



(12) 发明专利申请

(10) 申请公布号 CN 103051664 A

(43) 申请公布日 2013. 04. 17

(21) 申请号 201210288853. 0

(22) 申请日 2012. 08. 14

(71) 申请人 深圳市朗科科技股份有限公司

地址 518057 广东省深圳市高新区南区高新
南六道 10 号朗科大厦 16、18、19 层

(72) 发明人 刘一宁 边涛 骆林 卢赛文

(74) 专利代理机构 深圳市深佳知识产权代理事
务所 (普通合伙) 44285

代理人 唐华明

(51) Int. Cl.

H04L 29/08 (2006. 01)

H04L 29/06 (2006. 01)

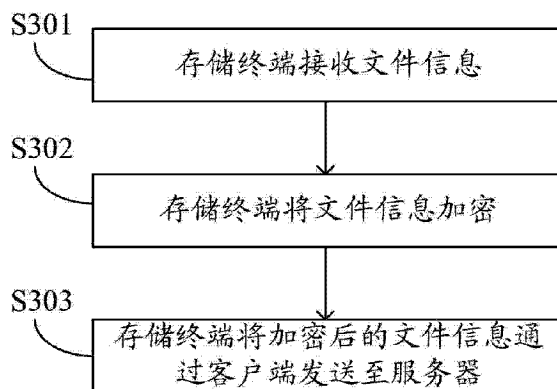
权利要求书 3 页 说明书 22 页 附图 18 页

(54) 发明名称

一种云存储系统的文件管理方法、装置及该云存储系统

(57) 摘要

本发明实施例提供一种云存储系统的文件管理方法及其装置,所述云存储系统包括存储终端、客户端和服务端,所述方法包括:所述存储终端接收文件信息;所述存储终端对所述文件信息加密;所述存储终端将加密后的所述文件信息通过所述客户端发送至所述服务器。根据本发明实施例提供的云存储系统中的文件管理方法及其装置,采用存储终端对文件信息进行加密后再将加密后的文件信息从客户端发送至服务器。本发明实施例提供的云存储系统的文件管理方法及其装置能够避免服务器或者传输通道遭受攻击造成文件数据泄露的情况发生,从而能够提高云存储系统的安全性。



1. 一种云存储系统的文件管理方法,所述云存储系统包括存储终端、客户端和服务端,其特征在于,所述方法包括:

所述存储终端接收文件信息;

所述存储终端将所述文件信息加密;

所述存储终端将加密后的所述文件信息通过所述客户端发送至所述服务器。

2. 根据权利要求1所述的文件管理方法,其特征在于,所述方法还包括:

所述存储终端生成操作指令;

所述存储终端将所述操作指令加密;

所述存储终端将加密后的所述操作指令通过所述客户端转发至所述服务器。

3. 根据权利要求1所述的文件管理方法,其特征在于,所述方法还包括:

所述存储终端接收所述客户端转发的由所述服务器加密并发送的处理结果信息;

所述存储终端将所述处理结果信息解密。

4. 根据权利要求1所述的文件管理方法,其特征在于,所述存储终端包括主控单元、安全单元,所述存储终端接收文件信息,包括:

所述主控单元接收文件信息;

所述存储终端对所述文件信息加密,包括:

所述主控单元将所述文件信息发送至所述安全单元;

所述安全单元对所述文件信息加密,并将加密后的所述文件信息返回至所述主控单元。

5. 根据权利要求1所述的文件管理方法,其特征在于,所述存储终端接收文件信息前,还包括:

所述存储终端验证用户输入的身份识别码是否正确,如果是,执行所述存储终端接收文件信息的步骤。

6. 根据权利要求5所述的文件管理方法,其特征在于,所述存储终端包括主控单元、安全单元和智能单元,所述存储终端验证用户输入的身份识别码,包括:

所述主控单元根据用户输入的所述身份识别码得到所述身份识别码对应的第一触摸点坐标值,并将所述第一触摸点坐标值发送至所述安全单元;

所述安全单元对所述第一触摸点坐标值进行译码及加密运算,得到加密后的身份识别码,并将所述加密后的身份识别码发送至智能单元;

所述智能单元对所述加密后的身份识别码进行验证。

7. 根据权利要求1所述的文件管理方法,其特征在于,所述存储终端接收文件信息前,还包括:

所述服务器验证用户的网络账户信息是否正确,如果是,执行所述存储终端接收文件信息的步骤。

8. 根据权利要求1所述的文件管理方法,其特征在于,所述存储终端接收文件信息前,还包括:

所述存储终端和所述服务器进行交叉认证,如果认证通过,执行所述存储终端接收文件信息的步骤。

9. 根据权利要求1所述的文件管理方法,其特征在于,所述方法还包括:所述客户端控

制所述存储终端完成所述接收、加密及发送操作。

10. 根据权利要求 9 所述的文件管理方法,其特征在于,所述客户端控制所述存储终端完成所述接收、加密及发送操作,包括:

所述存储终端获取本地的桌面信息,并对所述桌面信息进行视频编码以获得视频数据;

所述存储终端向所述客户端发送所述视频数据;

所述客户端解析所述视频数据,以显示所述存储终端的桌面信息;

所述客户端向所述存储终端发送鼠标键盘命令;

所述存储终端依照所述鼠标键盘命令做出响应,包括接收、加密及发送操作响应。

11. 根据权利要求 10 所述的文件管理方法,其特征在于,所述客户端通过 USB 接口与所述存储终端通信,

所述存储终端获取本地的桌面信息,包括:

所述存储终端接收所述客户端发送的控制命令并依据所述控制命令获取本地的桌面信息;

所述存储终端向所述客户端发送所述视频数据,包括:

所述存储终端接收所述客户端发送的所述视频数据的获取请求并依照所述获取请求向所述客户端发送所述视频数据。

12. 一种云存储系统的存储终端,所述云存储系统包括存储终端、客户端和服务端,其特征在于,所述存储终端包括:

第一接收单元,用于接收文件信息;

第一加密单元,用于将所述文件信息加密;

第一发送单元,用于将加密后的所述文件信息通过所述客户端发送至所述服务器。

13. 根据权利要求 12 所述的存储终端,其特征在于,还包括:

生成单元,用于生成操作指令;

第二加密单元,用于将所述操作指令加密;

第二发送单元,用于将加密后的所述操作指令通过所述客户端转发至所述服务器。

14. 根据权利要求 12 所述的存储终端,其特征在于,还包括:

第二接收单元,用于接收所述客户端转发的由所述服务器加密并发送的处理结果信息;

解密单元,用于将所述处理结果信息解密。

15. 根据权利要求 12 所述的存储终端,其特征在于,所述存储终端还包括主控单元、安全单元:

所述主控单元,用于接收文件信息,并将所述文件信息发送至所述安全单元;

所述安全单元,用于对所述文件信息加密,并将加密后的所述文件信息返回至所述主控单元。

16. 根据权利要求 12 所述的存储终端,其特征在于,所述存储终端还包括:

第一验证单元,用于验证用户输入的身份识别码是否正确。

17. 根据权利要求 16 所述的存储终端,其特征在于,所述存储终端还包括主控单元、安全单元和智能单元,

所述主控单元,用于根据用户输入的所述身份识别码得到所述身份识别码对应的第一触摸点坐标值,并将所述第一触摸点坐标值发送至所述安全单元;

所述安全单元,用于对所述第一触摸点坐标值进行译码及加密运算,得到加密后的身份识别码,并将所述加密后的身份识别码发送至所述智能单元;

所述智能单元,用于对所述加密后的身份识别码进行验证。

18. 根据权利要求 12 所述的存储终端,其特征在于,还包括:

认证单元,用于对所述存储终端和所述服务器进行交叉认证。

19. 根据权利要求 12 所述的存储终端,其特征在于,所述存储终端还包括:

获取单元,用于获取本地的桌面信息;

编码单元,用于对所述桌面信息进行视频编码以获得视频数据;

第三发送单元,用于向所述客户端发送所述视频数据;

第三接收单元,用于接收所述客户端发送的鼠标键盘命令;

响应单元,用于依照所述第三接收单元接收的所述鼠标键盘命令做出响应,包括接收、加密及发送操作响应。

20. 根据权利要求 19 所述的存储终端,其特征在于,所述存储终端还包括:

第四接收单元,用于接收所述客户端发送的控制命令;

第五接收单元,用于接收所述客户端发送的所述视频数据的获取请求。

21. 一种云存储系统,所述云存储系统包括如权 12-20 任一项所述的存储终端、客户端和服务器,其特征在于,

所述存储终端用于接收文件信息,将所述文件信息加密,并将加密后的所述文件信息发送至所述客户端;

所述客户端用于接收所述存储终端发送的加密后的所述文件信息,并将加密后的所述文件信息发送至所述服务器;

所述服务器用于接收所述客户端发送的加密后的所述文件信息。

22. 根据权利要求 21 所述的云存储系统,其特征在于,

所述服务器还用于处理加密后的所述文件信息,产生处理结果信息并所述处理结果信息加密,并将加密后的所述处理结果信息发送至所述客户端;

所述客户端还用于接收所述服务器发送的加密后的所述处理结果信息,并将所述加密后的处理结果信息发送至所述存储终端;

所述存储终端还用于接收所述客户端发送的加密后的所述处理结果信息,并将所述加密后的所述处理结果信息解密。

一种云存储系统的文件管理方法、装置及该云存储系统

技术领域

[0001] 本发明涉及云存储技术领域，具体涉及一种云存储系统的文件管理方法及其装置。

背景技术

[0002] 随着 IT 行业的普及和发展，信息量出现爆炸式增长，用户对于信息的获取提出了更高的要求，在这一需求下，云存储技术应运而生。该技术将大部分数据迁移到云存储上，所有的升级维护任务都由云存储服务提供商来完成，能够节约企业存储系统管理员的压力；另外，云存储技术具有强大的可扩展性，可以方便地在原有基础上扩展服务空间，满足信息量急剧增长的需求。

[0003] 目前，云存储技术已经得到了广泛应用，如图 1 所示，为现有技术中传统的云存储系统的结构示意图，云存储系统通常由客户端 101、网络、防火墙 102、开关 103 以及服务器 104 等几部分组成，其中服务器 104 通常采用分布式文件系统的架构。

[0004] 但是，传统的云存储系统都是基于账户密码形式的，在这种方式中，通过任何可以连接网络的设备都可以访问到用户云存储空间中的数据。这样，如果被病毒木马入侵则会泄露用户账户密码甚至云存储空间中的数据，或者，一旦服务器遭受攻击用户数据就会泄露，服务器加密的文件同样会被破解。这导致云存储的安全性较低。

发明内容

[0005] 有鉴于此，本发明的目的在于提供一种安全性较高的云存储系统的文件管理方法、装置及该云存储系统。

[0006] 为实现上述目的，本发明的一个实施例提供一种云存储系统的文件管理方法，所述云存储系统包括存储终端、客户端和服务端，所述方法包括：

[0007] 所述存储终端接收文件信息；

[0008] 所述存储终端将所述文件信息加密；

[0009] 所述存储终端将加密后的所述文件信息通过所述客户端发送至所述服务器。

[0010] 优选地，所述方法还包括：

[0011] 所述存储终端生成操作指令；

[0012] 所述存储终端将所述操作指令加密；

[0013] 所述存储终端将加密后的所述操作指令通过所述客户端转发至所述服务器。

[0014] 优选地，所述方法还包括：

[0015] 所述存储终端接收所述客户端转发的由所述服务器加密并发送的处理结果信息；

[0016] 所述存储终端将所述处理结果信息解密。

[0017] 优选地，所述存储终端包括主控单元、安全单元，所述存储终端接收文件信息，包括：

- [0018] 所述主控单元接收文件信息；
- [0019] 所述存储终端对所述文件信息加密，包括：
- [0020] 所述主控单元将所述文件信息发送至所述安全单元；
- [0021] 所述安全单元对所述文件信息加密，并将加密后的所述文件信息返回至所述主控单元。
- [0022] 优选地，所述存储终端接收文件信息前，还包括：
- [0023] 所述存储终端验证用户输入的身份识别码是否正确，如果是，执行所述存储终端接收文件信息的步骤。
- [0024] 优选地，所述存储终端包括主控单元、安全单元和智能单元，所述存储终端验证用户输入的身份识别码，包括：
- [0025] 所述主控单元根据用户输入的所述身份识别码得到所述身份识别码对应的第一触摸点坐标值，并将所述第一触摸点坐标值发送至所述安全单元；
- [0026] 所述安全单元对所述第一触摸点坐标值进行译码及加密运算，得到加密后的身份识别码，并将所述加密后的身份识别码发送至智能单元；
- [0027] 所述智能单元对所述加密后的身份识别码进行验证。
- [0028] 优选地，所述存储终端接收文件信息前，还包括：
- [0029] 所述服务器验证用户的网络账户信息是否正确，如果是，执行所述存储终端接收文件信息的步骤。
- [0030] 优选地，所述存储终端接收文件信息前，还包括：
- [0031] 所述存储终端和所述服务器进行交叉认证，如果认证通过，执行所述存储终端接收文件信息的步骤。
- [0032] 优选地，所述方法还包括：所述客户端控制所述存储终端完成所述接收、加密及发送操作。
- [0033] 优选地，所述客户端控制所述存储终端完成所述接收、加密及发送操作，包括：
- [0034] 所述存储终端获取本地的桌面信息，并对所述桌面信息进行视频编码以获得视频数据；
- [0035] 所述存储终端向所述客户端发送所述视频数据；
- [0036] 所述客户端解析所述视频数据，以显示所述存储终端的桌面信息；
- [0037] 所述客户端向所述存储终端发送鼠标键盘命令；
- [0038] 所述存储终端依照所述鼠标键盘命令做出响应，包括接收、加密及发送操作响应。
- [0039] 优选地，所述客户端通过 USB 接口与所述存储终端通信，
- [0040] 所述存储终端获取本地的桌面信息，包括：
- [0041] 所述存储终端接收所述客户端发送的控制命令并依据所述控制命令获取本地的桌面信息；
- [0042] 所述存储终端向所述客户端发送所述视频数据，包括：
- [0043] 所述存储终端接收所述客户端发送的所述视频数据的获取请求并依照所述获取请求向所述客户端发送所述视频数据。
- [0044] 另外，本发明实施例还提供一种云存储系统的存储终端，所述云存储系统包括存储终端、客户端和服务器，所述存储终端包括：

- [0045] 第一接收单元,用于接收文件信息;
- [0046] 第一加密单元,用于将所述文件信息加密;
- [0047] 第一发送单元,用于将加密后的所述文件信息通过所述客户端发送至所述服务器。
- [0048] 优选地,还包括:
- [0049] 生成单元,用于生成操作指令;
- [0050] 第二加密单元,用于将所述操作指令加密;
- [0051] 第二发送单元,用于将加密后的所述操作指令通过所述客户端转发至所述服务器。
- [0052] 优选地,还包括:
- [0053] 第二接收单元,用于接收所述客户端转发的由所述服务器加密并发送的处理结果信息;
- [0054] 解密单元,用于将所述处理结果信息解密。
- [0055] 优选地,所述存储终端还包括主控单元、安全单元:
- [0056] 所述主控单元,用于接收文件信息,并将所述文件信息发送至所述安全单元;
- [0057] 所述安全单元,用于对所述文件信息加密,并将加密后的所述文件信息返回至所述主控单元。
- [0058] 优选地,所述存储终端还包括:
- [0059] 第一验证单元,用于验证用户输入的身份识别码是否正确。
- [0060] 优选地,所述存储终端还包括主控单元、安全单元和智能单元,
- [0061] 所述主控单元,用于根据用户输入的所述身份识别码得到所述身份识别码对应的第一触摸点坐标值,并将所述第一触摸点坐标值发送至所述安全单元;
- [0062] 所述安全单元,用于对所述第一触摸点坐标值进行译码及加密运算,得到加密后的身份识别码,并将所述加密后的身份识别码发送至所述智能单元;
- [0063] 所述智能单元,用于对所述加密后的身份识别码进行验证。
- [0064] 优选地,还包括:
- [0065] 认证单元,用于对所述存储终端和所述服务器进行交叉认证。
- [0066] 优选地,所述存储终端还包括:
- [0067] 获取单元,用于获取本地的桌面信息;
- [0068] 编码单元,用于对所述桌面信息进行视频编码以获得视频数据;
- [0069] 第三发送单元,用于向所述客户端发送所述视频数据;
- [0070] 第三接收单元,用于接收所述客户端发送的鼠标键盘命令;
- [0071] 响应单元,用于依照所述第三接收单元接收的所述鼠标键盘命令做出响应,包括接收、加密及发送操作响应。
- [0072] 优选地,所述存储终端还包括:
- [0073] 第四接收单元,用于接收所述客户端发送的控制命令;
- [0074] 第五接收单元,用于接收所述客户端发送的所述视频数据的获取请求。
- [0075] 此外,本发明实施例还提供一种云存储系统,所述云存储系统采用本发明实施例中的存储终端、客户端和服务端,

[0076] 所述存储终端用于接收文件信息,将所述文件信息加密,并将加密后的所述文件信息发送至所述客户端;

[0077] 所述客户端用于接收所述存储终端发送的加密后的所述文件信息,并将加密后的所述文件信息发送至所述服务器;

[0078] 所述服务器用于接收所述客户端发送的加密后的所述文件信息。

[0079] 优选地,

[0080] 所述服务器还用于处理加密后的所述文件信息,产生处理结果信息并所述处理结果信息加密,并将加密后的所述处理结果信息发送至所述客户端;

[0081] 所述客户端还用于接收所述服务器发送的加密后的所述处理结果信息,并将所述加密后的处理结果信息发送至所述存储终端;

