥；

[0016] 根据所述可信安全环境下的公钥和所述私密文件的访问结构，并利用CPABE的加密功能对所述存储密钥进行加密。

[0017] 优选的，所述当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份，包括：

[0018] 在收到普通执行环境下的客户端发起的授权请求时，对所述授权请求进行PIN码认证；

[0019] 接收所述客户端在通过PIN码认证后发送的随机密钥密文；

[0020] 利用可信安全环境下的私钥解密所述随机密钥密文，获得带有RSA签名的随机密钥；所述带有RSA签名的随机密钥是由所述客户端，基于自身私钥对自身生成的随机密钥进行RSA签名而得到的；

[0021] 利用所述客户端的公钥对所述带有RSA签名的随机密钥进行验证，获得所述客户端的随机密钥；

[0022] 针对所述客户端生成一次性会话密钥，利用HMAC算法将所述客户端的随机密钥作为密钥，并将所述一次性会话密钥作为消息，生成消息摘要；

[0023] 向所述客户端返回所述消息摘要，以便于所述客户端利用自身的随机密钥验证所述消息摘要中携带的一次性会话密钥的完整性，从而获得所述一次性会话密钥。

[0024] 优选的，所述当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥，包括：

[0025] 当收到所述客户端在通过身份验证后发起的文件访问请求时，对所述文件访问请求进行验证；

[0026] 在确认所述文件访问请求通过验证后，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥。

[0027] 优选的，所述对所述文件访问请求进行验证，包括：

[0028] 根据所述文件访问请求中的一次性会话密钥所携带的ID，确认此前针对所述客户端生成的一次性会话密钥是否存在；

[0029] 如果存在，则根据所述一次性会话密钥解析所述文件访问请求，并验证解析后的文件访问请求的合法性和完整性。

[0030] 优选的，所述在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件，包括：

[0031] 在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥解密对应文件密文的存储密钥密文，获得存储秘钥；

[0032] 利用获得的存储秘钥解密对应文件密文，获得对应私密文件。

[0033] 另一方面，本申请实施例还提供了一种基于可信安全环境的访问控制系统，所述基于可信安全环境的访问控制系统包括位于可信安全环境下的认证服务器及文件管理器；

[0034] 所述认证服务器，用于当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份；

[0035] 所述文件管理器，用于预先在可信安全环境下，用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥；当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥；在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件；并向所述客户端返回所述私密文件。

[0036] 优选的，所述用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥，包括：

[0037] 在可信安全环境下生成存储密钥；

[0038] 基于所述存储密钥加密私密文件，获得文件密文；

[0039] 基于CPABE生成可信安全环境下的公钥及主密钥；

[0040] 根据所述可信安全环境下的公钥和所述私密文件的访问结构，并利用CPABE的加密功能对所述存储密钥进行加密。

[0041] 优选的，所述当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份，包括：

[0042] 在收到普通执行环境下的客户端发起的授权请求时，对所述授权请求进行PIN码认证；

[0043] 接收所述客户端在通过PIN码认证后发送的随机密钥密文；

[0044] 利用可信安全环境下的私钥解密所述随机密钥密文，获得带有RSA签名的随机密钥；所述带有RSA签名的随机密钥是由所述客户端，基于自身私钥对自身生成的随机密钥进行RSA签名而得到的；

[0045] 利用所述客户端的公钥对所述带有RSA签名的随机密钥进行验证，获得所述客户端的随机密钥；

[0046] 针对所述客户端生成一次性会话密钥，利用HMAC算法将所述客户端的随机密钥作为密钥，并将所述一次性会话密钥作为消息，生成消息摘要；

[0047] 向所述客户端返回所述消息摘要，以便于所述客户端利用自身的随机密钥验证所述消息摘要中携带的一次性会话密钥的完整性，从而获得所述一次性会话密钥。

[0048] 优选的，所述当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥，包括：

[0049] 当收到所述客户端在通过身份验证后发起的文件访问请求时，对所述文件访问请求进行验证；

[0050] 在确认所述文件访问请求通过验证后，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥。

[0051] 优选的，所述对所述文件访问请求进行验证，包括：

[0052] 根据所述文件访问请求中的一次性会话密钥所携带的ID，确认此前针对所述客户端生成的一次性会话密钥是否存在；

[0053] 如果存在，则根据所述一次性会话密钥解析所述文件访问请求，并验证解析后的文件访问请求的合法性和完整性。

[0054] 优选的，所述在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件，包括：

[0055] 在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥解密对应文件密文的存储密钥密文，获得存储秘钥；

