

(12) 发明专利

(10) 授权公告号 CN 101753539 B

(45) 授权公告日 2012.06.06

(21) 申请号 200810227900.4

H04L 12/56(2006.01)

(22) 申请日 2008.12.01

(56) 对比文件

CN 1567255 A, 2005.01.19, 全文.

(73) 专利权人 北京大学

CN 101247232 A, 2008.08.20, 全文.

地址 100871 北京市海淀区颐和园路 5 号

WO 2006/018874 A1, 2006.02.23, 全文.

专利权人 北大方正集团有限公司

审查员 张岩

北京方正电子政务信息科技有限公司

国家档案局档案科学技术研究所
国家档案局

(72) 发明人 王绪胜 王凡 杨汉强 马淑桂
刘伟晏

(74) 专利代理机构 北京同达信恒知识产权代理
有限公司 11291

代理人 郭润湘

(51) Int. Cl.

H04L 29/06(2006.01)

H04L 9/32(2006.01)

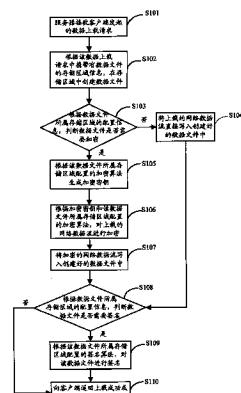
权利要求书 2 页 说明书 9 页 附图 4 页

(54) 发明名称

一种网络数据存储方法及服务器

(57) 摘要

本发明公开了一种网络数据存储方法及服务器，本发明提供烦扰网络数据存储方法包括：服务器根据数据文件所属存储区域的配置信息，判断数据文件是否需加密和 / 或是否需签名；当判断数据文件需加密不需签名时，对客户端上载的网络数据流进行加密，并将加密的网络数据流写入数据文件；当判断数据文件需签名不需加密时，将客户端上载的网络数据流写入数据文件，并对数据文件进行签名；当判断数据文件需要加密和签名时，对客户端上载的网络数据流进行加密，将加密的网络数据流写入数据文件，并对数据文件进行签名。本发明在保证数据存储的保密性和完整性的前提下，提高网络存储服务器的开放性、扩展性、健壮性和读 / 写访问效率。



1. 一种网络数据存储方法,其特征在于,包括:

服务器根据数据文件所属存储区域的配置信息,判断所述数据文件是否需加密和 / 或是否需签名;

当判断所述数据文件需加密不需签名时,对客户端上载的网络数据流进行加密,并将加密的所述网络数据流写入所述数据文件;

当判断所述数据文件需签名不需加密时,将所述客户端上载的网络数据流写入所述数据文件,对所述数据文件进行签名;

当判断所述数据文件需要加密和签名时,对所述客户端上载的网络数据流进行加密,将加密的网络数据流写入所述数据文件,对所述数据文件进行签名。

2. 如权利要求 1 所述的方法,其特征在于,还包括:

对预先划分的多个存储区域,分别配置其存储的数据文件是否需要加密以及加密算法和 / 或是否需要签名以及签名算法的参数信息;

所述对客户端上载网络数据流进行加密,包括:

根据所述数据文件所属存储区域配置的加密算法,生成加密密钥;

根据所述加密算法和生成的加密密钥,对客户端上载的网络数据流进行加密;

所述对数据文件进行签名,包括:

根据所述数据文件所属存储区域配置的签名算法,对所述数据文件进行签名。

3. 如权利要求 2 所述的方法,其特征在于,还包括:

对所述加密密钥进行加密;

将所述加密算法、加密后的加密密钥和 / 或所述签名算法、签名结果生成密钥文件并存储;所述密钥文件与所述数据文件一一对应。

4. 如权利要求 3 所述的方法,其特征在于,还包括:

所述服务器根据客户端请求下载的数据文件对应的密钥文件,判断所述数据文件是否已加密和 / 或是否已签名;

当判断所述数据文件已加密未签名时,对所述数据文件的数据流进行解密,并将解密的所述数据流输出到所述客户端;

当判断所述数据文件已签名未加密时,对所述数据文件验证签名,并在验证通过后,将所述数据文件的数据流输出到所述客户端;