[0082] 所述存储终端还用于接收所述客户端发送的加密后的所述处理结果信息,并将所述加密后的所述处理结果信息解密。

[0083] 根据本发明实施例提供的云存储系统中的文件管理方法及云存储系统的存储终端,采用存储终端对文件信息进行加密后再将加密后的文件信息从客户端发送至服务器。采用这种方式,可以使文件信息采用密文方式传输,文件信息只有通过存储终端才能进行解密;与传统的采用账户/密码方式的云存储系统相比,本发明实施例提供的云存储系统的文件管理方法及云存储系统的存储终端能够避免服务器或者传输通道遭受攻击造成文件数据泄露的情况发生,从而能够提高云存储系统的安全性。

附图说明

[0084] 为了更清楚地说明本发明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,下面描述中的附图是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0085] 图1是现有技术中传统的云存储系统的结构示意图;

[0086] 图2是本发明实施例的云存储系统的结构示意图;

[0087] 图3是本发明实施例的云存储系统的文件管理方法的流程图;

[0088] 图4是本发明实施例的云存储系统中的存储终端的结构示意图;

[0089] 图5是本发明实施例一的存储终端的文件管理方法的流程图;

[0090] 图6是本发明实施例一的云存储系统的文件管理方法中存储终端与服务器进行交叉认证的流程图;

[0091] 图7是本发明实施例一的云存储系统的文件管理方法的通过客户端实现存储终端与服务器通信的流程图;

[0092] 图8是本发明实施例一的云存储系统的文件管理方法的存储终端验证用户的网络账户信息的流程图;

[0093] 图9是本发明实施例一的云存储系统的文件管理方法的存储终端创建用户的网络账户信息的流程图;

[0094] 图10是本发明实施例一的云存储系统的文件管理方法的存储终端修改用户的网络账户信息的流程图;

[0095] 图 11 是本发明实施例一的云存储系统的文件管理方法的存储终端验证用户的身份识别码的流程图；

[0096] 图 12 是本发明实施例一的云存储系统的文件管理方法的存储终端创建用户的身份识别码的流程图；

[0097] 图 13 是本发明实施例一的云存储系统的文件管理方法的存储终端修改用户的身份识别码的流程图；

[0098] 图 14 是本发明实施例二的云存储系统的文件上传方法的流程图；

[0099] 图 15 是本发明实施例三的云存储系统的文件下载方法的流程图；

[0100] 图 16 是本发明实施例四的云存储系统的文件删除方法的流程图；

[0101] 图 17 是本发明实施例五的第一具体示例的流程图；

[0102] 图 18 是本发明实施例五的第二具体示例的流程图；

[0103] 图 19 是本发明实施例提供的云存储系统的存储终端的结构示意图。

具体实施方式

[0104] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0105] 为解决上述技术问题，本发明实施例提供一种安全云存储系统的文件管理方法、装置及该云存储系统，以提高云存储的安全性。

[0106] 其中，本发明实施例提供的云存储系统包括存储终端 201、客户端 202 和服务器 203，如图 2 所示。存储终端 201 可以通过 USB 接口或以太网与客户端 202 通信，客户端 202 可以通过互联网与服务器 203 通信。

[0107] 本发明实施例提供一种云存储系统的文件管理方法，如图 3 所示为该方法的流程图，该方法包括以下步骤：

[0108] 步骤 S301：存储终端 201 接收文件信息；

[0109] 该文件信息主要用于标识需要处理的文件的信息，可以是文件的文件名、文件的大小或者具体的文件数据等，如待上传文件的文件数据、待删除文件的文件名或者待下载文件的文件名等；

[0110] 该文件信息可以是与存储终端 201 相连的外部连接设备（如 U 盘、智能卡等）发送至存储终端 201 的，具体的，所述存储终端 201 具有与所述外部连接设备相连的 USB 接口和或智能卡卡槽；优选的，本发明实施例中的存储终端 201 可以是闪存盘。

[0111] 步骤 S302：存储终端 201 将文件信息加密；

[0112] 具体地，存储终端 201 可以具有加密芯片，可以采用 AES 对称式加密算法将文件信息加密。

[0113] 步骤 S303：存储终端 201 将加密后的文件信息通过客户端 202 发送至服务器 203；

[0114] 存储终端 201 将文件信息加密后，需要将加密后的文件信息按如下方式发送至服务器 203：首先，存储终端 201 可以将加密后的文件信息发送至客户端 202，然后客户端 202 将该加密后的文件信息发送至服务器 203。

[0115] 本发明实施例的云存储系统的文件管理方法,通过存储终端将文件信息加密,然后再通过客户端将加密后的文件信息发送至服务器,整个通讯过程中文件信息均采用密文传输,从而能够保证从客户端到服务器的文件传输过程中文件信息的安全性,进而提高云存储系统的安全性。

[0116] 同时,客户端还可以将操作指令发送至服务器,该操作指令用于标识要对文件执行何种操作,例如,文件上传指令用于标识向服务器上传某个文件,文件下载指令用于标识从服务器下载某个文件,文件删除指令用于标识删除服务器上的某个文件等等。

[0117] 在本发明的其他实施例中,该云存储系统的文件管理方法还可以包括以下步骤:

[0118] 首先,存储终端 201 接收客户端 202 转发的由服务器 203 加密并发送的处理结果信息;然后,存储终端 201 将加密的处理结果信息解密。

[0119] 此外,本发明实施例提供的云存储系统的文件管理方法还可以包括其他步骤以进一步提高该云存储系统的安全性,以下以一些具体示例对本发明的技术方案进行详细的说明,需要说明的是,下面这些示例仅是示例性的,仅用于解释本发明的技术方案,而不用用于限制本发明的技术方案,本领域普通技术人员可以在本发明提供的技术方案的基础上对本发明提供的技术方案进行改进和变形,这些都在本发明的保护范围之内。

[0120] 实施例一

[0121] 本发明实施例一提供一种云存储系统的文件管理方法,该云存储系统包括存储终端 201、客户端 202 以及服务器 203,其中,存储终端 201 可以包括主控单元 2011、安全单元 2012、智能单元 2013 以及保存单元 2014 等,存储终端 201 的具体结构可以如图 4 所示:

[0122] 具体地,本发明实施例中的主控单元 2011 即为存储终端 201 的核心处理芯片,可以采用高性能的 ARM Cortex A9 双核处理芯片,主频 1.2GHZ,内部带多媒体编解码器,可实现高清视频的编解码功能,例如可以采用 ARM-Linux2.6.x 内核;安全单元 2012 即为安全处理芯片,可以作为 USB 设备同主控单元 2011 连接,设备类型可以为 Mass Storage 设备,安全处理芯片内部带 AES256 位数据加解密引擎,保存单元 2014 访问接口,可实现保存单元 2014 的在线数据加解密,安全处理芯片内部带 7816 通信接口,可以同智能单元 2013 相互通信;智能单元 2013 即为智能卡芯片,可以采用通过了 FIPS 140-2 或 CC EAL5+ 认证的芯片,其具有 7816 接口,可以同安全单元 2012 通信。智能单元 2013 里具有 AES, RSA, SHA, OTP, RNG, GUID 等,可以满足系统所需的全部安全处理需求。保存单元 2014 为系统代码、普通数据及隐藏数据提供存储介质,通过闪存接口同安全单元 2012 相连接,除基本的 Boot Loader 外,其他所有数据均加密存储,必须通过数据解密后才可以访问,保存单元 2014 具体可以采用 NAND FLASH。

[0123] 具体地,安全处理芯片可以采用 32 位精简指令处理器 (RISC) 结构,内含共 4K 字节,16 位宽 Cache,32 字节存储 Buffer,集成 4-Entry MMU(存储管理单元),具有灵活的访问权限管理机制;Supervisor/user 访问权限,Read/write/Execute 访问权限;外部 I/O 上,该芯片可以包含 USB 2.0HS 控制器、72 个 GPIO 口,双片选 NAND FLASH 接口,1027/53 字节模式下支持每页 30 bit BCH ECC 数据纠错,支持 SCI/SMART CARD,UCI/读卡器,SPI 等接口,可实现上述接口的数据通信;安全处理芯片内部可含 32K 字节 SRAM,4K 字节 USB FIFO,8K BOOT ROM,384K 字节片内 FLASH,2K 字节 OTP FLASH,40 路的内部中断控制器,4 路的片外中断控制器,2 个定时器,1 个 WDT,7 个复位终端源控制器,1 个可编程全向 DMA 控制器;芯

片可以支持 DES 64(56), 3DES 128(112), 192(168) 位算法, 支持 AES 128/192/256 位 CBC, ECB 算法, 支持 RSA 1024/2048 算法, 支持硬件真随机数发生器 HRNG。简言之, 该芯片可以在完成编程、封闭编程、仿真接口后, 包括开发人员自身也无法获得芯片内部数据或篡改芯片内部数据。

[0124] 具体地, 智能卡芯片可以采用 SECURE_MX 51 处理核心, 内含 MMU (存储管理单元), 1 个 TRIPLES-DES 协处理器, 1 个 AES 协处理器, 1 个 16 位循环冗余校验 (CRC) 计算单元, 1 个快速随机数生成单元; 外部 I/O 上, 该芯片包含 1 个 USB 1.1 控制器、1 个 ISO 7816 接口, 支持 ISO 1443 接口, 可实现上述接口的数据通信; 芯片内部可含 4608 字节 SRAM, 72KB EEPROM, 160KB ROM, 2 个 16 位定时器; 芯片可以支持 DES, 3DES 位算法, 支持 AES128/192/256 位 CBC, ECB 算法, 支持 RSA 4096 算法, 支持硬件真随机数发生器 HRNG。无论在硬件结构还是软件层次上, 该芯片都是安全可靠的, 在关闭编程、仿真、调试接口后, 包括开发人员自身, 也无法获得芯片内部数据或篡改芯片内部数据。

[0125] 图 5 示出了本发明实施例一提供的云存储系统的文件管理方法的流程图, 该方法包括以下步骤:

[0126] 步骤 S501: 存储终端进行初始化。

[0127] 存储终端出厂后首次使用时, 需要首先进行初始化。存储终端与服务器在出厂前均已生成并保存相关存储终端的 ID、密钥等, 以便在实现云存储功能时使用。

[0128] 存储终端进行初始化时, 具体可以按以下步骤进行:

[0129] 1) 存储终端中的智能单元生成 PIN 码加密密钥、存储终端 RSA 认证密钥对、文件加密密钥并保存, 具体地可以保存在智能单元的 OTP 区域中;

[0130] 2) 存储终端中的主控单元生成存储终端的 ID, 将存储终端的 ID 写入智能单元, 存储终端的序列号采用安全单元的 ID, 具体地, 主控单元可以控制其内部的初始化程序生成存储终端的 ID;

[0131] 3) 存储终端中的主控单元导出存储终端的序列号、RSA 公钥以及存储终端的 ID, 将其存储在服务器 (具体可以存储在数据库服务器上) 上以便做存储终端的合法性验证, 具体地, 主控单元可以控制其内部的初始化程序导出存储终端的序列号、RSA 公钥以及存储终端的 ID;

[0132] 4) 存储终端中的主控单元将 RSA 公钥写入存储终端的智能单元, 具体地, 主控单元可以控制其内部的初始化程序将 RSA 公钥写入智能单元中的 OTP 区域。

[0133] 步骤 S502: 存储终端验证用户输入的身份识别码是否正确, 如果是, 执行步骤 S503。

[0134] 为进一步提高云存储系统的文件管理的安全性, 本发明实施例一还可以在用户对存储终端进行操作之前对用户的身份识别码进行验证, 本发明实施例一中用户的身份识别码即用户的 PIN 码, 具体地验证过程可以在存储终端内的主控单元、安全单元和智能单元之间进行, 参见图 6 所示:

[0135] 步骤 S601: 用户在存储终端输入 PIN 码;

[0136] 具体地, 用户可以根据存储终端产生的虚拟键盘通过与存储终端中的主控单元连接的显示单元的触摸屏输入 PIN 码, 该虚拟键盘可以由存储终端的安全单元随机产生, 由主控单元获取该随机虚拟键盘并控制与主控单元连接的显示单元显示。

[0137] 步骤 S602 :主控单元根据用户输入的 PIN 码得到该 PIN 码对应的第一触摸点坐标值 ;

[0138] 步骤 S603 :主控单元将该第一触摸点坐标值发送给安全单元,具体地,主控单元可以通过 USB 接口与安全单元通信 ;

[0139] 步骤 S604 :安全单元对第一触摸点坐标值进行译码,得到 PIN 码,具体地,安全单元可以根据随机产生的虚拟键盘对第一触摸点坐标值进行译码 ;

[0140] 步骤 S605 :安全单元对 PIN 码做 HASH 及 AES 运算(加密运算),得到 AES-HASH-PIN ;

[0141] 步骤 S606 :安全单元将 AES-HASH-PIN 发送给智能单元 ;

[0142] 步骤 S607 :智能单元对 AES-HASH-PIN 进行验证,具体地,智能单元对接收到的 AES-HASH-PIN 和预先存储在智能单元中的该用户的预存 AES-HASH-PIN 进行比较,如果比较结果一致,执行步骤 S608 ;

[0143] 步骤 S608 :智能单元产生验证通过提示消息 ;

[0144] 步骤 S609 :智能单元将验证通过提示消息发送至安全单元 ;

[0145] 步骤 S610 :安全单元将验证通过提示消息发送至主控单元 ;最后,主控单元可以通过与其连接的显示单元将验证通过提示消息显示出来 ;

[0146] 另外,如果智能单元对接收到的 AES-HASH-PIN 和该用户的预存 AES-HASH-PIN 进行比较后的比较结果不一致,则智能单元可以产生验证失败提示消息,将验证失败提示消息发送至安全单元 ;安全单元可以置 PIN 码验证错误状态,拒绝所有后续文件管理操作,并向主控单元发送验证失败提示消息,主控单元通过与其相连的显示单元将该验证失败提示消息显示 ;

[0147] 此外,存储终端对用户的 PIN 码验证失败之后还可以再次进行 PIN 码验证,即重复执行步骤 S601~ 步骤 S607,如果验证失败次数超过 10 次,则存储终端默认该用户进行 PIN 码验证的行为属于恶意攻击,此时存储终端将启用自毁程序自毁。

[0148] 在采用存储终端对文件进行管理之前,首先对用户的身份识别码进行验证,有利于确保文件管理的安全性,防止恶意攻击,从而提高云存储系统的安全性。

[0149] 另外,如果用户首次使用该存储终端,则还需要创建该存储终端的 PIN 码。具体地,创建 PIN 码的过程可以在存储终端内的主控单元、安全单元和智能单元之间进行,参见图 7 所示 :

[0150] 步骤 S701 :用户在存储终端输入要设置的 PIN 码 ;

[0151] 具体地,用户可以根据存储终端产生的虚拟键盘通过与存储终端中的主控单元连接的显示单元的触摸屏输入 PIN 码,该虚拟键盘可以由存储终端的安全单元随机产生,由主控单元获取该随即虚拟键盘并控制与主控单元连接的显示单元显示。

[0152] 步骤 S702 :主控单元根据用户输入的 PIN 码得到该 PIN 码对应的第二触摸点坐标值 ;

[0153] 步骤 S703 :主控单元将第二触摸点坐标值发送给安全单元,具体地,主控单元可以通过 USB 接口与安全单元通信 ;

[0154] 步骤 S704 :安全单元对第二触摸点坐标值进行译码,得到 PIN 码,具体地,安全单元可以根据其随机产生的虚拟键盘对第二触摸点坐标值进行译码 ;

[0155] 步骤 S705 :安全单元将 PIN 码做 HASH 及 AES 运算(加密运算),得到 AES-HASH-PIN ;

[0156] 步骤 S706 :安全单元将 AES-HASH-PIN 发送给智能单元 ;

[0157] 步骤 S707 :智能单元将 AES-HASH-PIN 保存 ;具体地可以保存在其内部的 NOR 中 ;

[0158] 步骤 S708 :智能单元产生 PIN 码设置成功提示消息 ;

[0159] 步骤 S709 :智能单元将 PIN 码设置成功提示消息发送至安全单元 ;

[0160] 步骤 S710 :安全单元将 PIN 码设置成功提示消息发送至主控单元,最后,主控单元可以通过与其连接的显示单元将验证通过提示消息显示 ;

[0161] 其中,智能单元具有一次性写入功能,可以防止开发人员后续更改存储终端的运行代码和数据 ;其中智能单元具有只写区域,关键密钥(如存在 IC 中的密钥以及 RSA 公私钥)等只能写入,关键密钥可参与加解密运算但无法读出 ;另外,可以由安全单元发起随机虚拟键盘显示功能,以做到存储终端每次显示的虚拟键盘按键排布不一致。具体地,PIN 码字符集可以为 96 字符集,可以强制性要求包含字母、数字、特殊字符的组合方式,长度不低于 12 字符等,以进一步提高云存储系统文件管理的安全性。

[0162] 需要说明的是,本发明实施例一中创建用户身份识别码的步骤可以依据具体要求在任何需要的步骤执行。

[0163] 基于上述描述,在云存储系统中,用户每次访问服务器都需要首先进行 PIN 码验证,这样,用户的 PIN 码使用频率可能会较高,导致 PIN 码泄露的几率和可能性较大,为此,本发明实施例一还提供一种使用存储终端对 PIN 码进行修改的方法。具体地修改过程可以如图 8 所示 :

[0164] 步骤 S801 :用户在存储终端输入新、旧 PIN 码 ;

[0165] 具体地,用户可以根据存储终端产生的虚拟键盘通过与存储终端中的主控单元连接的显示单元的触摸屏输入新、旧 PIN 码,该虚拟键盘可以由存储终端的安全单元随机产生,由主控单元获取该随即虚拟键盘并控制与主控单元连接的显示单元显示。