[0056] 利用获得的存储秘钥解密对应文件密文，获得对应私密文件。

[0057] 另一方面，本申请实施例还提供了一种移动终端，所述移动终端配置有基于可信安全环境的访问控制系统，所述基于可信安全环境的访问控制系统包括位于可信安全环境下的认证服务器及文件管理器；

[0058] 所述认证服务器，用于当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份；

[0059] 所述文件管理器，用于预先在可信安全环境下，用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥；当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥；在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件；并向所述客户端返回所述私密文件。

[0060] 由以上本申请实施例提供的技术方案可见，本申请实施例预先在可信安全环境下，用存储密钥加密私密文件，并用CPABE及私密文件的访问结构加密存储密钥；当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证客户端的身份；当收到客户端在通过身份验证后发起的文件访问请求时，根据文件访问请求中携带的客户端属性集生成客户端的CPABE私钥；当客户端属性集满足对应文件密文的访问结构时，根据CPABE私钥获得对应私密文件，并向客户端返回私密文件。由此可见，本申请实施例在TEE中存储相关密钥以及进行加解密和授权认证，而且整个过程的安全性既有CPABE算法的保护，也有ARM TrustZone架构的TEE提供的物理隔离，从而极大地提高了移动终端的信息安全。

附图说明

[0061] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。在附图中：

[0062] 图1是本申请一实施方式的基于可信安全环境的访问控制系统安全框架示意图；

[0063] 图2是本申请一实施方式的基于可信安全环境的访问控制系统内部的基本层次结构示意图；

[0064] 图3是本申请一实施方式的基于可信安全环境的访问控制方法的流程图；

[0065] 图4是本申请一实施方式的客户端与认证服务器的通信示意图；

[0066] 图5是本申请一实施方式的客户端与文件管理器的通信示意图。

具体实施方式

[0067] 为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护

的范围。

[0068] 本申请实施方式提出了一种基于密文策略的属性加密算法(CPABE,ciphertext-policy attribute-based encryption)和TEE的基于可信安全环境的访问控制系统,在TEE中存储相关密钥以及进行加解密和授权认证,而且整个过程的安全性既有哈希运算的消息认证码(Hash-based Message Authentication Code,HMAC),CPABE,RSA等算法的保护,也有ARM TrustZone架构的TEE提供的物理隔离,是软硬件结合的基于可信安全环境的访问控制系统。

[0069] 图1示出了本申请实施方式的基于可信安全环境的访问控制系统的一种基于ARM TrustZone的安全框架,自ARM v6开始引入ARM架构规范,支持用户自主开发设计特定的安全系统,目前可应用于大部分嵌入式设备中。它将硬件和软件资源划分为两个执行环境,安全环境和普通环境。其中:

[0070] 普通环境包含命令调用器组件(Command caller)和客户端接口组件(TEE_CLIENT_API)。其中,命令调用器组件可用于直接与客户端进行交互,接收客户端发送给安全环境的服务请求,并将该请求解析发送给客户端接口组件。客户端接口组件用于实现命令的发送,发送请求与安全环境进行交互,并等待安全环境的数据返回。

[0071] 安全环境中包含密钥处理器(Key function)、加密处理器(Crypt function)和TEE内部接口(TEE_INNER_API)。其中,密钥处理器用于提取密钥,并将密钥用于RSA、HMAC算法等中。加密处理器使用密钥为数据提供密码学算法支持,保证数据的安全性和完整性,其中所述密码学算法可以包括对称和非对称加密解密,签名验证以及消息验证摘要算法等。TEE内部接口用于处理普通环境中发送来的请求和数据,并将这个信息交由相应的可信应用。REE_Driver组件和TEE_Driver组件分别对应用于处理两个执行环境的切换和响应,利用共享内存,保证两个执行环境可以正常通信,这种通信遵守TrustZone API调用规范;监控器用于控制底层硬件,完成两个执行环境的切换。