当判断所述数据文件已签名且已加密时,对所述数据文件验证签名,并在验证通过后,对所述数据文件的数据流进行解密,将解密的数据流输出到所述客户端。

5. 如权利要求 4 所述的方法,其特征在于,所述对数据文件验证签名,包括:

根据所述数据文件对应的密钥文件中包含的签名算法和签名结果,对读取的数据文件验证签名;

所述对数据文件的数据流进行解密,包括:

将所述密钥文件中加密后的加密密钥进行解密,得到解密密钥;使用所述解密密钥和所述密钥文件中的加密算法对所述数据文件的数据流进行解密。

6. 一种网络存储服务器,其特征在于,包括:判断模块、加密模块、签名模块和配置信息存储模块;

所述判断模块,用于根据配置信息存储模块中存储的数据文件所属存储区域的配置信

息,判断所述数据文件是否需加密和 / 或是否需签名;

所述加密模块,用于当所述判断模块判断出所述数据文件需加密不需签名时,对客户端上载的网络数据流进行加密,并将加密的网络数据流写入所述数据文件;以及当所述判断模块判断出所述数据文件需加密和签名时,在对所述客户端上载的网络数据流进行加密并写入所述数据文件后,将所述数据文件传送至所述签名模块;

所述签名模块,用于当所述判断模块判断出所述数据文件需签名不需加密时,将所述客户端上载的网络数据流写入所述数据文件,并对所述数据文件进行签名;以及接收加密模块传送的数据文件,对接收的所述数据文件进行签名;

所述配置信息存储模块,用于存储各存储区域的配置信息。

7. 如权利要求 6 所述的服务器,其特征在于,还包括:配置模块,用于对预先划分的多个存储区域分别配置其存储的数据文件是否需要加密以及加密算法和 / 或是否需要签名以及签名算法的参数信息,并将配置的所述参数信息存储于所述配置信息存储模块中;

所述加密模块,还用于根据所述配置信息存储模块存储的所述数据文件所属存储区域配置的加密算法,生成加密密钥;根据所述加密算法和生成的加密密钥,对读取的网络数据流进行加密,生成加密的网络数据流;

所述签名模块,还用于根据所述配置信息存储模块存储的所述数据文件所属存储区域配置的签名算法,对数据文件进行签名。

8. 如权利要求 7 所述的服务器,其特征在于,还包括:

密钥文件生成模块,用于对所述加密密钥进行加密;以及将所述加密算法、加密后的加密密钥和 / 或所述签名算法、签名结果生成密钥文件,并与所述数据文件一一对应;

密钥文件存储模块,用于存储所述密钥文件。

9. 如权利要求 8 所述的服务器,其特征在于,还包括:验证模块和解密模块;

所述判断模块,还用于根据客户端请求下载的数据文件对应的密钥文件,判断请求下载的数据文件是否已加密和 / 或是否已签名;

所述验证模块,用于当所述判断模块判断所述数据文件已签名未加密时,对所述数据文件验证签名,并在验证通过后,将所述数据文件的数据流输出到所述客户端;以及当所述判断模块判断数据文件已签名且已加密时,对所述数据文件验证签名,并在验证通过后,将所述数据文件发送至所述解密模块;

所述解密模块,用于当所述判断模块判断所述数据文件已加密未签名时,对所述数据文件的数据流进行解密,并将解密的数据流输出到所述客户端;以及接收所述验证模块发送的数据文件,对接收的所述数据文件的数据流进行解密,将解密的数据流输出到所述客户端。

10. 如权利要求 9 所述的服务器,其特征在于,所述验证模块,还用于根据所述密钥文件中包含的签名算法和签名结果,对读取的数据文件验证签名;

所述解密模块,还用于对所述密钥文件中的加密后的加密密钥进行解密,得到解密密钥;使用所述解密密钥和所述密钥文件中的加密算法对所述数据文件的数据流进行解密。

一种网络数据存储方法及服务器

技术领域

[0001] 本发明涉及网络安全领域，尤其涉及一种网络数据存储方法及服务器。

背景技术

[0002] 随着 TCP/IP 网络技术的发展，文件传输协议 (File Transfer Protocol, FTP) 和万维网分布式创作和版本控制 (Web-based Distributed Authoring and Versioning, WEBDAV) 协议得到了越来越广泛的应用，服务器端利用 FTP 和 WEBDAV 协议为客户端提供网络存储，形成了支持标准协议的网络存储，使用者可以使用支持 FTP 或 WEBDAV 的客户端通过网络进行服务器侧文件读访问（下载网络数据）和写访问（上载网络数据）等操作。