[0166] 步骤 S802 :主控单元根据用户输入的新、旧 PIN 码得到新、旧 PIN 码对应的第三触摸点坐标值(与新 PIN 码对应)和第四触摸点坐标值(与旧 PIN 码对应) ;

[0167] 步骤 S803 :主控单元将第三触摸点坐标值和第四触摸点坐标值发送给安全单元,具体地,主控单元可以通过 USB 接口与安全单元通信 ;

[0168] 步骤 S804 :安全单元对第三触摸点坐标值和第四触摸点坐标值进行译码,得到旧 PIN 码 OLD-PIN 和新 PIN 码 NEW-PIN ;具体地,安全单元可以根据其随机产生的虚拟键盘对第三触摸点坐标值和第四触摸点坐标值进行译码 ;

[0169] 步骤 S805 :安全单元将旧 PIN 码 OLD-PIN 和新 PIN 码值 NEW-PIN 分别做 HASH 及 AES 运算,得到 AES-HASH-OLD-PIN 和 AES-HASH-NEW-PIN ;

[0170] 步骤 S806 :安全单元将 AES-HASH-OLD-PIN 和 AES-HASH-NEW-PIN 发送给智能单元 ;

[0171] 步骤 S807 :智能单元对 AES-HASH-OLD-PIN 和保存在存储终端内的预存旧 PIN 码 AES-HASH-PIN 和进行比较,如果比较结果一致,执行步骤 S808 ;

[0172] 步骤 S808 :智能单元保存新的 PIN 码码值 AES-HASH-NEW-PIN,并产生 PIN 码修改成功提示消息 ;

[0173] 步骤 S809 :智能单元将 PIN 码修改成功提示消息发送至安全单元 ;

[0174] 步骤 S810 :安全单元将 PIN 码修改成功提示消息发送至主控单元,最后,主控单元可以通过与其连接的显示单元将验证通过提示消息显示 ;

[0175] 另外,如果智能单元对接收到的旧 AES-HASH-PIN 和该用户的预存 AES-HASH-PIN 进行比较后的比较结果不一致,则智能单元不允许修改 PIN 码,并且可以修改失败提示消息,将修改失败提示消息发送至安全单元 ;安全单元向主控单元发送修改失败提示消息,主控单元通过与其相连的显示单元将该修改失败提示消息显示 ;

[0176] 此外,存储终端对用户修改 PIN 码失败之后还可以再次进行 PIN 码修改,即重复执行步骤 S801~ 步骤 S807,如果修改失败次数超过 10 次,则存储终端默认该用户修改 PIN 码的行为属于恶意攻击,此时存储终端将启用自毁程序自毁。

[0177] 需要说明的是,本发明实施例中修改 PIN 码的步骤可以在用户通过存储终端的身份识别码之后的任一步骤执行。

[0178] 本发明实施例一提供的采用存储终端修改 PIN 码的方法,可以为用户提供一种方便快捷的 PIN 码修改方式,用户及时对 PIN 码进行修改,有利于避免因 PIN 码泄露或者丢失而影响云存储系统的安全性的情况发生,有利于进一步提高云存储系统的安全性。

[0179] 步骤 S503 :存储终端与服务器进行交叉认证。

[0180] 存储终端出厂时,存储终端的 ID、序列号 SN、RSA 公钥等均已经记录在服务器中,服务器的 RSA 公钥已经写入存储终端中,设定服务器的 RSA 公钥为 SP、服务器的 RSA 私钥为 SS、存储终端的 RSA 公钥为 DP、存储终端的 RSA 私钥为 DS,则存储终端与服务器之间的交叉认证可以按如下步骤进行,如图 9 所示 :

[0181] 步骤 S901 :首先存储终端生成随机数 R1,使用存储终端的 RSA 私钥 DS 对随机数 R1 加密得到 M1,然后读取存储终端的 ID 和序列号 SN ;接着,存储终端用服务器的 RSA 公钥 SP 对 M1、存储终端的 ID 和序列号 SN 加密得到 M2,公式如下 :

[0182] $M1 = \text{RSA_E}(R1, DS)$;

[0183] $M2 = \text{RSA_E}((M1, ID, SN), SP)$;

[0184] 步骤 S902 :存储终端通过客户端将 M2 发送到服务器 ;

[0185] 步骤 S903 :服务器接收到加密数据 M2 后用服务器的 RSA 私钥 SS 将 M2 解密得到存储终端的 ID 和序列号 SN 以及 M1,公式如下 :

[0186] $(M1, ID, SN) = \text{RSA_D}(M2, SS)$;

[0187] 服务器根据存储终端的 ID 和序列号 SN 查询数据库中是否存在该存储终端,如果存在,则读取该存储终端对应的存储终端的 RSA 公钥 DP,用存储终端的 RSA 公钥 DP 对 M1 进行解密得到 R1',公式如下 :

[0188] $R1' = \text{RSA_D}(M1, DP)$;

[0189] 服务器生成随机数 R2,服务器使用服务器的 RSA 私钥 SS 对随机数 R2 进行加密得到 M3,接着服务器使用存储终端的 RSA 公钥 DP 对 M3 和 R1' 进行加密得到 M4,公式如下 :

[0190] $M3 = \text{RSA_E}(R2, SS)$;

[0191] $M4 = \text{RSA_E}((M3, R1'), DP)$;

[0192] 步骤 S904 :服务器通过客户端将 M4 返回给存储终端 ;

[0193] 步骤 S905 :存储终端接收到加密数据 M4 后,使用存储终端的 RSA 私钥 DS 对 M4 进

行解密得到随机数 $R1'$ 和 $M3$, 存储终端对比 $R1'$ 和 $R1$, 如果一致则表明服务器可信且服务器已得到存储终端公钥, 公式如下:

[0194] $(M3, R1') = \text{RSA_D}(M4, DS)$;

[0195] 存储终端使用服务器的 RSA 公钥 SP 对 $M3$ 进行解密得到 $R2'$, 存储终端使用存储终端的 RSA 私钥 DS 对 $R2'$ 进行加密得到 $M5$, 公式如下:

[0196] $R2' = \text{RSA_D}(M3, SP)$;

[0197] $M5 = \text{RSA_E}(R2', DS)$;

[0198] 步骤 S906: 存储终端通过客户端将 $M5$ 发送到服务器;

[0199] 步骤 S907: 服务器收到加密数据 $M5$ 后, 使用存储终端的 RSA 公钥 DP 对 $M5$ 进行解密得到 $R2'$, 服务器比较 $R2'$ 和 $R2$, 如果一致则表明该存储终端可信, 公式如下:

[0200] $R2' = \text{RSA_D}(M5, DP)$;

[0201] 服务器随机产生通信密钥 AES-KEY , 服务器使用存储终端的 RSA 公钥 DP 对 AES-KEY 进行加密得到 $M6$, 公式如下:

[0202] $M6 = \text{RSA_E}(\text{AES-KEY}, DP)$;

[0203] 步骤 S908: 服务器通过客户端将 $M6$ 返回给存储终端,

[0204] 步骤 S909: 存储终端接收到 $M6$ 后使用存储终端的 RSA 私钥 DS 对 $M6$ 进行解密得到 AES-KEY , 则后续服务器与存储终端之间的命令通信都可以采用该 AES-KEY 加密通信, 公式如下:

[0205] $\text{AES-KEY} = \text{RSA_D}(M6, DS)$ 。

[0206] 存储终端在出厂时已经和服务器相互交换了 RSA 公钥, 通过随机数完成存储终端与服务器相互认证后最终生成通信密钥, 之后每个数据通信命令包都是经过加密的, 网络窃听无法得到真实数据; 采用网络抓包过程录制数据回放, 连接建立后两次请求和应答都采用了随机数, 事件回放不可能认证通过, 避免了事件回放的可能性; 存储终端在出厂时已经预设了服务器的公钥, 仿冒服务器则无法产生同样的 RSA 密钥对, 仿冒服务器会导致数据解密失败而整个通信结束; 由于无法知道存储终端的私钥, 就算获取了存储终端传输的公钥并仿冒存储终端同服务器进行通信, 后续的通信过程也无法正常进行; 同时服务器上记录有存储终端合法的 ID 及序列号, 对于非法的存储终端 ID, 服务器会拒绝提供服务。

[0207] 需要说明是, 存储终端自身并不具有网络传输接口, 也不具有网络传输的相关功能, 所以, 存储终端与服务器之间的通信需要通过客户端实现。因此, 在存储终端与服务器进行交叉认证之前, 即执行步骤 S503 之前, 还可以进行以下步骤(如图 10 所示):

[0208] 步骤 S1001: 存储终端接收客户端发送的获取数据请求;

[0209] 步骤 S1002: 存储终端产生连接服务器请求;

[0210] 步骤 S1003: 存储终端将连接服务器请求发送至客户端;

[0211] 步骤 S1004: 客户端将存储终端发送的连接服务器请求发送至服务器;

[0212] 步骤 S1005: 服务器产生允许连接消息;

[0213] 步骤 S1006: 服务器将允许连接消息发送至客户端;

[0214] 步骤 S1007: 客户端将服务器发送的允许连接消息发送至存储终端。

[0215] 这样, 存储终端就可以通过客户端与服务器实现通信; 即存储终端可以通过客户端将相关数据发送至服务器, 同时, 服务器也可以通过客户端将相关数据返回至存储终端。

[0216] 另外,存储终端也可以与服务器断开连接:存储终端可以通过客户端将断开连接请求发送至服务器,然后服务器产生断开连接消息并发送至客户端,之后,存储终端与服务器的连接断开。

[0217] 步骤 S504:存储终端验证用户的网络账户信息是否正确,如果是,执行步骤 S505。

[0218] 存储终端与服务器之间的交叉认证通过之后,存储终端使用服务器返回的通信密钥 AES-KEY,存储终端与服务器后续通信过程使用 AES-KEY 加密,在执行后续通信步骤之前,存储终端可以验证用户的网络账户信息是否正确,网络账户信息可以包括账号和密码,具体的验证过程可以按如下步骤操作(如图 11 所示):

[0219] 步骤 S1101:用户在存储终端输入账号和密码;

[0220] 具体地,存储终端还可以包括输入单元,该输入单元可以与主控单元连接,用户可以通过该输入单元在存储终端中输入账号和密码;

[0221] 步骤 S1102:存储终端将用户输入的账号和密码加密;

[0222] 本发明实施例中的存储终端可以包括安全单元和主控单元,因此具体地加密过程可以按如下步骤进行:

[0223] 1) 用户在存储终端输入账号和密码后,存储终端中的主控单元将用户输入的账号和密码发送至存储终端中的安全单元;

[0224] 2) 安全单元采用通信密钥(如 AES-KEY)将账号和密码加密;

[0225] 3) 安全单元将加密后的账号和密码返回至主控单元。

[0226] 步骤 S1103:存储终端将加密后的账号和密码发送至客户端;

[0227] 具体地,存储终端可以通过其内部的主控单元将加密后的账号和密码发送至客户端;

[0228] 步骤 S1104:客户端将加密后的账号和密码发送至服务器;

[0229] 步骤 S1105:服务器将加密后的账号和密码解密;

[0230] 步骤 S1106:服务器产生随机数,并将该随机数与存储终端的 ID 以及解密后的账号和密码经过 HASH 算法加密,并将加密后的结果与存储在数据库服务器中的该账户对应的密码进行比较,如果加密后的结果与存储的密码一致,则进行步骤 S1107;

[0231] 步骤 S1107:服务器通过密码验证,并产生登录成功密文响应;

[0232] 步骤 S1108:服务器将登录成功密文响应发送至客户端;

[0233] 步骤 S1109:客户端将服务器发送的登录成功密文响应发送至存储终端;

[0234] 步骤 S1110:存储终端将登录成功密文响应解密,并显示登录成功明文;

[0235] 具体地,存储终端中的主控单元接收到客户端发送的登录成功密文响应后,可以将该密文响应发送至安全单元,随后安全单元将该密文响应解密,并将解密后的登录成功明文发送至主控单元,通过与主控单元相连的显示单元将该登录成功明文显示出来。

[0236] 另外,用户在首次使用云存储系统时需要首先进行注册,即创建该用户的网络账户信息(包括账号和密码),网络账户信息可以在存储终端上输入(如通过与主控单元相连的显示单元),用户通过存储终端输入相关的网络账户信息,通过通信密钥(如 AES-KEY)加密后通过客户端发送到服务器进行注册,服务器解密得到账号和密码后,使用服务器的随机数 R1 和存储终端的 ID 对账号和密码进行加密(如 HASH 算法加密)后以密文形式存储在服务器上,注册后用户可以利用该账号和密码登录云存储系统。即在执行步骤 S503 之前,

还可以创建用户的网络账户的账号和密码,如图 12 所示,具体地可以按如下步骤创建用户的账号和密码:

- [0237] 步骤 S1201:用户在存储终端输入账号和密码;
- [0238] 具体地,用户可以通过存储终端中与主控单元连接的输入单元输入账号和密码;
- [0239] 步骤 S1202:存储终端将用户输入的账号和密码加密,生成账号和密码密文;
- [0240] 具体地,用户在存储终端输入账号和密码后,存储终端中的主控单元将该账号和密码发送至存储终端中的安全单元;然后,安全单元采用通信密钥(如 AES-KEY)将账号和密码加密,并将加密后的账号和密码返回至主控单元。
- [0241] 步骤 S1203:存储终端将加密后的账号和密码发送至客户端;
- [0242] 步骤 S1204:客户端将加密后的账号和密码发送至服务器;
- [0243] 步骤 S1205:服务器对加密后的账号和密码进行解密,并产生注册成功密文响应;
- [0244] 步骤 S1206:服务器将注册成功密文响应发送至客户端;
- [0245] 步骤 S1207:客户端将注册成功密文响应发送至存储终端;
- [0246] 步骤 S1208:存储终端将注册成功密文响应解密,并显示注册成功明文;
- [0247] 具体地,存储终端中的主控单元接收到客户端发送的注册成功密文响应后,将该注册成功密文响应发送至安全单元,随后安全单元将该密文响应解密并将解密后的注册成功明文,通过与主控单元相连的显示单元将该注册成功明文显示出来。
- [0248] 在本发明的一个具体示例中,网络账户信息中的账号可以默认是存储终端的 ID,此时,上述验证和创建网络账户信息的步骤可以仅是验证和创建网络账户信息中的密码。
- [0249] 此外,本发明实施例中的云存储系统的文件管理方法还可以对用户的网络账户信息进行修改,即对密码进行修改,具体的修改过程可以参见图 13 所示:
- [0250] 步骤 S1301:用户在存储终端输入原始密码和新密码;
- [0251] 具体地,用户可以通过存储终端中与主控单元连接的输入单元输入原始密码和新密码;
- [0252] 步骤 S1302:存储终端将用户输入的原始密码和新密码加密;
- [0253] 具体地,对用户输入的原始密码和新密码进行加密可以按如下步骤进行:用户在存储终端输入原始密码和新密码后,存储终端中的主控单元将用户输入的原始密码和新密码发送至存储终端中的安全单元;随后,安全单元采用通信密钥(如 AES-KEY)将原始密码和新密码加密并将加密后的原始密码和新密码返回至主控单元。
- [0254] 步骤 S1303:存储终端将加密后的原始密码和新密码发送至客户端;
- [0255] 步骤 S1304:客户端将加密后的原始密码和新密码发送至服务器;
- [0256] 步骤 S1305:服务器对加密后的原始密码和新密码进行解密;
- [0257] 步骤 S1306:服务器产生随机数,并将该随机数与存储终端的 ID 以及解密后的原始密码经过 HASH 算法加密,并将加密后的结果与存储在数据库服务器中的该账户对应的原始密码进行比较,如果加密后的结果与存储的密码一致,则进行步骤 S1307;
- [0258] 步骤 S1307:服务器将随机数与加密后的新密码经过 HASH 加密存储在本地(数据库服务器);
- [0259] 步骤 S1308:服务器产生密码修改成功密文响应;
- [0260] 步骤 S1309:服务器将密码修改成功密文响应发送至客户端;

[0261] 步骤 S1310 :客户端将服务器发送的密码修改成功密文响应发送至存储终端 ;

[0262] 步骤 S1311 :存储终端将密码修改成功密文响应解密,并显示密码修改成功明文 ;

[0263] 具体地,存储终端中的主控单元接收到客户端发送的密码修改成功密文响应后,可以将该密文响应发送至安全单元,随后安全单元将该密文响应解密,并将解密后的密码修改成功明文发送至主控单元,通过与主控单元相连的显示单元将该密码修改成功明文显示出来。

[0264] 需要说明的是,修改网络账户信息的步骤(即步骤 S1301~ 步骤 S1311)可以在存储终端验证用户的网络账户信息(即步骤 S504)之前进行,也可以在存储终端验证用户的网络账户信息之后进行,还可以在本发明实施例提供的云存储系统的文件管理方法的其他步骤的之前或者之后进行,总之,本发明实施例中的修改网络账户信息的步骤在何时执行不受限制。

[0265] 步骤 S505 :存储终端向客户端发送请求处理信息 ;

[0266] 具体地,存储终端可以通过与其内部的主控单元相连的 USB 接口向客户端发送请求处理信息,该请求处理信息可以由存储终端的主控单元产生 ;另外,存储终端还可以首先对该请求处理信息进行加密,然后再将加密后的请求处理信息发送至客户端。

[0267] 步骤 S506 :客户端将请求处理信息发送至服务器,具体地,客户端可以将加密后的请求处理信息发送至服务器。

[0268] 步骤 S507 :服务器向客户端返回确定处理文件信息,具体地,服务器可以首先将加密后的请求处理信息解密,然后对请求处理信息进行处理,如果服务器能够依照该请求处理信息处理文件,则向客户端返回确定处理文件信息,其中,服务器可以首先将确定处理文件信息加密,然后将加密后的确定处理文件信息返回至客户端。