[0072] 图2示出了本申请实施方式的基于可信安全环境的访问控制系统内部的基本层次结构。本申请实施方式中,按照可信执行环境的相关要求,构建了两个可信应用:认证服务器和文件管理器,用于与普通环境中的客户端进行交互,以完成普通环境中的不同请求。所述认证服务器可用于当收到普通执行环境下的客户端发起的可信安全环境访问请求时,验证所述客户端的身份;所述文件管理器可用于预先在可信安全环境下,用存储密钥加密私密文件,并用CPABE及所述私密文件的访问结构加密所述存储密钥;当收到所述客户端在通过身份验证后发起的文件访问请求时,根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥;在所述客户端属性集满足对应文件密文的访问结构(访问结构是指定的各个客户端的安全属性集合)时,根据所述CPABE私钥获得对应私密文件;并向所述客户端返回所述私密文件。操作层为了给不同的可信应用提供不同功能的API接口,例如认证服务端需要授权验证以及生成密钥包的功能;基础内核是用来为特殊的扩展功能模块提供基础系统功能的,如内存管理和任务管理等。

[0073] 本申请实施方式的基于可信安全环境的访问控制系统可配置于移动终端中,从而使得所述移动终端的安全性能得以大幅提升。其中,所述移动终端包括但不限于智能手机、笔记本、平板电脑、POS机等。

[0074] 在介绍了以上基于可信安全环境的访问控制系统的基础上,结合图3所示,在本申

请实施方式的基于可信安全环境的访问控制方法可以包括以下步骤：

[0075] 首先，预先在可信安全环境下，用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥；

[0076] 其次，当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份；

[0077] 然后，当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥；

[0078] 其次，在所述客户端属性集满足对应文件密文的访问结构时，根据所述CPABE私钥获得对应私密文件。而当所述客户端属性集不满足对应文件密文的访问结构时，向所述客户端返回失败声明。

[0079] 最后，向所述客户端返回所述私密文件。

[0080] 本申请实施方式中，所述用存储密钥加密私密文件，并用CPABE及所述私密文件的访问结构加密所述存储密钥可以包括以下步骤：

[0081] 1)、在可信安全环境下生成存储密钥。存储密钥sk(storage key)可用来加密私密文件，生成方式为sk←KGF("TA identity")。存储密钥存放在可信端，不可导出，也不能存放在移动设备的非易失性存储器上，这样保证了加密私密文件的安全性。

[0082] 2)、基于所述存储密钥加密私密文件，获得文件密文；即$ENC_{sk}(file)$。私密文件加密在SW的可信服务中来进行，利用存储密钥sk(storage key)实现加密函数Encrypt()，加密封装后的文件可以存储在移动设备的公共非易失性存储器中。

[0083] 以私密文件m为例，利用k_hmac和k_enc对其进行封装，其步骤为：

[0084] message←Encrypt_package("HMAC+ENC",k_hmac,k_enc,m)

[0085] 具体过称为：$message = ENC_{k\_enc}(m) || HMAC_{k\_mac}(ENC_{k\_enc}(m))$。

[0086] 其中，$HMAC_k(m)$函数表示使用密钥k对敏感数据m计算消息验证码，$Sign_k(m)$函数表示使用密钥k对数据进行签名，$ENC_k(m)$函数表示使用密钥k对敏感数据m进行加密，根据k的类型采取相应的对称与非对称加密，||表示数据的连接操作。我们利用$HMAC_k(m)$和$ENC_k(m)$来保证敏感数据的安全性和完整性。

[0087] 3)、基于CPABE生成可信安全环境下的公钥及主密钥；即利用CPABE算法生成公钥(PK)和主密钥(MK)：(PK,MK)＝CPABE-Setup()。

[0088] 4)、根据所述可信安全环境下的公钥和所述私密文件的访问结构，并利用CPABE的加密功能对所述存储密钥进行加密；即使用CPABE算法的加密功能加密存储密钥：$CT_{(sk)}$＝CPABE-Encrypt(PK,sk,T)；其中，T为所述私密文件的访问结构。

[0089] 默认应用服务提供商为安全可信的，在移动终端下载合法的普通应用时，应用服务提供商一般为其选取好了唯一标识符，例如使用PKI技术，利用密钥生成器中的密钥生成函数KGF，生成临时RSA公私密钥对，将私钥保存在客户端中，同时将公钥连同个人信息打包，利用SW中的公钥tpk进行加密并发送，SW利用私钥tsk解密后通过对比打包好的个人信息，生成新的证书和公私密钥对(cpk,csk)，使用客户端的临时公钥进行加密并发送，客户端得到消息后，利用临时私钥解密，装载新的证书和客户端密钥对(cpk,csk)。通常情况下，不使用客户端密钥对，只有涉及到需要与可信端交互访问敏感数据时才会使用，生成方式为：(cpk,csk)←KGF("unique identity")。