[0003] 为实现支持 FTP 和 WEBDAV 协议的网络存储，往往会在服务器侧安装部署相应的服务器系统 (FTP 服务器和 WEBDAV 服务器)，现有的 FTP 服务器和 WEBDAV 服务器大多是基于服务器端的文件系统提供存储服务，而且文件采用明码存储，这种采用明码存储文件的方法无法保证数据的保密性和完整性。

[0004] 为了保证文件的保密性和完整性，现有的解决方案通常是在服务器端使用额外的专门的安全文件系统，安全文件系统将多个需要保密的文件加密后封装在底层文件系统的某个单一文件中，并在系统内部统一维护文件信息（如文件名、文件大小等）以及每个文件的密钥信息。采用安全文件系统作为 FTP 服务器和 WEBDAV 服务器的后台存储存在以下几个问题：

[0005] 1、安全文件系统一般是私有系统，没有统一的接口，开放性不足；

[0006] 2、整个安全文件系统的加密算法是固定的统一的，扩展性不足；

[0007] 3、由于安全文件系统内的所有文件都集中封装在底层文件系统的单一文件中，在读访问安全文件系统内的某个特定文件时，需要先从底层文件系统的单一文件中将该文件提取出来；在写访问安全文件系统内的某个特定文件时，需要将该文件写入底层文件系统的单一文件中，读 / 写访问效率较低。

[0008] 4、安全文件系统的加密算法相对固定，且安全文件系统将内部的文件信息和密钥集中管理，存储文件信息或密钥部分的区域（磁盘扇区）发生损坏，会导致整个安全文件系统发生无法访问，系统健壮性不足。

发明内容

[0009] 本发明提供了一种网络数据存储方法及服务器，用以在保证数据存储的保密性和完整性的前提下，提高网络存储服务器的开放性、扩展性、健壮性和读 / 写访问效率。