[0269] 步骤 S508 :客户端将服务器返回的确定处理文件信息发送至存储终端 ;具体地,客户端可以将服务器返回的加密后的确定处理文件信息发送至存储终端。

[0270] 步骤 S509 :存储终端接收文件信息 ;

[0271] 该文件信息主要用于标识需要处理的文件的信息,可以是文件的文件名、文件大小、文件类型或者具体的文件数据等,如待上传文件的文件数据、待删除文件的文件名或者待下载文件的文件名等 ;

[0272] 该文件信息可以是与存储终端 201 相连的外部连接设备(如 U 盘、智能卡等)发送的 ;具体地,存储终端 201 可以是闪存盘。

[0273] 步骤 S510 :存储终端将文件信息加密 ;

[0274] 本发明实施例中的存储终端可以包括主控单元、安全单元、智能单元以及保存单元等等,本发明实施例一中的存储终端对文件信息加密可以按以下步骤进行 :

[0275] A、主控单元将文件信息发送至安全单元 ;

[0276] 具体地,本发明实施例中的主控单元可以与 USB 主机、读卡器以及 USB 设备等外设设备连接,该文件信息可以由 USB 主机和 / 或读卡器发送至存储终端中的主控单元,然后由主控单元发送至安全单元 ;

[0277] B、安全单元将文件信息加密,并将加密后的文件信息返回至主控单元 ;

[0278] 具体地,安全单元可以采用本发明实施例提到的加密算法将文件信息加密,也可以采用本发明实施例没有提到的本领域常用的其他加密算法将文件信息加密。

[0279] 步骤 S511 :存储终端将加密后的文件信息发送至客户端 ;

[0280] 具体地,存储终端中的主控单元可以将加密后的文件信息通过 USB 接口等发送至客户端 ;

[0281] 如果文件信息由 USB 主机、读卡器以及 USB 设备等外设设备通过存储终端发送至客户端,则需要首先在存储终端对该文件信息加密,然后再将加密后的文件信息发送至客户端 ;如果文件信息是存储终端自身携带,例如保存在存储终端的保存单元中的文件信息,则无需加密,保存单元可将该文件信息通过安全单元发送至主控单元,然后主控单元可通过 USB 接口等将该文件信息直接发送至客户端。

[0282] 步骤 S512 :存储终端将加密后的文件信息发送至服务器 ;

[0283] 步骤 S513 :服务器对加密后的文件信息进行处理,并产生处理结果信息密文 ;

[0284] 具体地,服务器可以首先将客户端发送的文件信息解密,然后对解密后的文件信息进行处理,并产生处理结果信息明文,然后将处理结果信息明文加密成为处理结果信息密文。

[0285] 步骤 S514 :服务器将处理结果信息密文发送至客户端 ;

[0286] 步骤 S515 :客户端将处理结果信息密文发送至存储终端 ;

[0287] 具体地,客户端可以通过 USB 接口等将处理结果信息密文发送至存储终端的主控单元。

[0288] 步骤 S516 :存储终端将处理结果信息密文解密成为处理结果信息明文 ;

[0289] 具体地,存储终端中的主控单元接收到处理结果信息密文后,将该密文发送至安全单元,安全单元将该处理结果信息密文解密成为处理结果信息明文。

[0290] 本发明实施例一提供的云存储系统的文件管理方法,在对文件进行处理之前,首先进行存储终端初始化、用户的身份识别码验证、用户的网络账户信息验证等步骤,并在存储终端将文件信息加密再将加密后的文件信息通过客户端发送至服务器 ;另外,由服务器返回的操作结果信息需要通过存储终端进行解密。采用这种方式,可以使文件信息和操作结果信息采用密文方式传输,文件信息和操作结果信息只有通过存储终端才能解密,与传统的基于账户 / 密码方式的云存储系统相比,本发明实施例一提供的云存储系统的文件管理方法能够避免服务器或者传输通道遭受攻击造成文件数据泄露,从而能够提高云存储系统的安全性。

[0291] 需要说明的是,本发明实施例中的文件管理方法可以有多种具体方式,例如文件上传、文件下载以及文件删除等。下面通过一些具体示例对本发明实施例的技术方案做详细说明。但是,下面给出的示例只是示例性的,只用于解释本发明实施例的技术方案,而对本发明实施例的技术方案没有限制,所有基于本发明技术方案的构思并且能够实现本发明目的的相关方案都在本发明的保护范围内。

[0292] 实施例二

[0293] 可以采用本发明实施例中的文件管理方法进行文件上传操作,本发明实施例二示出了采用该文件管理方法进行文件上传操作(以下统称文件上传方法)的具体过程,如图 14 所示,为其流程图,该文件上传方法包括以下步骤 :

[0294] 步骤 S1401 :存储终端接收待上传文件的文件数据 X ;

[0295] 步骤 S1402 :存储终端产生将该待上传文件的文件数据 X 上传的文件上传指令 ;具

体地,待上传文件的文件数据可以通过 USB 接口等发送至存储终端内的主控单元,另外,文件上传指令也可以由主控单元产生。

[0296] 步骤 S1403:存储终端将文件上传指令和待上传文件的文件数据 X 加密;

[0297] 主控单元将接收到的文件上传指令和待上传文件的文件数据 X 发送至安全单元,安全单元将文件上传指令和待上传文件的文件数据 X 加密,具体地,可以采用 AES 对称式加密算法。

[0298] 步骤 S1404:存储终端将加密后的文件上传指令和待上传文件的文件数据 X 发送至客户端;

[0299] 安全单元将加密后的文件上传指令和待上传文件的文件数据 X 发送至主控单元,然后主控单元再通过 USB 接口将加密后的文件上传指令和待上传文件的文件数据 X 等发送至客户端;

[0300] 另外,如果待上传文件的文件数据来自于存储终端内的保存单元,则该待上传文件的文件数据 X 已经经过加密,无需再次通过安全单元进行加密,保存单元可以将该待上传文件的文件数据 X 通过安全单元发送至主控单元,再由主控单元通过 USB 接口发送至客户端;与该待上传文件的文件数据 X 相应的文件上传指令可以由主控单元产生,发送至安全单元加密并返回主控单元,再由主控单元通过 USB 接口发送至客户端。

[0301] 步骤 S1405:客户端将加密后的文件上传指令和待上传文件的文件数据 X 发送至服务器。

[0302] 在本发明的其他实施例中,文件上传指令也可以不经过存储终端加密,直接由客户端发送至服务器。

[0303] 步骤 S1406:服务器依据文件上传指令将待上传文件的文件数据 X 保存至本地。

[0304] 具体地,云存储系统中的服务器可以采用分布式文件系统的结构,如图 15 所示,为服务器的系统架构图,该服务器可以分为三个主要的部分:Storage 服务器、Tracker 服务器以及 DB 数据库服务器。各部分的主要作用和特点如下:

[0305] Storage 存储服务器:主要负责处理用户上传、下载、删除文件请求,文件最终存储在 Storage 服务器上,Storage 服务器可以划分为多个组(Group),每一组内包含若干台 Storage 服务器,不同组之间的 Storage 服务器没有连接,同一组之间的 Storage 服务器相互连接备份数据,实现了软件组内镜像磁盘阵列(Redundant Array of Independent Disks 1, RAID1)。

[0306] Tracker 服务器:其核心功能为系统调度,存储负载均衡和用户的认证,多个 Tracker 服务器可以组成集群,每个 Tracker 服务器都和每一组中多个 Storage 服务器连接,记录 Storage 服务器及 Storage 服务器(Group)的状态信息,对用户请求做负载均衡处理,每一个 Tracker 服务器都是对等的,具有相同的功能,不存在下头结点,Tracker 服务器集群是多活热备的,任何一个 Tracker 服务器出现故障,其他 Tracker 服务器都可以完全接替其工作。

[0307] DB 数据库服务器:用于记录用户的基本信息和用户文件信息,用户信息包括存储终端的 ID、用户的文件数、最后一次使用时间等。用户的文件信息包括用户的文件名、文件存储的 Storage 服务器地址等。客户端连接 Storage 服务器上传完文件后,Storage 服务器会在数据库中增加一条用户文件信息;用户删除文件后,Storage 服务器会删除数据库

里面的用户文件信息。当用户连接 Tracker 服务器查询用户当前文件信息时, Tracker 服务器就能很快从数据库中检索到用户的文件信息, Tracker 服务器和 Storage 服务器可以共享 DB 数据库服务器。

[0308] 鉴于服务器具有上述结构,所以步骤 S1406 可以按照如下方式进行:Tracker 服务器对客户端发送的加密后的文件上传指令和待上传文件的文件数据 X 解密,并依据文件上传指令将待上传文件的文件数据 X 发送至 Storage 服务器进行保存。

[0309] 另外,该文件上传方法还可以包括以下步骤:

[0310] 步骤 S1407:服务器将待上传文件的文件数据 X 保存至本地后,生成该待上传文件的文件数据 X 的文件名(该文件名可以包括文件的组名和 / 或文件的网络名),并将该文件名加密。

[0311] 具体地,该步骤可以按如下方式进行:

[0312] Storage 服务器将待上传文件的文件数据 X 保存至本地后,生成该待上传文件的文件数据 X 的文件名, Tracker 服务器可以通过 DB 数据库服务器共享该文件名,并将该文件名加密。

[0313] 步骤 S1408:服务器将加密后的文件名发送至客户端。具体地,可以由 Tracker 服务器将加密后的文件名发送至客户端。

[0314] 步骤 S1409:客户端将服务器发送的加密后的文件名发送至存储终端;

[0315] 具体地,客户端可以将加密后的文件名发送至存储终端中的主控单元。

[0316] 步骤 S1410:存储终端将该文件名解密;

[0317] 主控单元可以将接收到的加密后的文件名发送至安全单元,安全单元将加密后的文件名解密,然后将解密后的文件名发送至保存单元保存和 / 或主控单元。

[0318] 另外,Storage 服务器将待上传文件的文件数据 X 保存至本地后,还可以生成该待上传文件的文件数据 X 存储在 Storage 服务器中的地址 X-1,并将该地址 X-1 通过客户端发送至存储终端。

[0319] 另外,在客户端将文件上传指令和待上传文件的文件数据 X 发送至存储终端之前,还可以包括以下步骤:

[0320] A、存储终端与服务器进行交叉认证;

[0321] B、存储终端与服务器进行网络账户验证;

[0322] C、存储终端向服务器发送请求文件上传地址,具体可以是存储终端向 Tracker 服务器发送请求文件上传的 Storage 服务器中的地址;

[0323] D、Tracker 服务器将请求文件上传的 Storage 服务器中的地址返回至存储终端;

[0324] E、存储终端对 Storage 服务器进行验证。

[0325] 上述步骤 A~E 的具体操作与本发明实施例一中的相应操作类似,在此不再赘述。

[0326] 此外,本发明实施例二中的文件上传方法还可以包括存储终端对用户的 PIN 码进行验证等其他步骤,本发明实施例一中的所有步骤都可以与本发明实施例二的技术方案进行组合得到其他技术方案。

[0327] 本发明实施例二提供的文件上传方法,采用存储终端对文件上传指令和待上传文件的文件数据进行加密,并在服务器将文件上传指令和待上传文件的文件数据保存至本地,并返回该文件上传指令和待上传文件的文件数据的文件名加密并返回客户端之后采用

存储终端对该文件名解密。通过这种方式,能够保证文件上传指令和待上传文件的文件数据和对应的文件名在客户端、服务器以及传输过程中均是加密的,只有通过存储终端解密才能得到该文件上传指令和待上传文件的文件数据和对应的文件名的明文,保证了文件上传的安全性。

[0328] 本发明实施例的文件管理方法除了包括文件上传方法,还可以包括文件下载方法,下面在实施例三中对文件下载方法进行详细说明。

[0329] 实施例三

[0330] 本发明实施例三提供一种云存储系统的文件下载方法,图 15 示出了该方法的流程图,该方法可以包括以下步骤:

[0331] 步骤 S1501:存储终端接收待下载文件的文件名 Y (包括待下载文件的组名、网络文件名);

[0332] 步骤 S1502:存储终端产生该待下载文件的文件名 Y 对应的文件下载指令;

[0333] 步骤 S1503:存储终端将该文件下载指令和待下载文件的文件名 Y 加密,该加密过程可以采用本发明实施例一中的加密算法。

[0334] 步骤 S1504:存储终端将加密后的该文件下载指令和待下载文件的文件名 Y 发送至客户端;

[0335] 步骤 S1505:客户端将文件下载指令和加密后的该文件下载指令和待下载文件的文件名 Y 发送至服务器。

[0336] 步骤 S1506:服务器依据文件下载指令将对应该文件下载指令和待下载文件的文件名 Y 的文件数据下载至本地。

[0337] 存储终端可以首先连接 Tracker 服务器依据待下载文件的文件名 Y 获取文件下载地址,然后再连接 Storage 服务器依照文件下载指令和获取的文件下载地址提取出存储在本地与待下载文件的文件名 Y 对应的文件数据 Y-1。

[0338] 步骤 S1507:服务器将下载的文件数据 Y-1 发送至客户端。

[0339] 步骤 S1508:客户端将服务器发送的下载文件数据 Y-1 发送至存储终端。

[0340] 步骤 S1509:存储终端将客户端转发的下载文件数据 Y-1 解密,至此,完成文件下载过程。

[0341] 需要说明的是,在客户端读取文件下载指令和待下载文件的文件名(即步骤 S1502)之前,本发明实施例三中的文件下载方法还可以包括如本发明实施例二中的类似步骤,鉴于这些步骤可以由本发明实施例二中的对应步骤简单推导得出,因此,在此对这些步骤不再赘述。

[0342] 本发明实施例三提供的文件下载方法,采用存储终端对文件下载指令和待下载文件的文件名进行加密,并在服务器依据该文件下载指令和待下载文件的文件名读取与其对应的待下载文件数据并将该待下载文件数据返回客户端之后采用存储终端对该待下载文件数据解密。通过这种方式,能够保证文件下载指令和待下载文件的文件名以及待下载文件数据在客户端、服务器以及传输过程中均是加密的,只有通过存储终端解密才能得到该文件下载指令和待下载文件的文件名以及待下载文件数据的明文,保证了文件下载的安全性。

[0343] 除了文件上传方法和文件下载方法,本发明实施例的文件管理方法还可以包括采

用存储终端删除云存储系统中服务器上的文件的方法。

[0344] 实施例四

[0345] 本发明实施例四提供一种云存储系统的文件删除方法,图 16 示出了该方法的流程图,该方法可以包括以下步骤:

[0346] 步骤 S1601:存储终端接收待删除文件的文件名 Z(包括待删除文件的组名和/或文件的网络名);

[0347] 步骤 S1602:存储终端产生文件删除指令;

[0348] 步骤 S1603:存储终端将文件删除指令和待删除文件的文件名 Z 加密,该加密过程可以采用本发明实施例一中的加密算法,也可以采用本领域其他常用的加密算法。

[0349] 步骤 S1604:存储终端将加密后的文件删除指令和待删除文件的文件名 Z 发送至客户端;

[0350] 步骤 S1605:客户端将加密后的文件删除指令和待删除文件的文件名 Z 和文件删除指令发送至服务器。

[0351] 步骤 S1606:服务器对客户端发送的加密后的文件删除指令和待删除文件的文件名 Z 解密,依据文件删除指令将对应文件删除指令和待删除文件的文件名 Z 中的文件数据删除。

[0352] 具体地,存储终端可以首先连接 Tracker 服务器依据待删除文件的文件名 Z 获取该待删除文件的地址,然后再连接 Storage 服务器依照文件删除指令和获取的该待删除文件的地址将存储在本地的与待删除文件的文件名对应的文件数据删除。

[0353] 另外,本发明实施例三提供的文件删除方法还可以包括以下步骤:

[0354] 步骤 S1607:服务器将删除成功信息加密,并将加密后的删除成功信息发送至客户端。

[0355] 步骤 S1608:客户端将服务器发送删除成功信息发送至存储终端。

[0356] 步骤 S1609:存储终端将客户端转发的删除成功信息解密。

[0357] 需要说明的是,在客户端读取文件删除指令和待删除文件的文件名(即步骤 S1602)之前,本发明实施例三中的文件删除方法还可以包括如本发明实施例二中的类似步骤,鉴于这些步骤可以由本发明实施例二中的对应步骤简单推导得出,在此对这些步骤不再赘述。

[0358] 本发明实施例三提供的文件删除方法,采用存储终端对文件删除指令和待删除文件的文件名进行加密,并在服务器依据该文件删除指令和待删除文件的文件名删除与其对应的待删除文件数据并将删除成功信息加密并返回客户端之后,采用存储终端对该删除成功信息解密。通过这种方式,能够保证文件删除指令和待删除文件的文件名以及删除成功信息在客户端、服务器以及传输过程中均是加密的,只有通过存储终端解密才能得到删除成功信息的明文,保证了文件删除过程的安全性。

[0359] 需要说明的是,本发明实施例中存储终端的所有操作(例如接收、加密及发送等操作)都可以通过外部设备控制存储终端完成,其中,该外部设备可以是本发明实施例的云存储系统中的客户端。以下以客户端控制存储终端完成接收、加密及发送等操作为例进行详细说明。

[0360] 实施例五

[0361] 客户端可以通过多种方式和存储终端通信,相应地,针对不同的通信方式,客户端也可以通过不同的方式控制存储终端完成接收、加密及发送等操作,以下以两个具体示例进行说明。

[0362] 第一示例:

[0363] 当客户端与存储终端通过以太网通信时,客户端控制存储终端完成接收、加密及发送等操作的方法的流程图如图 17 所示,该方法包括以下步骤:

[0364] 步骤 S1701:存储终端获取本地的桌面信息,其中该桌面信息可以包括存储终端的屏幕显示和声音;

[0365] 步骤 S1702:存储终端对获取的桌面信息进行视频编码以获得视频数据;

[0366] 步骤 S1703:存储终端将视频数据发送至客户端;

[0367] 步骤 S1704:客户端接收到存储终端发送的视频数据之后,解析该视频数据,并显示存储终端的桌面信息;

[0368] 步骤 S1705:客户端向存储终端发送鼠标键盘命令;

[0369] 步骤 S1706:存储终端接收到客户端发送的鼠标键盘命令后,依照该鼠标键盘命令做出响应,该响应可以包括接收、加密和 / 或发送操作响应。

[0370] 需要说明的是,本发明上述实施例提到的所有的存储终端执行的操作均可以由外部设备控制存储终端完成,另外,本发明上述实施例没有提到的一些操作也可以由外部设备控制存储终端完成,在此不再赘述。

[0371] 第二示例:

[0372] 本发明实施例中的存储终端可以通过 USB Device 接口客户端连接,通过 USB Mass storage 协议在客户端产生光盘盘符,光盘中含有客户端软件,通过 Auto run 自动运行。

[0373] 当客户端与存储终端通过 USB 接口通信时,客户端可以通过图 18 所示的方法控制存储终端完成接收、加密及发送等操作的方法的流程图,该方法包括以下步骤:

[0374] 步骤 S1801:存储终端接收客户端发送的控制命令,该控制命令可以用于控制存储终端启动获取本地的桌面信息的操作;

[0375] 存储终端在客户端出现光盘盘符,客户端软件运行后可以通过 USB 协议中的 SISI 私有命令和存储终端进行通信,具体地客户端软件可以向存储终端发送控制存储终端启动获取本地的桌面信息的 SISI 私有命令;

[0376] 步骤 S1802:存储终端获取本地的桌面信息,该桌面信息可以包括存储终端的屏幕显示和声音;;

[0377] 步骤 S1803:存储终端对获取的桌面信息进行视频编码,获得视频数据;

[0378] 步骤 S1804:存储终端将视频数据保存至视频文件队列,以等待将视频数据发送至客户端;

[0379] 步骤 S1805:存储终端接收客户端发送的该视频数据的获取请求;

[0380] 具体地,本发明实施例中,在执行步骤 S1805 之前,还可以包括以下步骤:存储终端向客户端发送请求发送视频数据的请求消息,当然,本发明的其他实施例中也可以不包括此步骤。

[0381] 步骤 S1806:存储终端依照客户端发送的视频数据的获取请求将视频数据发送至客户端;

[0382] 步骤 S1807:客户端对视频数据进行解析,显示存储终端的桌面信息;

[0383] 步骤 S1808:客户端向存储终端发送鼠标键盘命令;

[0384] 步骤 S1809:存储终端接收到客户端发送的鼠标键盘命令后,依照该鼠标键盘命令做出响应,该响应可以包括接收、加密和 / 或发送操作响应。

[0385] 具体地,客户端可以在本地播放存储终端的屏幕显示和声音,这样,可以在客户端对存储终端进行操作,完成接收、加密及发送等本发明实施例中提及和未提及的操作步骤。

[0386] 客户端向存储终端发送控制存储终端启动获取本地的桌面信息的命令后可以启动两个线程 M 和 N, M 线程可以通过 SISI 私有命令获取存储终端的视频数据,解析后播放,以此达到实时显示存储终端的桌面的目的;N 线程可以通过私有 SISI 命令将客户端的鼠标键盘命令发送到存储终端,存储终端收到鼠标键盘命令后做相应处理,以此实现通过控制存储终端完成各种操作的目的。

[0387] 本领域技术人员可以通过下述描述获知其他外部设备控制存储终端完成接收、加密及发送等操作的步骤,在此不再一一列举。

[0388] 本发明实施例中采用客户端控制存储终端完成接收、加密及发送等操作步骤,一方面能够在本地或者远程浏览或者操作存储终端,从而进一步提高云存储系统的安全性;另一方面能够为云存储系统提供一种方便快捷的操作方式。

[0389] 需要说明的是,本发明实施例中的控制存储终端完成各种操作的客户端也可以是其他外部设备,还可以是本地计算机,即可以通过本地计算机对与该本地计算机相连的存储终端进行各项操作。

[0390] 此外,本发明实施例还提供一种云存储系统的存储终端,以配合上述所有实施例中云存储系统的文件管理方法的实施,如图 19 所示,为该存储终端的结构示意图,该存储终端 1900 包括:

[0391] 第一接收单元 1901,用于接收文件信息;

[0392] 第一加密单元 1902,用于将第一接收单元接收的文件信息加密;

[0393] 第一发送单元 1903,用于将加密后的文件信息通过客户端发送至服务器。

[0394] 其中,文件信息可以为待上传文件的文件数据、待下载文件的文件名或者待删除文件的文件名。

[0395] 具体的,本发明云存储系统的存储终端各构成部分的相互关系及作用,以配合上述所有实施例中云存储系统的文件管理方法能够实施为准,详细内容请参考上述的方法实施例的描述,以下为存储终端的简述。

[0396] 另外,本发明实施例中的云存储系统的存储终端还可以包括:

[0397] 生成单元,用于生成操作指令;

[0398] 第二加密单元,用于将生成单元生成的操作指令加密;

[0399] 第二发送单元,用于将加密后的操作指令通过客户端转发至服务器;

[0400] 第二接收单元,用于接收客户端转发的由服务器加密并发送的处理结果信息;

[0401] 解密单元,用于将第二接收单元接收的处理结果信息解密;

[0402] 存储终端还可以包括主控单元、安全单元;

[0403] 主控单元,用于接收文件信息,并将该文件信息发送至安全单元;

[0404] 安全单元,用于对主控单元发送的文件信息加密,并将加密后的文件信息返回至

主控单元；

[0405] 存储终端还可以包括：

[0406] 第一验证单元，用于验证用户输入的身份识别码是否正确；

[0407] 存储终端还可以包括主控单元、安全单元和智能单元，

[0408] 主控单元，用于根据用户输入的身份识别码得到该身份识别码对应的第一触摸点坐标值，并将该第一触摸点坐标值发送至安全单元；

[0409] 安全单元，用于对该第一触摸点坐标值进行译码及加密运算，得到加密后的身份识别码，并将该加密后的身份识别码发送至智能单元；

[0410] 智能单元，用于对加密后的身份识别码进行验证；

[0411] 该存储终端还可以包括：

[0412] 认证单元，用于对存储终端和服务器进行交叉认证；

[0413] 获取单元，用于获取本地的桌面信息；

[0414] 编码单元，用于对该桌面信息进行视频编码以获得视频数据；

[0415] 第三发送单元，用于向客户端发送视频数据；

[0416] 第三接收单元，用于接收客户端发送的鼠标键盘命令；

[0417] 响应单元，用于依照第三接收单元接收的鼠标键盘命令做出响应，包括接收、加密及发送操作响应。

[0418] 第四接收单元，用于接收客户端发送的控制命令；

[0419] 第五接收单元，用于接收客户端发送的视频数据的获取请求。

[0420] 此外，本发明实施例还提供一种云存储系统，如图 2 所示，该云存储系统包括本发明上述实施例中的存储终端 201、客户端 202 和服务器 203，其中，

[0421] 存储终端 201 用于接收文件信息，将文件信息加密，并将加密后的文件信息发送至客户端 202；

[0422] 客户端 202 用于接收存储终端 201 发送的加密后的文件信息，并将加密后的文件信息发送至服务器 203；

[0423] 服务器 203 用于接收客户端 202 发送的加密后的文件信息。

[0424] 另外，

[0425] 服务器 203 还用于处理加密后的文件信息，产生处理结果信息并处理结果信息加密，并将加密后的处理结果信息发送至客户端 202；

[0426] 客户端 202 还用于接收服务器 203 发送的加密后的处理结果信息，并将加密后的处理结果信息发送至存储终端 201；

[0427] 存储终端 201 还用于接收客户端 202 发送的加密后的处理结果信息，并将加密后的处理结果信息解密。

[0428] 需要说明的是，本发明实施例中的文件信息可以为待上传文件的文件数据、待删除文件的文件名或者待下载文件的文件名，当文件信息为待下载文件的文件名时，相应的处理结果信息可以为待下载文件。