[0090] 结合图4所示，本申请实施方式中，所述当收到普通执行环境下的客户端发起的可信安全环境访问请求时，验证所述客户端的身份可以包括以下步骤：

[0091] 1)、在收到普通执行环境下的客户端发起的授权请求时，对所述授权请求进行PIN码认证。在发起的授权请求前，所述客户端可调用授权申请API：Authorize()函数，生成授权请求消息m_authorize:m_authorize←Authorize(csk,k_r)，并将消息发送给认证服务器，具体实现如下：

[0092] (1)加载客户端中的私钥csk以及认证服务器的公钥tpk；

[0093] (2)调用签名函数生成签名：$\beta \leftarrow Sign_{csk}(k_r)$；

[0094] (3)调用加密函数生成最终的授权请求消息：$m\_authorize \leftarrow Enc_{tpk}(k_r,\beta)$。

[0095] 2)、接收所述客户端在通过PIN码认证后发送的随机密钥密文。在发送随机密钥密文之前，在NW中，所述客户端可利用密钥生成函数，生成保护消息完整性的随机密钥k_r，生成方式为$k_r \leftarrow KGF("session_key",r)$，其中r为随机生成数；然后依次对所述随机密钥$k_r$进行RSA签名和RSA加密，从而生成随机密钥密文。

[0096] 而如果所述客户端未通过PIN码认证，则终止所述客户端与SW间的交互。

[0097] 3)、利用可信安全环境下的私钥解密所述随机密钥密文，获得带有RSA签名的随机密钥；所述带有RSA签名的随机密钥是由所述客户端，基于自身私钥对自身生成的随机密钥进行RSA签名而得到的。

[0098] 4)、利用所述客户端的公钥对所述带有RSA签名的随机密钥进行验证，获得所述客户端的随机密钥。

[0099] 5)、针对所述客户端生成一次性会话密钥，利用HMAC算法将所述客户端的随机密钥作为密钥，并将所述一次性会话密钥作为消息，生成消息摘要。其中，在基于可信安全环境的访问控制系统内部，认证服务器为客户端和文件服务器生成一次性会话密钥(ID,k_enc,k_hmac)，其中ID是该密钥包的唯一标识；k_hmac用来保护会话的完整性，k_enc用来保护会话的机密性。在生成一次性会话密钥后，认证服务器通过安全信道将一次性会话密钥连同user信息一同发送给文件服务器。

[0100] 6)、向所述客户端返回所述消息摘要，以便于所述客户端利用自身的随机密钥验证所述消息摘要中携带的一次性会话密钥的完整性，从而获得所述一次性会话密钥。至此完成了对所述客户端的授权验证。

[0101] 本申请实施方式中，所述当收到所述客户端在通过身份验证后发起的文件访问请求时，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥可以包括：

[0102] 当收到所述客户端在通过身份验证后发起的文件访问请求时，对所述文件访问请求进行验证；

[0103] 在确认所述文件访问请求通过验证后，根据所述文件访问请求中携带的客户端属性集生成所述客户端的CPABE私钥。

[0104] 本申请实施方式中，所述对所述文件访问请求进行验证可以包括以下步骤：

[0105] 首先，根据所述文件访问请求中的一次性会话密钥所携带的ID，确认此前针对所述客户端生成的一次性会话密钥是否存在；

[0106] 如果存在，则根据所述一次性会话密钥解析所述文件访问请求，并验证解析后的

文件访问请求的合法性和完整性;如果不存在,则拒绝所述文件访问请求。

[0107] 结合图5所示,本申请实施方式中,所述在所述客户端属性集满足对应文件密文的访问结构时,根据所述CPABE私钥获得对应私密文件可以包括以下步骤:

[0108] 首先,在所述客户端属性集满足对应文件密文的访问结构时,根据所述CPABE私钥解密对应文件密文的存储密钥密文,获得存储秘钥;