[0010] 本发明实施例提供的一种网络数据上载方法，包括：

[0011] 服务器根据数据文件所属存储区域的配置信息，判断所述数据文件是否需加密和 / 或是否需签名；

[0012] 当判断所述数据文件需加密不需签名时，对客户端上载的网络数据流进行加密，并将加密的所述网络数据流写入所述数据文件；

- [0013] 当判断所述数据文件需签名不需加密时,将所述客户端上载的网络数据流写入所述数据文件,对所述数据文件进行签名;
- [0014] 当判断所述数据文件需要加密和签名时,对所述客户端上载的网络数据流进行加密,将加密的网络数据流写入所述数据文件,对所述数据文件进行签名。
- [0015] 对预先划分的多个存储区域,分别配置其存储的数据文件是否需要加密以及加密算法和 / 或是否需要签名以及签名算法的参数信息;
- [0016] 所述对客户端上载网络数据流进行加密,包括:
- [0017] 根据所述数据文件所属存储区域配置的加密算法,生成加密密钥;
- [0018] 根据所述加密算法和生成的加密密钥,对客户端上载的网络数据流进行加密;
- [0019] 所述对数据文件进行签名,包括:
- [0020] 根据所述数据文件所属存储区域配置的签名算法,对所述数据文件进行签名。
- [0021] 对所述加密密钥进行加密;
- [0022] 将所述加密算法、加密后的加密密钥和 / 或所述签名算法、签名结果生成密钥文件并存储;所述密钥文件与所述数据文件一一对应。
- [0023] 所述服务器根据客户端请求下载的数据文件对应的密钥文件,判断所述数据文件是否已加密和 / 或是否已签名;
- [0024] 当判断所述数据文件已加密未签名时,对所述数据文件的数据流进行解密,并将解密的所述数据流输出到所述客户端;
- [0025] 当判断所述数据文件已签名未加密时,对所述数据文件验证签名,并在验证通过后,将所述数据文件的数据流输出到所述客户端;
- [0026] 当判断所述数据文件已签名且已加密时,对所述数据文件验证签名,并在验证通过后,对所述数据文件的数据流进行解密,将解密的数据流输出到所述客户端。
- [0027] 所述对数据文件验证签名,包括:
- [0028] 根据所述数据文件对应的密钥文件中包含的签名算法和签名结果,对读取的数据文件验证签名;
- [0029] 所述对数据文件的数据流进行解密,包括:
- [0030] 将所述密钥文件中加密后的加密密钥进行解密,得到解密密钥;使用所述解密密钥和所述密钥文件中的加密算法对所述数据文件的数据流进行解密。
- [0031] 本发明实施例提供的一种网络存储服务器,包括:判断模块、加密模块、签名模块和配置信息存储模块;
- [0032] 所述判断模块,用于根据配置信息存储模块中存储的数据文件所属存储区域的配置信息,判断所述数据文件是否需加密和 / 或是否需签名;
- [0033] 所述加密模块,用于当所述判断模块判断出所述数据文件需加密不需签名时,对客户端上载的网络数据流进行加密,并将加密的网络数据流写入所述数据文件;以及当所述判断模块判断出所述数据文件需加密和签名时,在对所述客户端上载的网络数据流进行加密并写入所述数据文件后,将所述数据文件传送至所述签名模块;
- [0034] 所述签名模块,用于当所述判断模块判断出所述数据文件需签名不需加密时,将所述客户端上载的网络数据流写入所述数据文件,并对所述数据文件进行签名;以及接收加密模块传送的数据文件,对接收的所述数据文件进行签名;

- [0035] 所述配置信息存储模块,用于存储各存储区域的配置信息。
- [0036] 本发明实施例提供的网络存储服务器,还包括:
- [0037] 配置模块,用于对预先划分的多个存储区域分别配置其存储的数据文件是否需要加密以及加密算法和 / 或是否需要签名以及签名算法的参数信息,并将配置的所述参数信息存储于所述配置信息存储模块中。
- [0038] 所述加密模块,还用于根据所述配置信息存储模块存储的所述数据文件所属存储区域配置的加密算法,生成加密密钥;根据所述加密算法和生成的加密密钥,对读取的网络数据流进行加密,生成加密的网络数据流;
- [0039] 所述签名模块,还用于根据所述配置信息存储模块存储的所述数据文件所属存储区域配置的签名算法,对数据文件进行签名。
- [0040] 本发明实施例提供的网络存储服务器,还包括:
- [0041] 密钥文件生成模块,用于对所述加密密钥进行加密;以及将所述加密算法、加密后的加密密钥和 / 或所述签名算法、签名结果生成密钥文件,并与所述数据文件一一对应;
- [0042] 密钥文件存储模块,用于存储所述密钥文件。
- [0043] 本发明实施例提供的网络存储服务器,还包括:验证模块和解密模块;
- [0044] 所述判断模块,还用于根据客户端请求下载的数据文件对应的密钥文件,判断请求下载的数据文件是否已加密和 / 或是否已签名;
- [0045] 所述验证模块,用于当所述判断模块判断所述数据文件已签名未加密时,对所述数据文件验证签名,并在验证通过后,将所述数据文件的数据流输出到所述客户端;以及当所述判断模块判断数据文件已签名且已加密时,对所述数据文件验证签名,并在验证通过后,将所述数据文件发送至所述解密模块;
- [0046] 所述解密模块,用于当所述判断模块判断所述数据文件已加密未签名时,对所述数据文件的数据流进行解密,并将解密的数据流输出到所述客户端;以及接收所述验证模块发送的数据文件,对接收的所述数据文件的数据流进行解密,将解密的数据流输出到所述客户端。
- [0047] 本发明实施例提供的网络存储服务器中的验证模块,还用于根据所述密钥文件中包含的签名算法和签名结果,对读取的数据文件验证签名;
- [0048] 本发明实施例提供的网络存储服务器中的解密模块,还用于对所述密钥文件中的加密后的加密密钥进行解密,得到解密密钥;使用所述解密密钥和所述密钥文件中的加密算法对所述数据文件的数据流进行解密。
- [0049] 本发明有益效果如下:
- [0050] 本发明实施例提供的一种网络数据存储方法及服务器,服务器接收客户端发起的数据上载请求,创建数据文件,根据数据文件所属存储区域的配置信息,对客户端上载的网络数据流进行加密,将加密后的网络数据流写入数据文件;或将上载的网络数据流写入数据文件后,对数据文件进行签名,或对客户端上载的网络数据流进行加密后,将加密后的网络数据流写入数据文件,并对数据文件进行签名。本发明实施例提供的网络存储方法及服务器,由于可以将数据文件分散存储于预先划分的多个存储区域中,避免了现有技术中的安全文件系统中所有加密的文件都存储于单一文件所带来的读 / 写访问的效率不高的问题;再者,由于不同存储区域的配置的加密和 / 或签名的参数信息可以不同,不仅提高了系