[0429] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

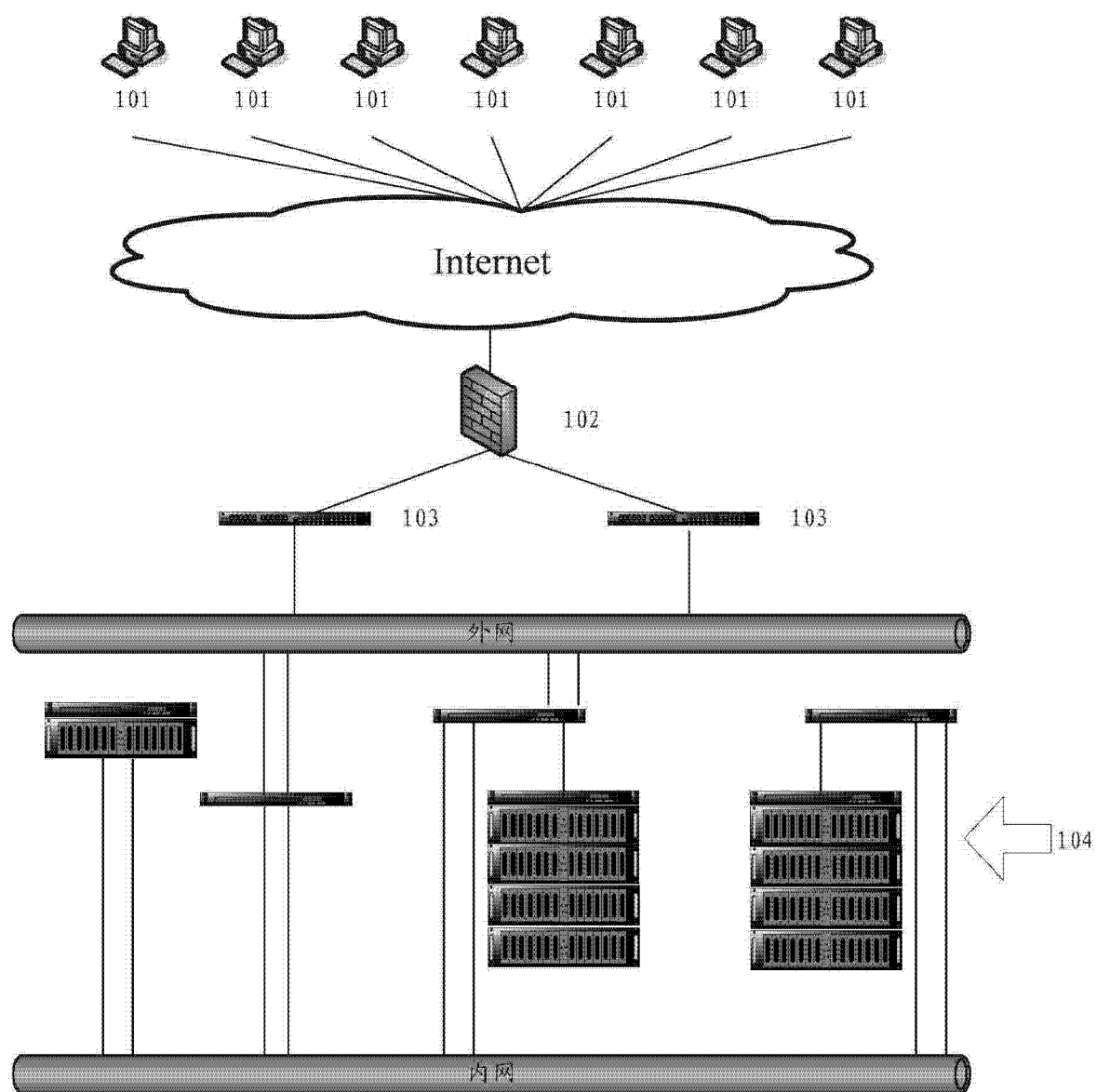


图 1

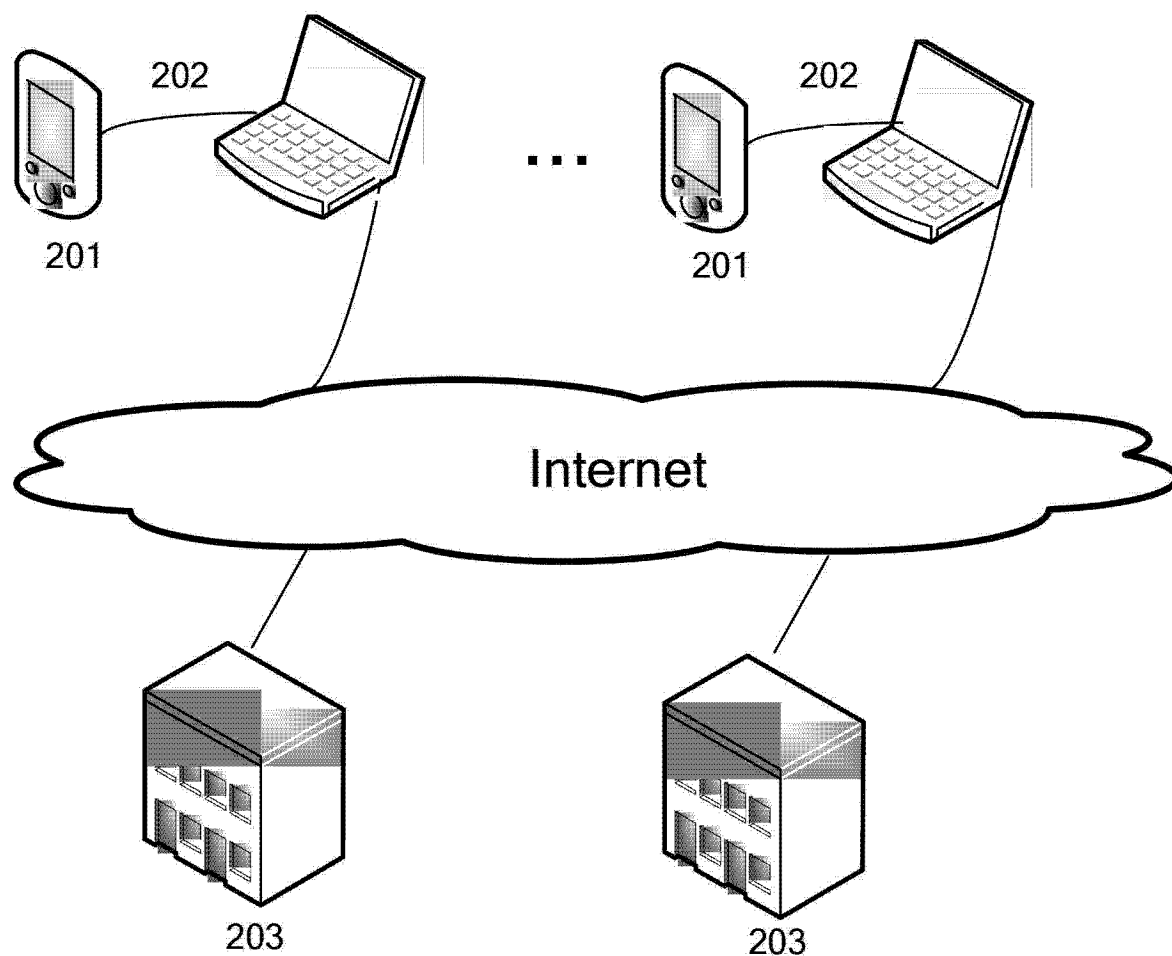


图 2

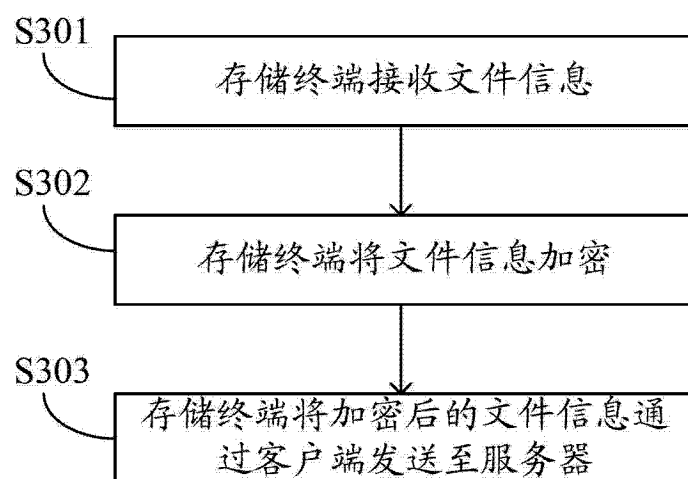


图 3

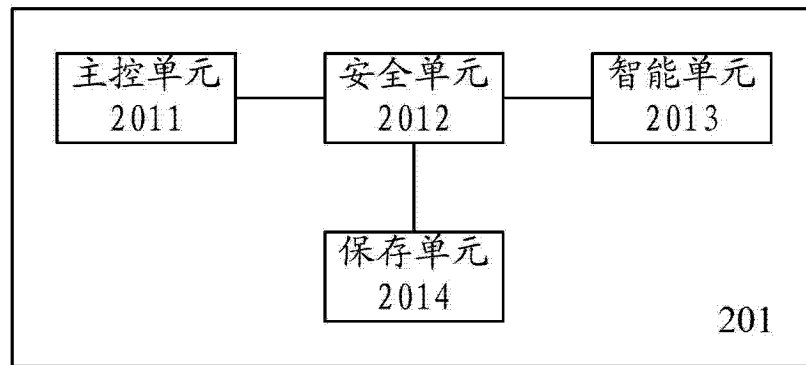


图 4

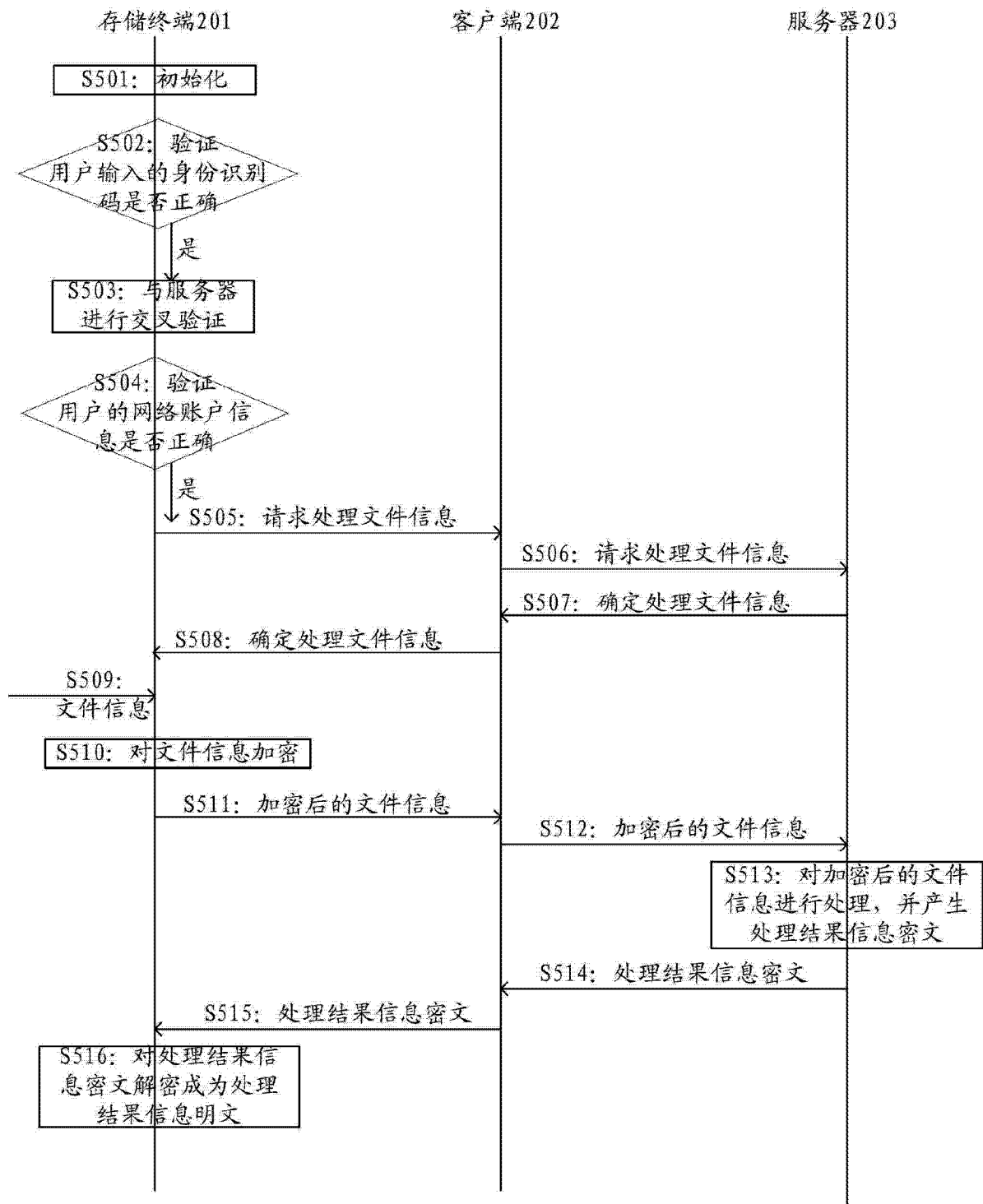


图 5

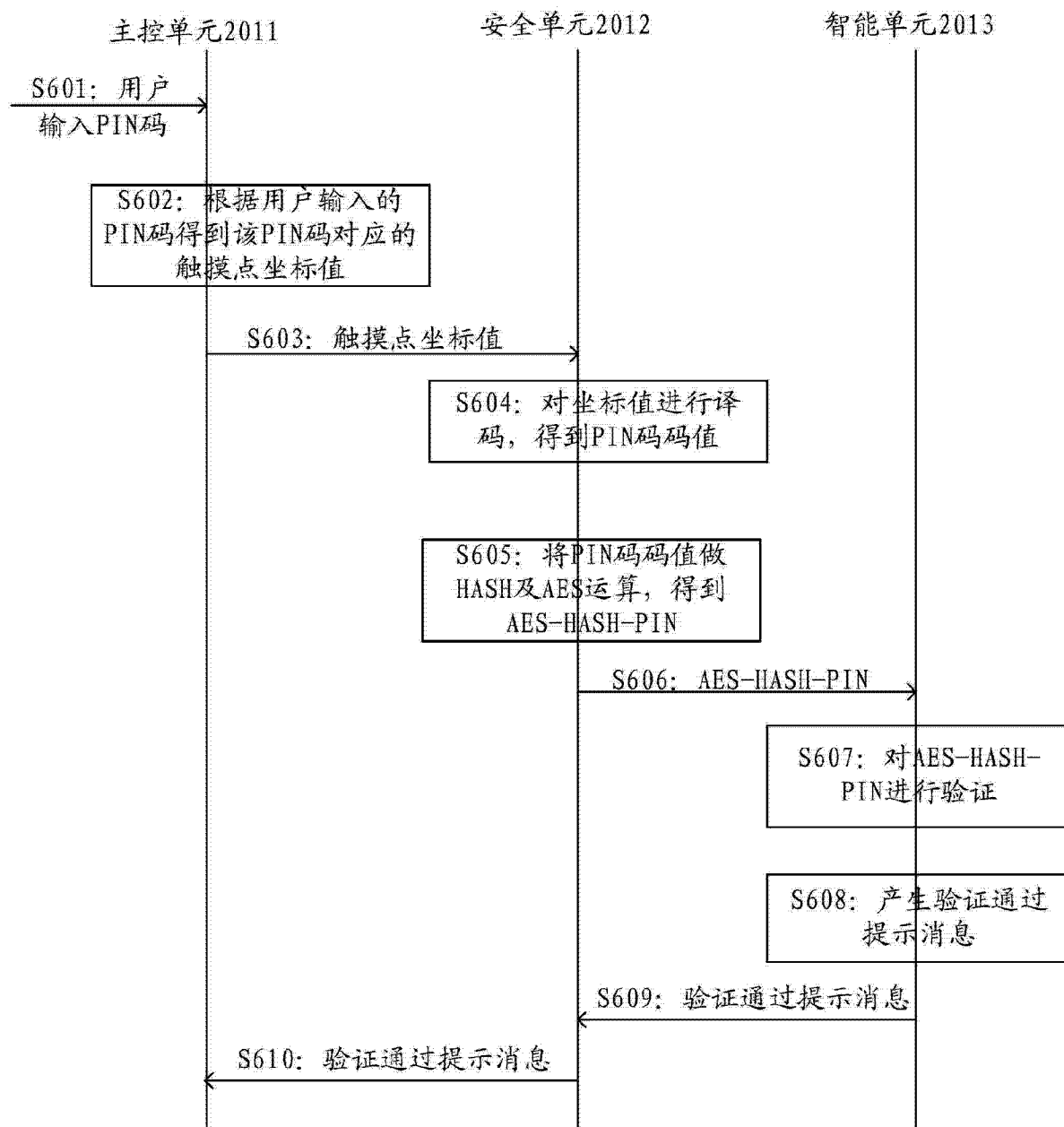