[0109] 然后,利用获得的存储秘钥解密对应文件密文,获得对应私密文件。

[0110] 当然,所述客户端在通过身份验证后发起的文件访问请求之前,可利用所述一次性会话密钥对所述文件访问请求和自身属性集S进行加密。

[0111] 下面分析本申请实施方式的基于可信安全环境的访问控制系统的安全性

[0112] 在本申请实施方式的基于可信安全环境的访问控制系统下,文件访问者需要根据授权验证所获得的密钥信息对加密的文件进行相应的访问操作。在实际应用中,可能会有不同的安全漏洞出现,下面考虑了不同的敌手攻击:

[0113] 1)、敌手具有一定的物理接入能力,可以直接窃取移动设备中非易失性存储器的数据;

[0114] 2)、敌手试图盗用或伪装客户端和用户的合法身份进行授权申请;

[0115] 3)、敌手试图窃取,伪造或篡改客户端与可信端的一次性会话密钥,直接申请私密文件的访问;

[0116] 4)、敌手试图利用一次性会话密钥进行重放攻击;

[0117] 5)、敌手直接攻击客户端,意图通过攻击获取文件内容;

[0118] 针对以上提出的敌手攻击,对本申请实施方式的基于可信安全环境的访问控制系统的安全性进行如下分析:

[0119] 1)、数据的机密性和安全性:

[0120] 首先,私密文件经过SW加密处理后,受保护的存放在存储器中,而加密的密钥不会泄露在SW之外,因此数据存储在非易失性存储器中是安全的。

[0121] 其次,可信端和客户端之间通信的数据也受到完整性和安全性保护,如若敌手攻击移动设备的NW,由于SW传入NW的敏感数据都是经过加密封装的,所以敌手无法通过SW的可信服务接口获取有价值的数据;

[0122] 2)、授权信息安全性:

[0123] 首先,客户端和用户要通过PIN码验证,证明其合法性;

[0124] 其次,假设客户端使用认证服务端的公钥加密相关数据后,生成授权申请消息m_authorize,由于缺乏私钥,敌手无法解密m_authorize,同时也无法生成具有认证服务端签名的并且由随机密钥保护完整性的授权相应消息m_answer,这样敌手也就无法向客户端发送伪造的一次性会话密钥,类似的,敌手也无法直接与文件管理端进行通信。

[0125] 3)、防止重放攻击:

[0126] 本文中的一次性会话密钥仅能使用一次,使用过后即被删除,所以如果敌手想要利用一次性会话密钥来达到欺骗系统的目的是不能实现的。并且密钥包的发送和接收都需要私钥进行封装,敌手无法得到私钥,就无法进行重放攻击。

[0127] 虽然上文描述的过程流程包括以特定顺序出现的多个操作,但是,应当清楚了解,这些过程可以包括更多或更少的操作,这些操作可以顺序执行或并行执行(例如使用并行

处理器或多线程环境)。

[0128] 为了描述的方便,描述以上装置时以功能分为各种单元分别描述。当然,在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0129] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0130] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0131] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0132] 在一个典型的配置中,计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0133] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0134] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[0135] 还需要说明的是,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、商品或者设备不仅包括那些要素,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、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0136] 本领域技术人员应明白,本申请的实施例可提供为方法、系统或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形

式。

[0137] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0138] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0139] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