统的扩展性,还保证了网络存储数据的完整性和保密性。

[0051] 进一步地,本发明实施例提供的网络存储方法中,还将加密算法、加密后的加密密钥和 / 或签名算法、签名结果生成密钥文件,并与数据文件一一对应,某个数据文件的密钥文件被破解或损坏,不会对其他数据文件的安全造成影响,避免了现有网络存储服务器采用的安全文件系统将所有加密文件的密钥集中管理带来的弊端,进一步地提高了系统的健壮性。由于密钥文件的存在,使得数据文件的解密不依赖于所属存储区域的配置参数,因此随时可以根据需要修改存储区域的配置参数,进一步提高了系统的扩展性,还进一步保证了网络存储数据的完整性和保密性。

[0052] 发明实施例提供的网络数据存储方法,通过采用现有网络服务器操作系统自身的文件系统即可实现,由于操作系统的文件系统对上层系统而言具有统一的接口,保证了网络存储服务器的开放性。

附图说明

[0053] 图 1 为本发明实施例提供的网络数据存储方法中数据上载流程图;

[0054] 图 2 为本发明实施例提供的生成密钥文件的流程图;

[0055] 图 3 为本发明实施例提供的网络数据存储方法中数据下载流程图;

[0056] 图 4 为本发明实施例提供的网络存储服务器的结构示意图。

具体实施方式

[0057] 下面结合附图,以具体的实施例对本发明提供的一种网络数据存储方法及服务器进行详细的说明。

[0058] 本发明实施例提供的网络数据存储方法,针对服务器侧进行了改进。本发明实施例提供的网络数据存储方法可以应用于常见的网络存储服务器如 FTP 或 WEBDAV 服务器等,利用 FTP 或 WEBDAV 服务器现有操作系统提供的文件系统就可以实现,而不需要额外采用专门的安全文件系统作为网络数据的后台存储系统。这样,由于操作系统的文件系统对外的接口是统一的接口(例如标准的 FTP 或 WEBDAV 接口),保证了网络存储服务器的开放性。从读写访问的角度来说,直接访问服务器操作系统自身文件系统的效率,也优于通过服务器操作系统访问另外的安全文件系统的效率。

[0059] 本发明实施例提供的网络数据存储方法,可以预先将服务器本地的存储空间中划分多个存储区域,每个存储区域例如可以对应文件系统的一个目录,如“Server1/area1”、“Server1/area2”等等。还可以实现对存储区域增加、删除和修改等操作。

[0060] 并且,对于每个存储区域,需要预先对其中存储的数据文件是否需要加密以及加密算法和 / 或是否需要签名以及签名算法的参数信息分别进行配置,各个存储区域的配置信息是相互独立的,可以对不同的区域配置不同的加密算法和不同的签名算法,可以设置某一区域的数据文件仅加密不签名,而另外一个区域的数据文件不仅需要加密还需要进行签名,等等。在此不再枚举。在具体使用过程中,还可以根据需要,对存储区域的配置信息进行修改。