图 6

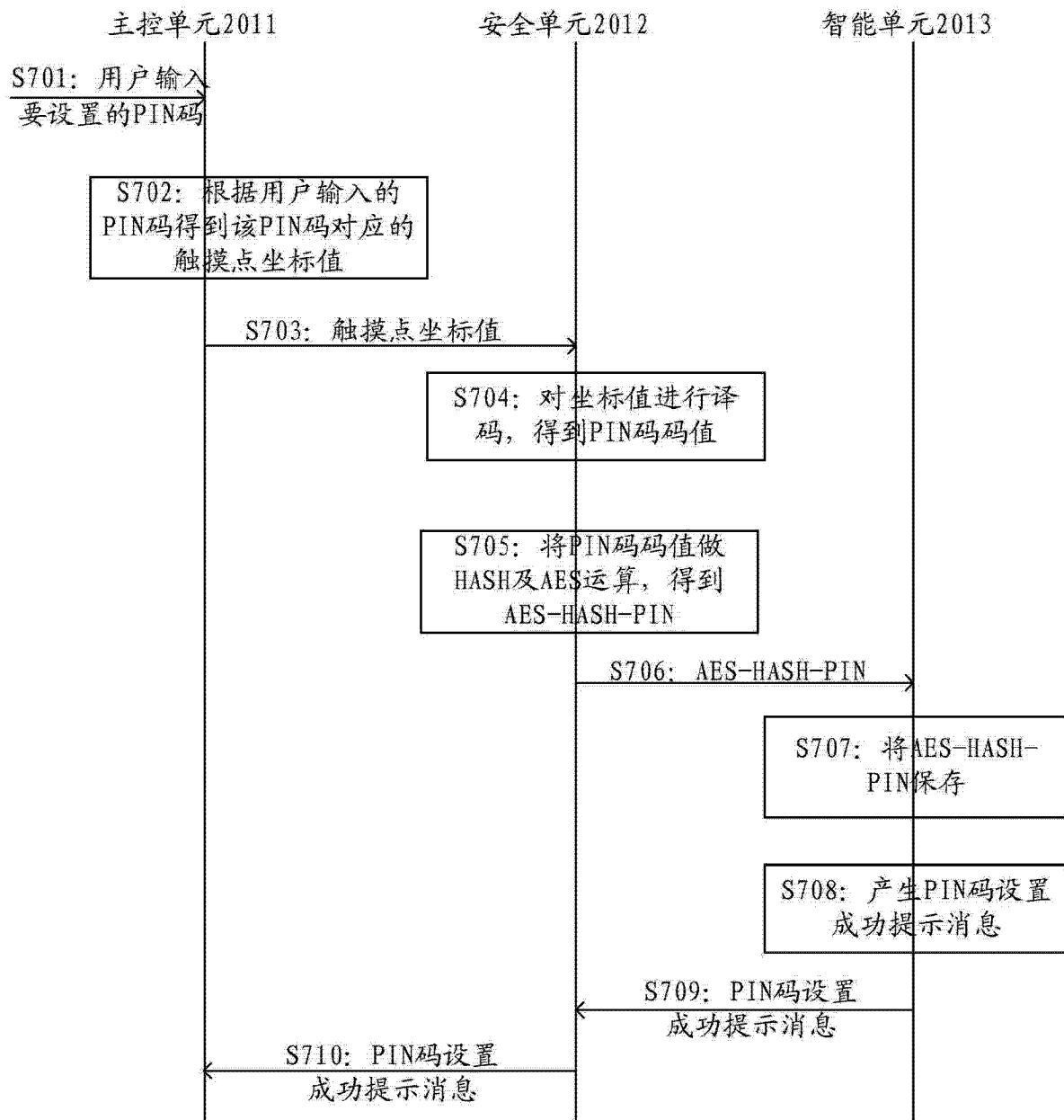


图 7

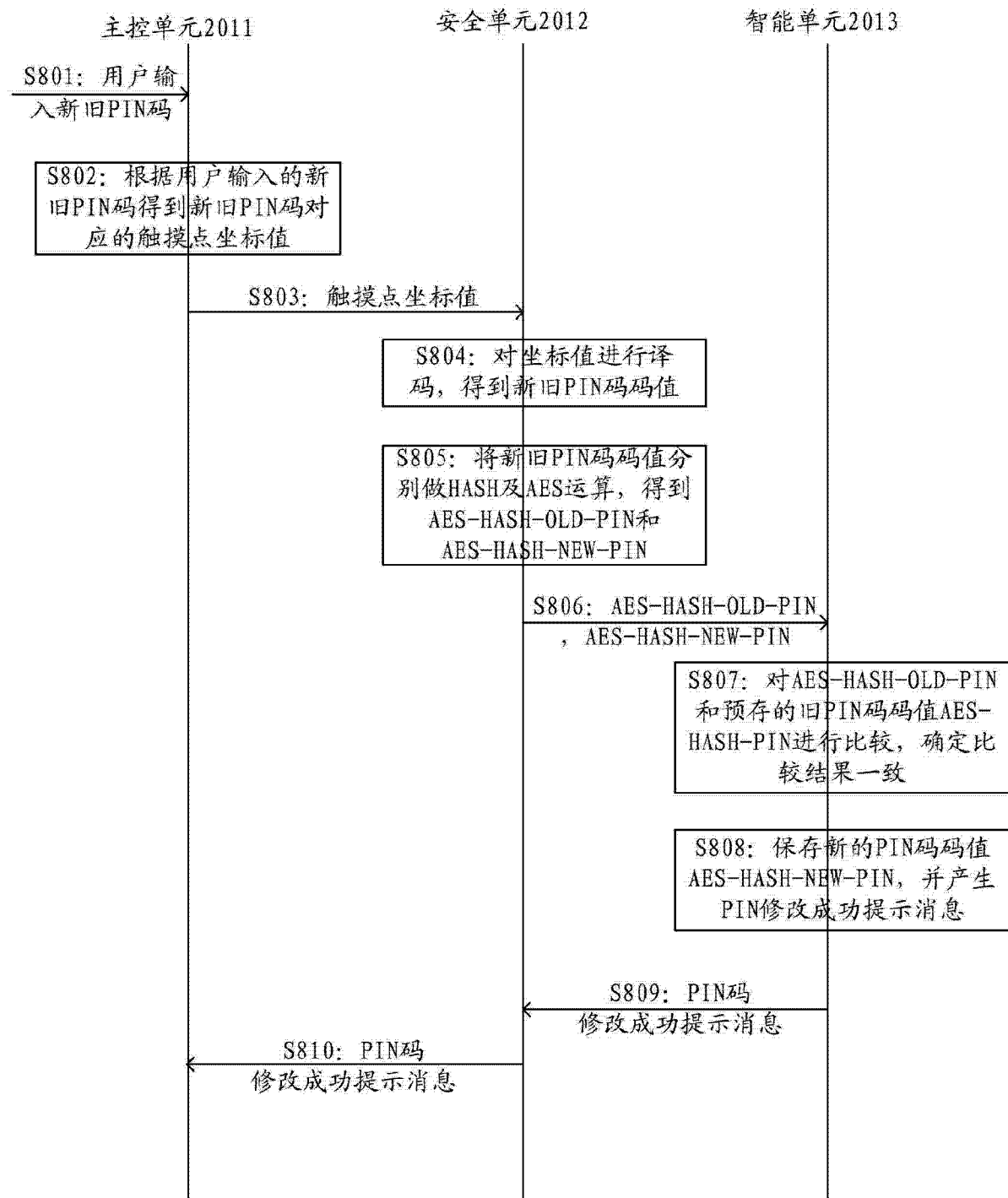


图 8

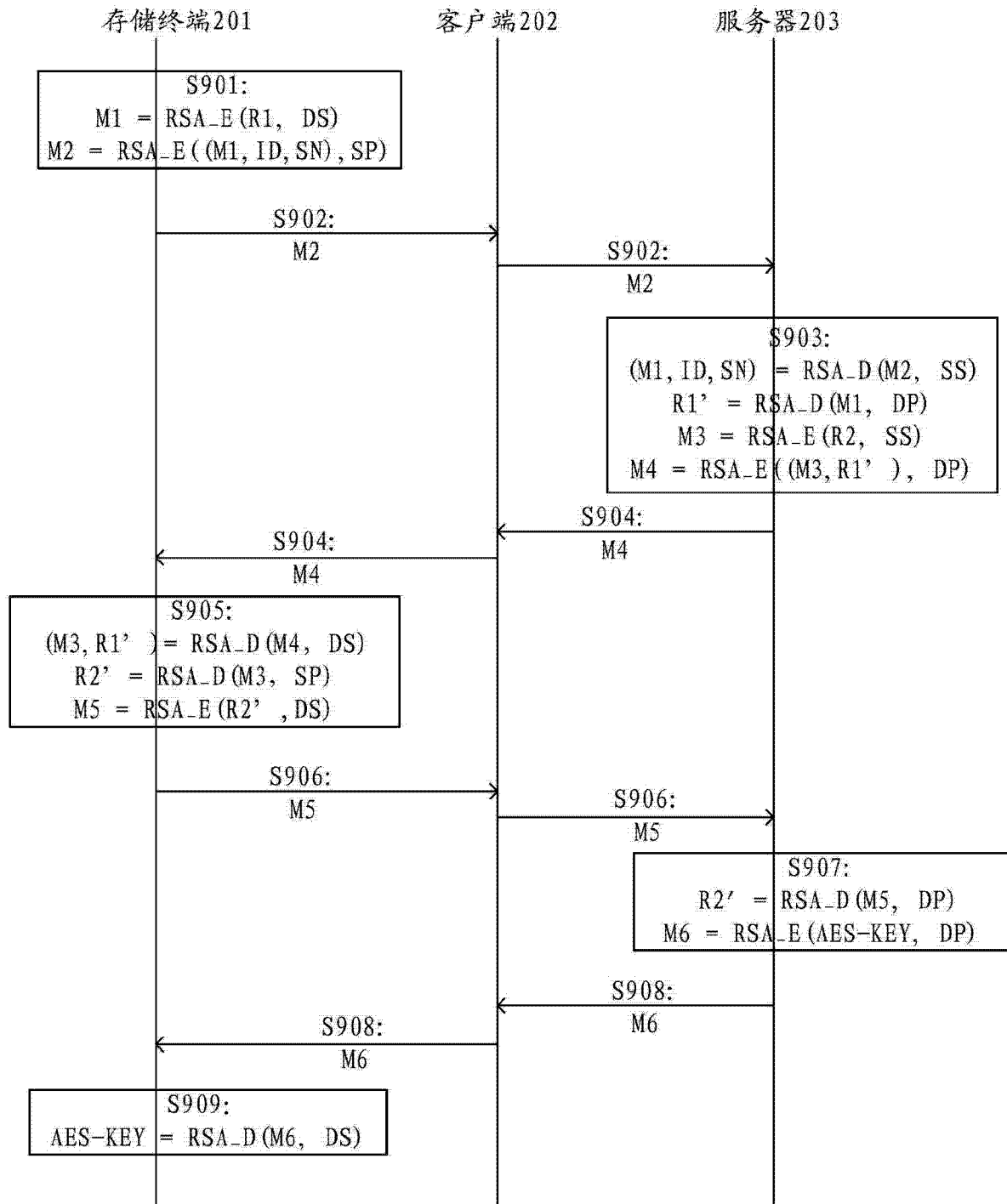


图 9

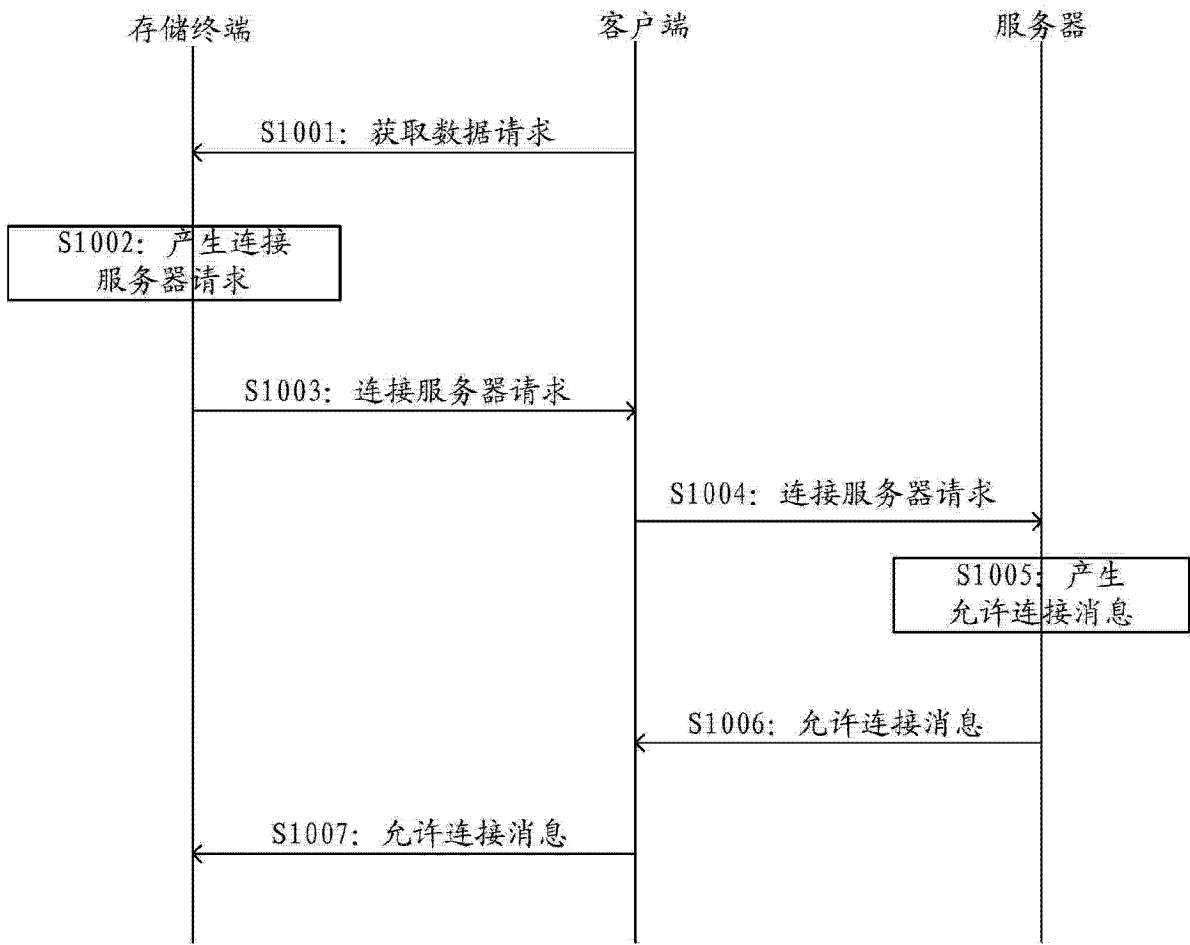


图 10

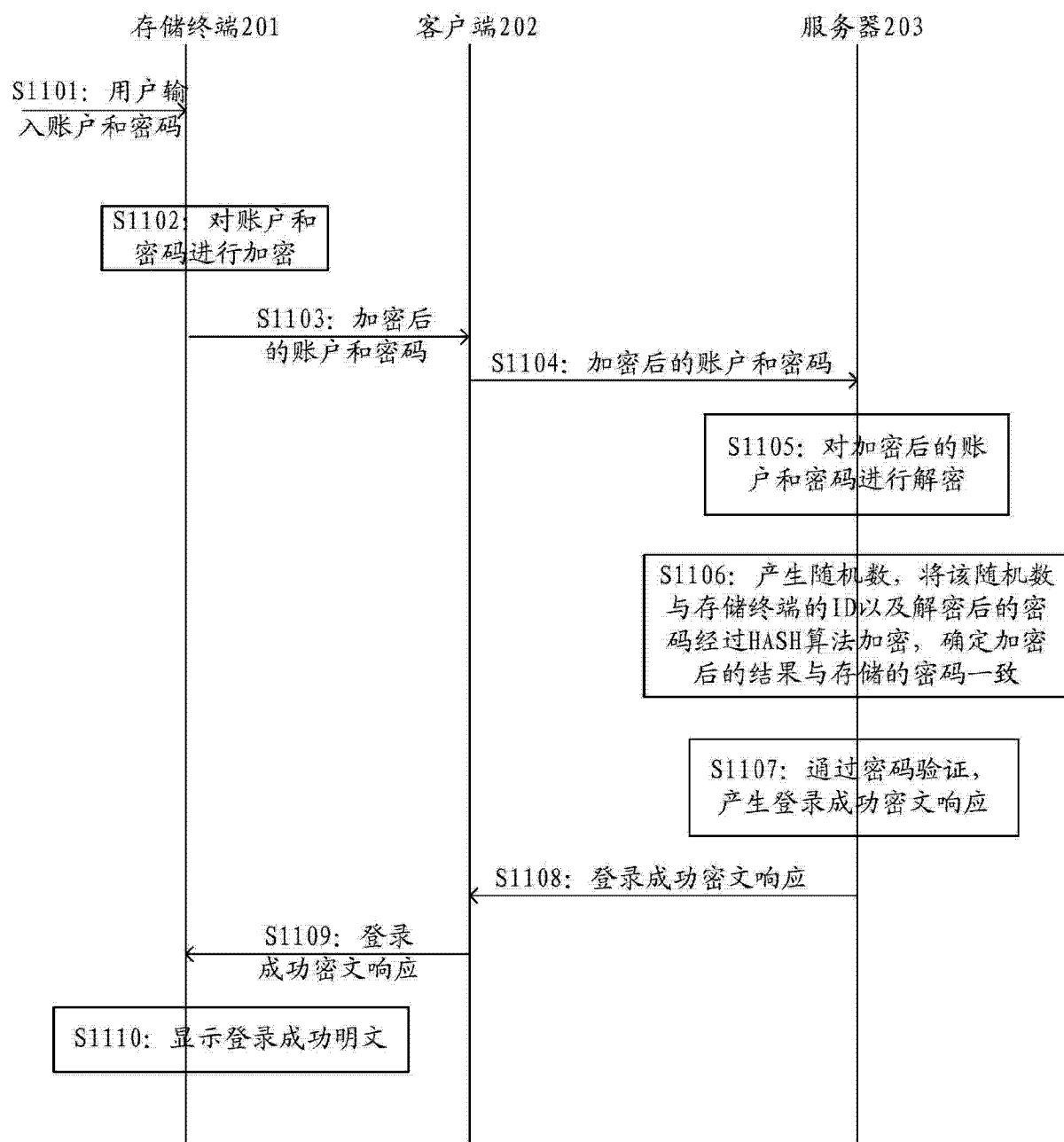


图 11

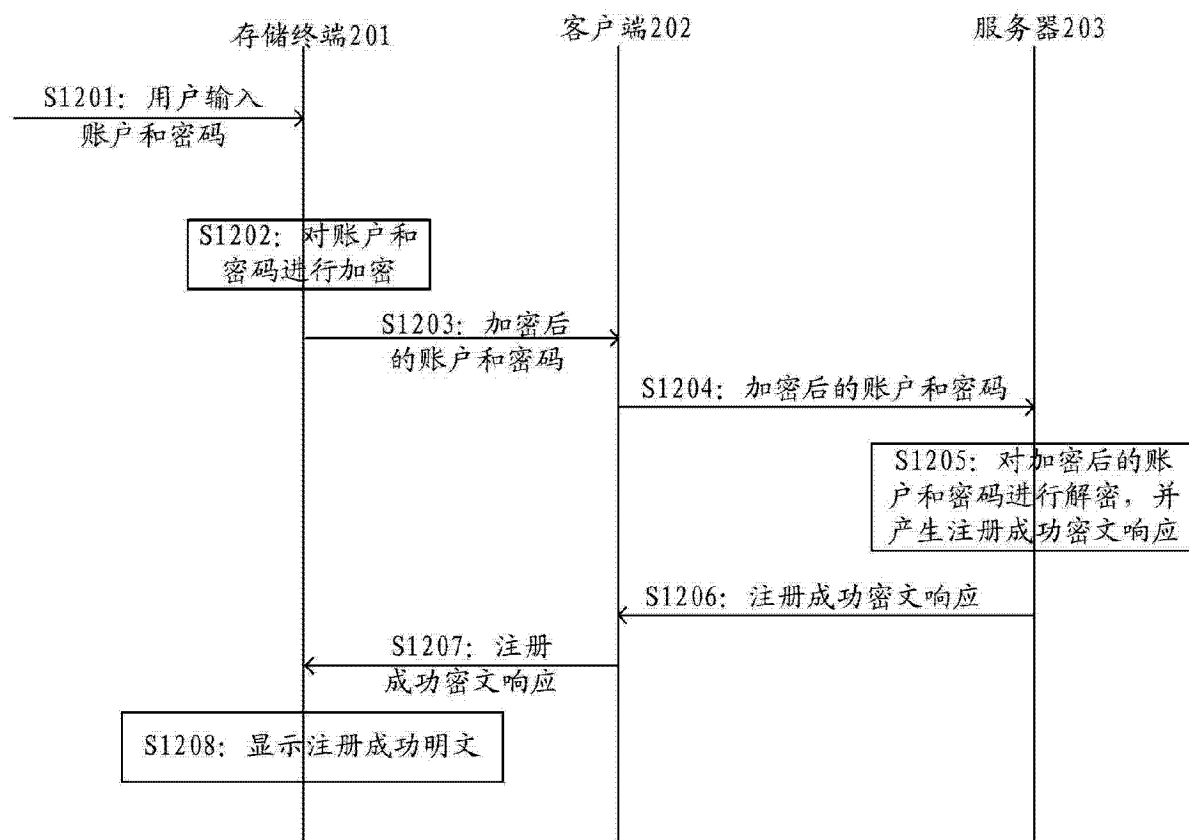


图 12