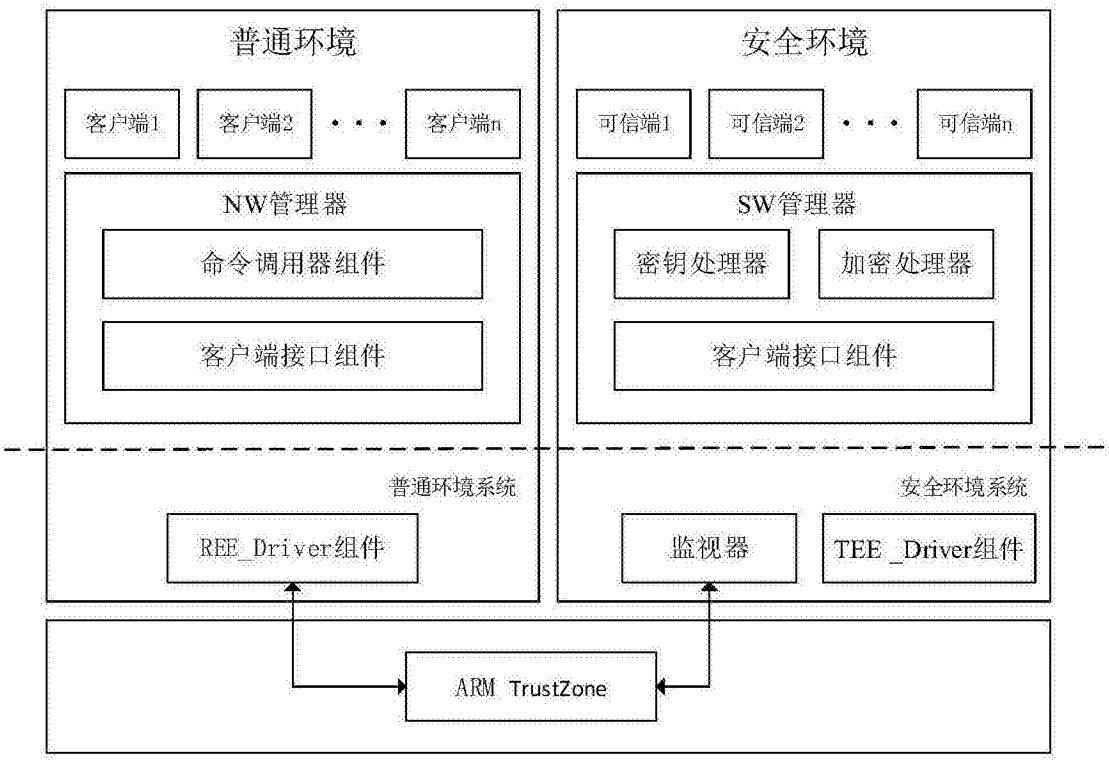

普通环境
客户端1
客户端2
客户端n
NW管理器
命令调用器组件
客户端接口组件
普通环境系统
REE_Driver组件
安全环境
可信端1
可信端2
可信端n
SW管理器
密钥处理器
加密处理器
客户端接口组件
安全环境系统
监视器
TEE _Driver组件
ARM TrustZone

图1

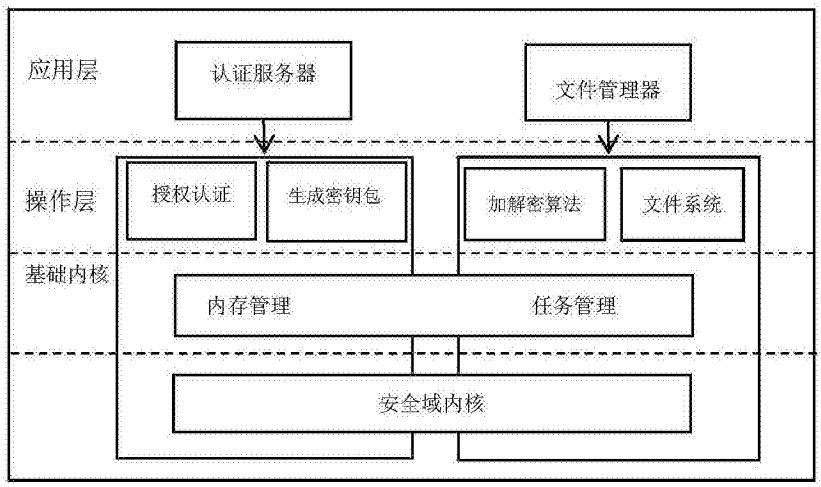

应用层
认证服务器
文件管理器
操作层
授权认证
生成密钥包
加解密算法
文件系统
基础内核
内存管理
任务管理
安全域内核

图2

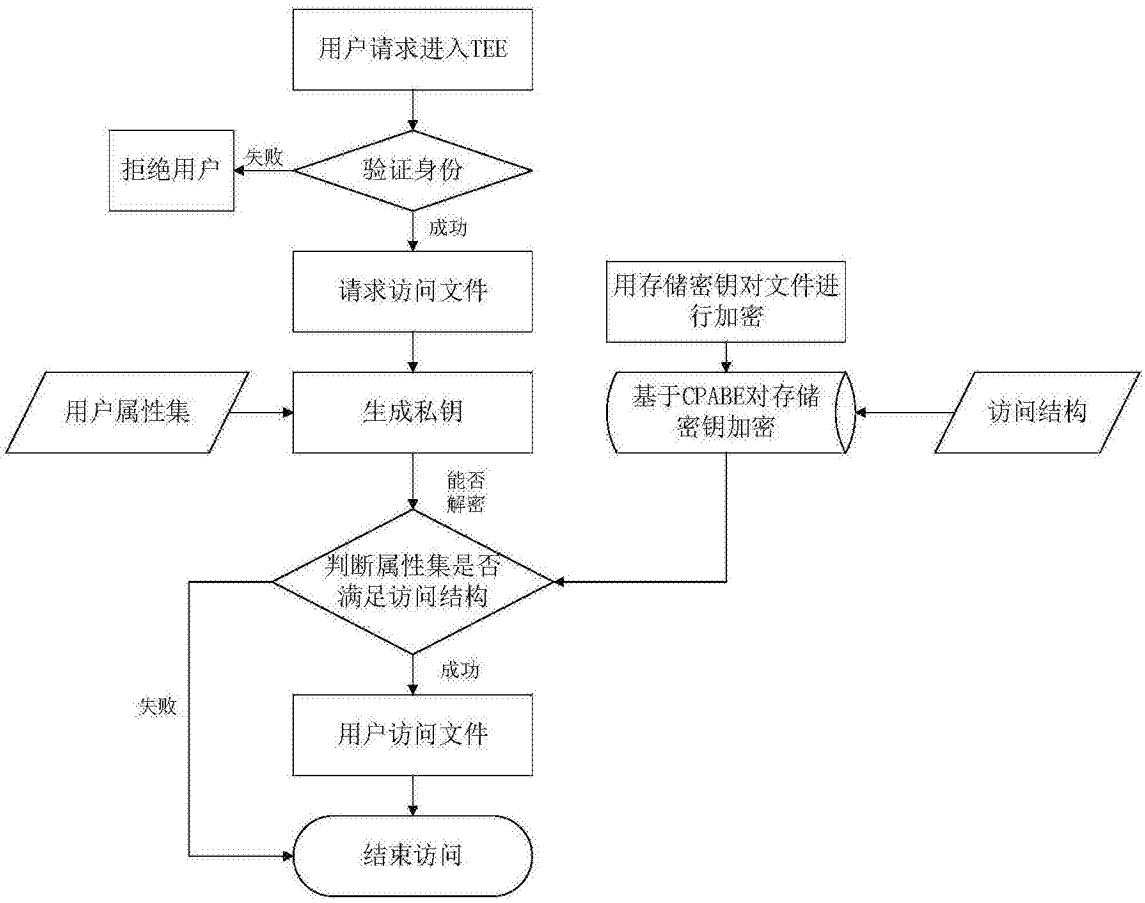

用户请求进入TEE
验证身份
失败
拒绝用户
成功
请求访问文件
用存储密钥对文件进行加密
用户属性集
生成私钥
基于CPABE对存储密钥加密
访问结构
能否解密
判断属性集是否满足访问结构
成功
失败
用户访问文件
结束访问