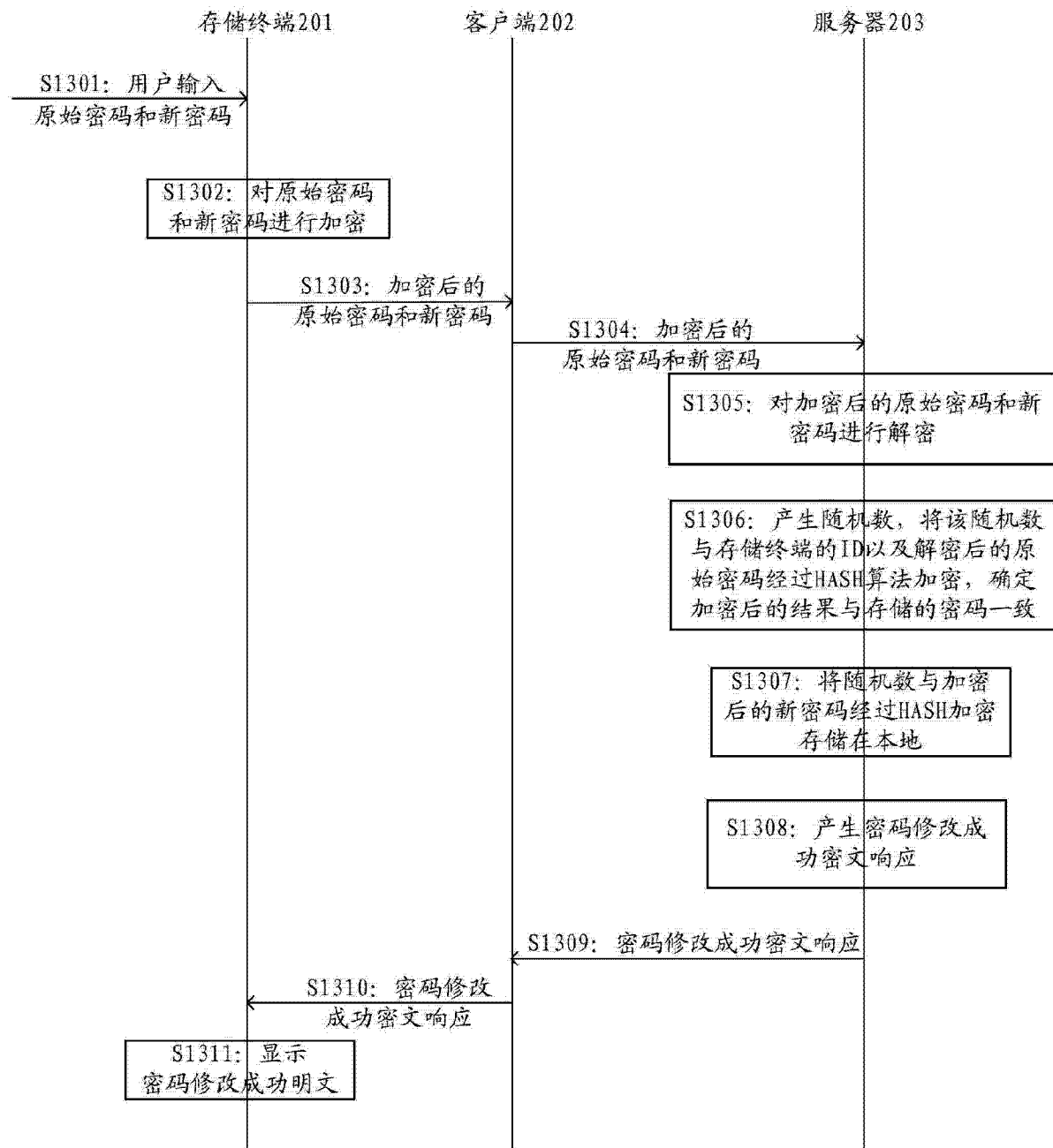


图 13

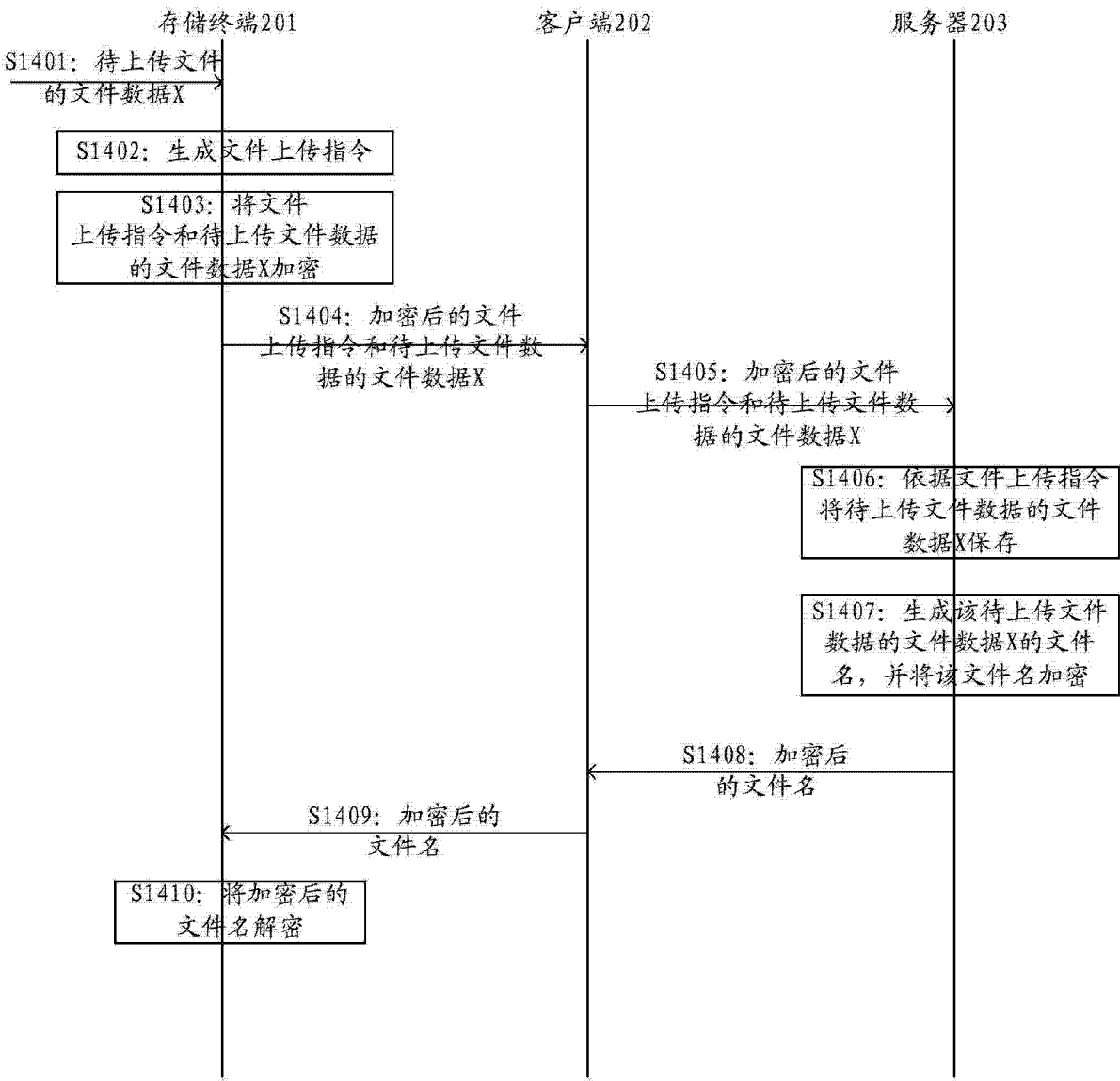


图 14

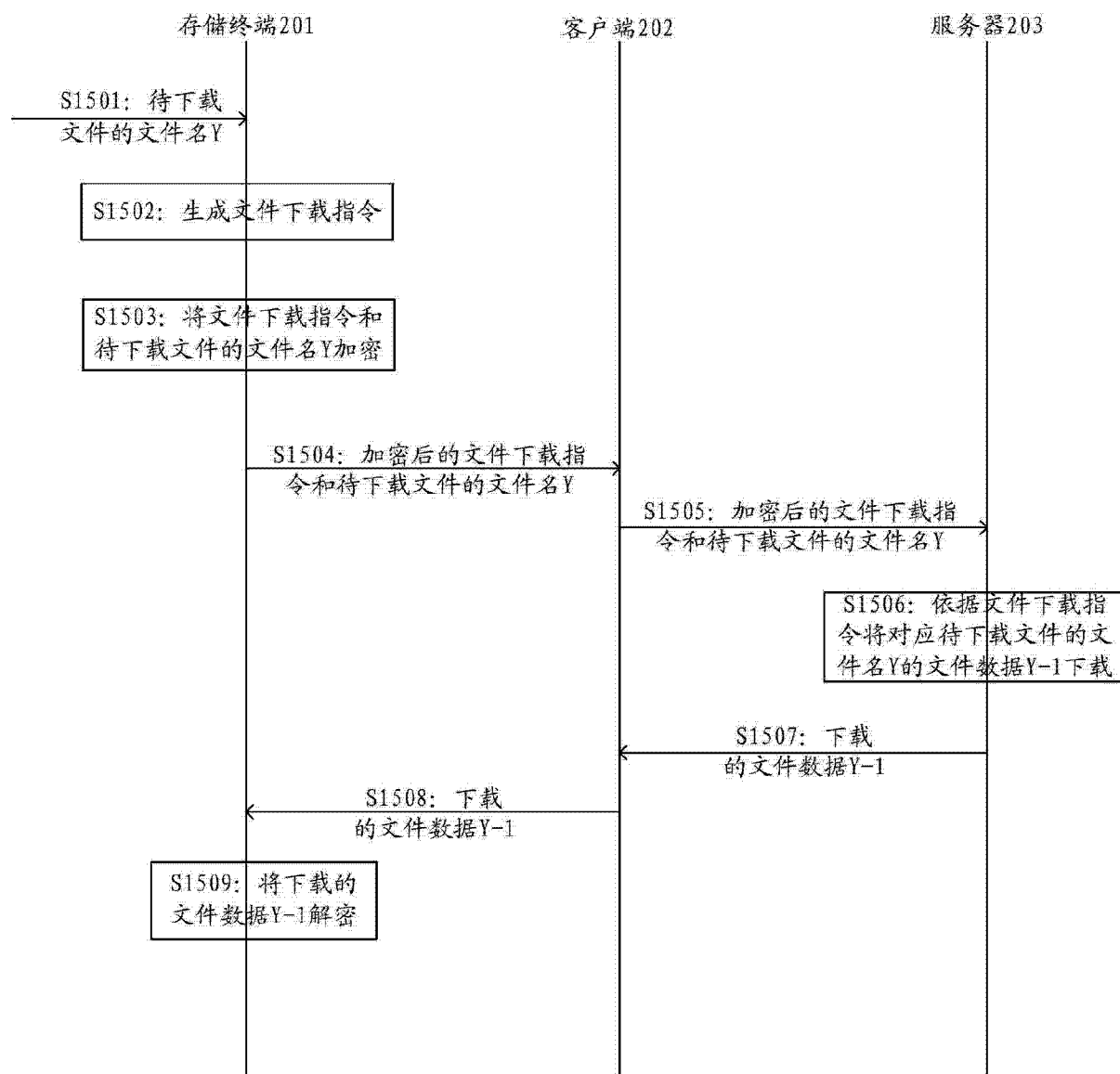


图 15

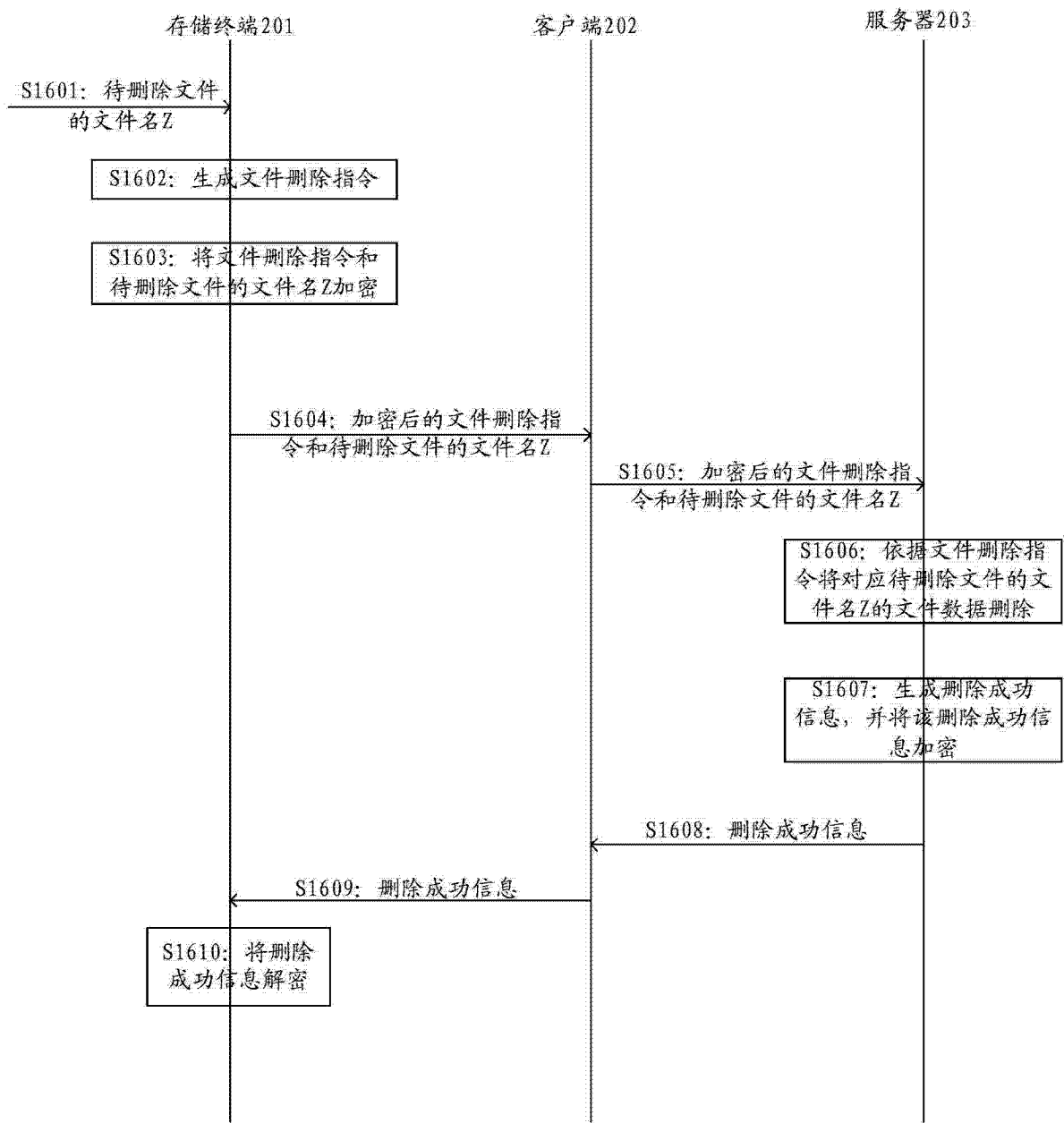


图 16

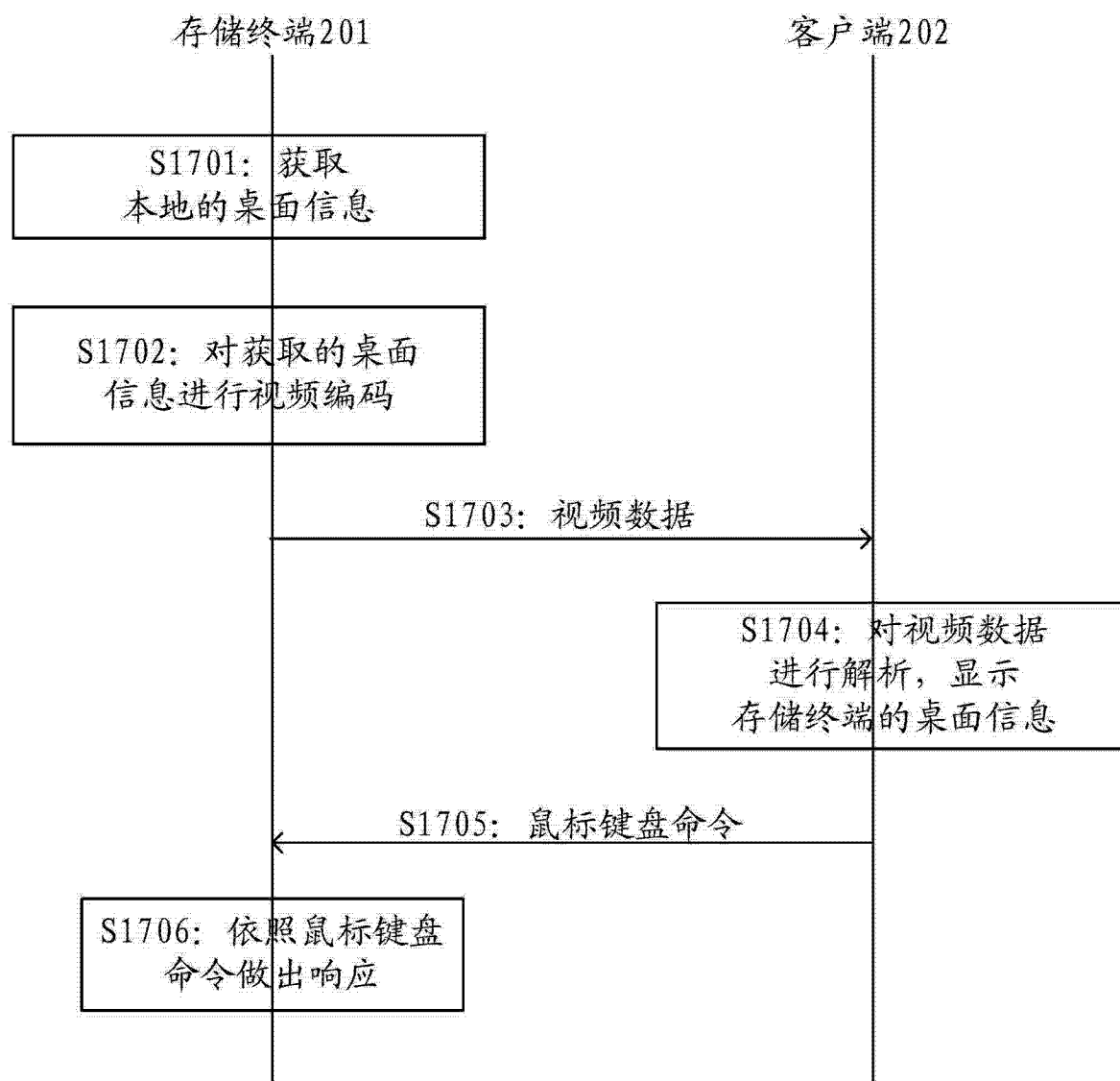


图 17

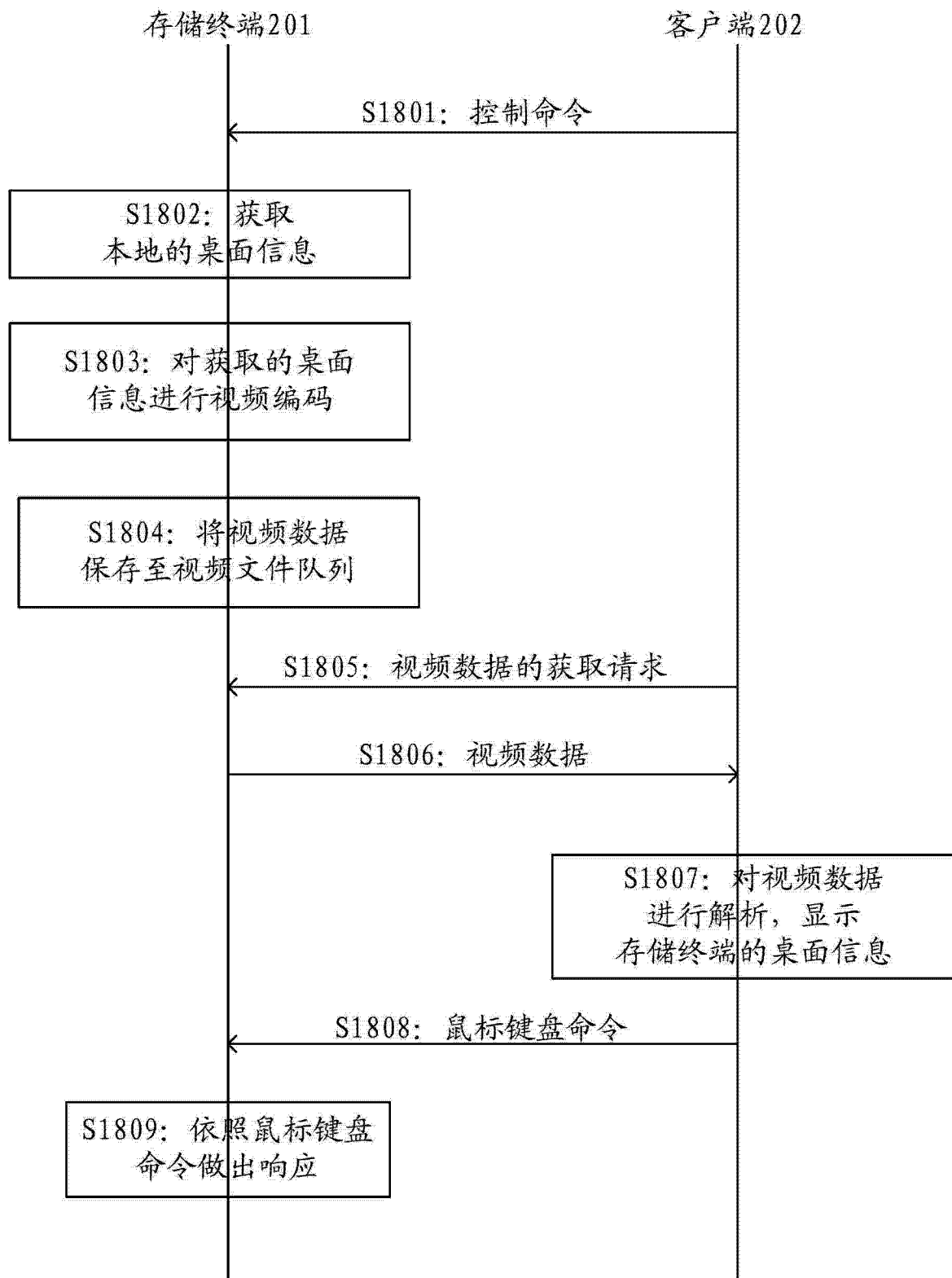


图 18

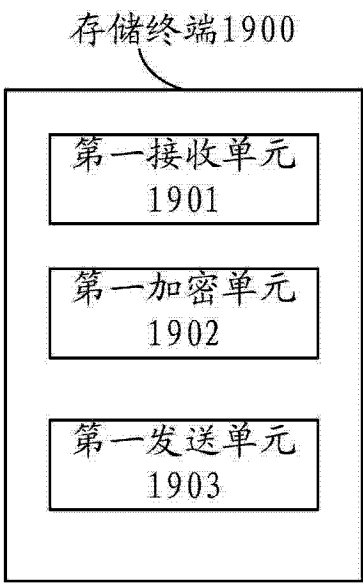


图 19