图3

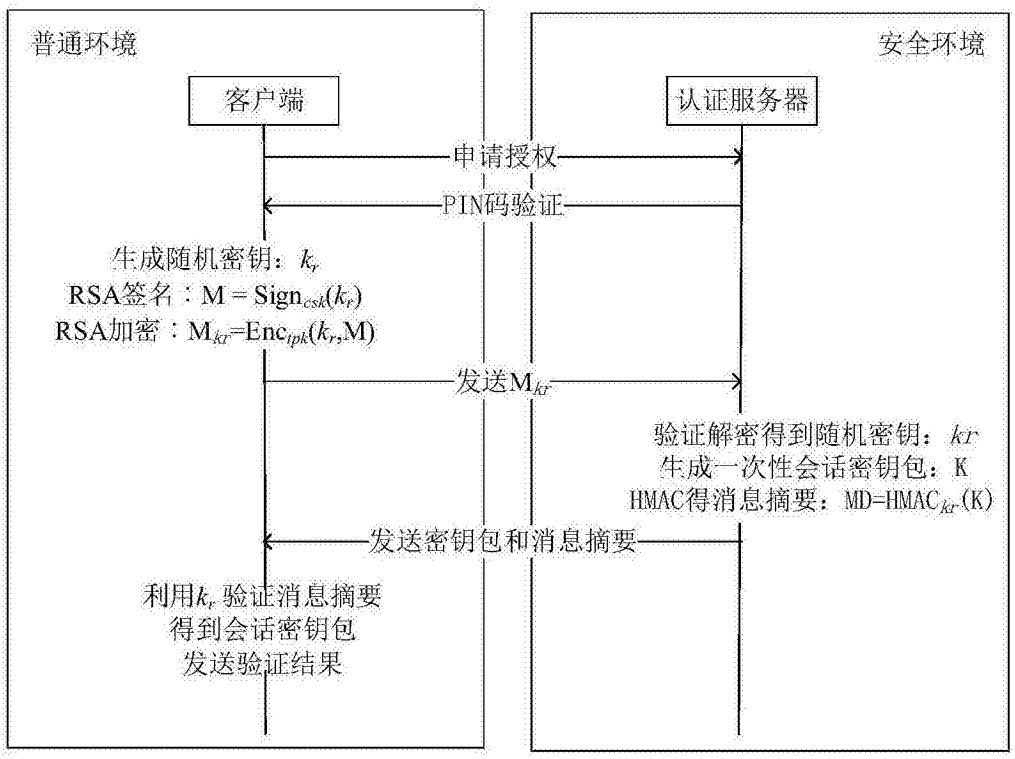

普通环境
安全环境
客户端
认证服务器
申请授权
PIN码验证
生成随机密钥：k_r
RSA签名：M = $Sign_{csk}(k_r)$
RSA加密：M_{kr}=$Enc_{tpk}(k_r,M)$
发送M_{kr}
验证解密得到随机密钥：kr
生成一次性会话密钥包：K
HMAC得消息摘要：MD=$HMAC_{kr}$(K)
发送密钥包和消息摘要
利用k_r验证消息摘要
得到会话密钥包
发送验证结果

图4

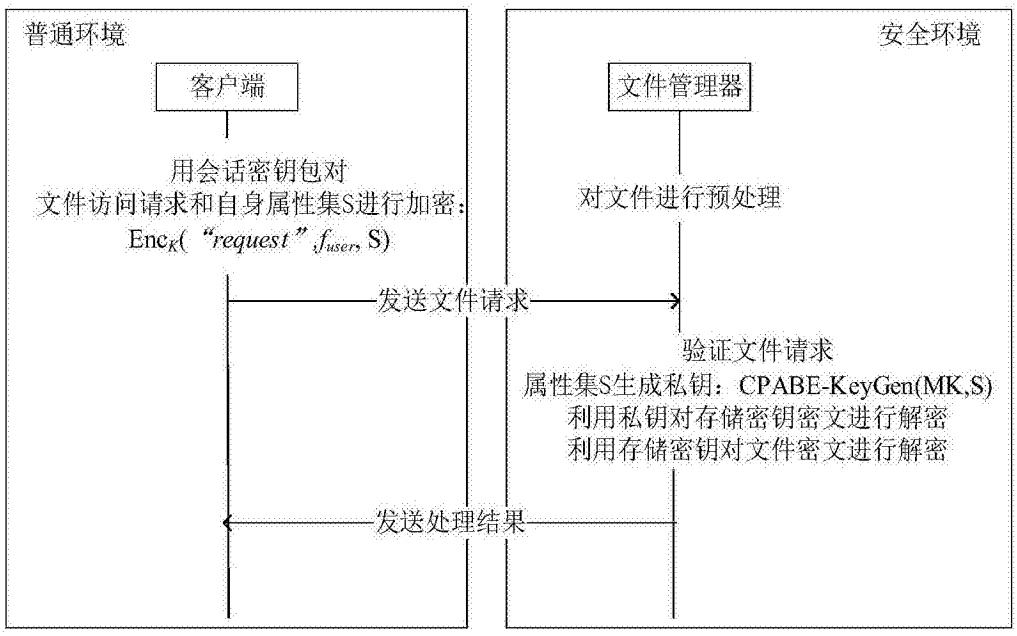

普通环境
安全环境
客户端
文件管理器
用会话密钥包对
文件访问请求和自身属性集S进行加密：
Enc_K(“request” f_{user}, S)
对文件进行预处理
发送文件请求
验证文件请求
属性集S生成私钥：CPABE-KeyGen(MK,S)
利用私钥对存储密钥密文进行解密
利用存储密钥对文件密文进行解密
发送处理结果

图5