[0061] 下面结合客户端发起的网络数据上载流程,说明本发明实施例提供的网络数据存储方法。

- [0062] 本发明实施例提供的网络数据存储方法，如图 1 所示，包括以下步骤：
- [0063] 步骤 S101、服务器接收客户端发起的数据上载请求。
- [0064] 对于客户端来说，可以根据需要，请求将上载的数据流以文件的形式存储于服务器侧的任何一个存储区域中。
- [0065] 步骤 S102、服务器根据该数据上载请求中携带有数据文件的存储区域信息，在存储区域中创建数据文件。
- [0066] 客户端发送的数据上载请求中可以通过携带存储区域的统一资源定位标识(Uniform Resource Locator, URL) 来指示具体是哪个存储区域，例如“`ftp://Server1/area1`”、“`http://Server1/area2`”等。
- [0067] 步骤 S103、根据数据文件所属存储区域的配置信息，判断数据文件是否需要加密；若判断结果为否，执行步骤 S104，若是，执行步骤 S105；
- [0068] 步骤 S104、将上载的网络数据流直接写入创建好的数据文件中，然后执行步骤 S108。
- [0069] 步骤 S105、根据该数据文件所属存储区域配置的加密算法生成加密密钥。
- [0070] 本步骤 S105 中的加密密钥是随机实时生成的，在每次上载数据流的过程中生成的加密密钥都不相同。
- [0071] 步骤 S106、根据该数据文件所属存储区域配置的加密算法和步骤 S105 生成的加密密钥，对上载的网络数据流进行加密。
- [0072] 步骤 S107、将加密的网络数据流写入创建好的数据文件中。
- [0073] 步骤 S108、根据数据文件所属存储区域的配置信息，判断数据文件是否需要签名；若判断结果为是，执行步骤 S109，若否，跳转至步骤 S110。
- [0074] 步骤 S109、根据该数据文件所属存储区域配置的签名算法，对该数据文件进行签名。签名完成后，执行下述步骤 S110。
- [0075] 步骤 S110、向客户端返回上载成功的确认消息。
- [0076] 本发明实施例中，还可以在上述流程的基础上，增加生成密钥文件的流程，生成密钥文件的流程可以独立与图 1 所示的流程之外，也可以包含在图 1 所示的流程之中，与上述步骤 S101 至步骤 S110 合为一个整体的流程。为了说明地清楚，使用用图 2 的流程图进行示意。
- [0077] 如图 2 所示，本发明实施例中生成密钥文件的流程，包括以下步骤：
- [0078] 步骤 S201、根据数据文件所属存储区域的配置信息，判断数据文件是否需要加密和是否需要签名，当任一判断结果为是时，执行步骤 S202；若否，即判断该数据文件既不需要加密也并不需要签名时，直接跳转至步骤 S208 结束当前流程。
- [0079] 本步骤 S201 可以在图 1 所示的步骤 S104 或步骤 S107 之后，步骤 S108 之前执行。
- [0080] 步骤 S202、按照设定的数据文件和密钥文件的对应规则，创建密钥文件。
- [0081] 本发明实施例并不限定密钥文件采用何种具体类型，例如文本文件类型或关系数据库记录等。
- [0082] 步骤 S203、根据数据文件所属存储区域的配置信息，判断数据文件是否需要签名，若是，执行下述步骤 S204、若否，跳转至步骤 S206。
- [0083] 本步骤 S203 可以与图 1 中的步骤 S108 为同一个步骤。

- [0084] 步骤 S204、将签名算法、签名结果写入密钥文件。
- [0085] 本步骤 S204 可以在图 1 所示的步骤 S109 之后执行。
- [0086] 步骤 S205、根据数据文件所属存储区域的配置信息，判断数据文件是否需要加密，若是，执行步骤 S206、若否，直接执行步骤 S208。
- [0087] 步骤 S206、使用公钥对加密密钥进行加密。
- [0088] 服务器可以预先配置公私密钥对，在此步骤中使用配置的公钥对加密密钥进行加密。
- [0089] 步骤 S207、将加密算法、加密后的加密密钥写入密钥文件。
- [0090] 步骤 S208、结束流程。
- [0091] 本流程结束后，可以执行图 1 所示的最后一个步骤 S110。
- [0092] 本发明实施例中，在创建密钥文件时，可以采用预先设定的对应规则，将创建的密钥文件与数据文件之间一一对应，并且可以存储在同一个存储区域中。举例来说，密钥文件和数据文件的对应规则可以如下：
- [0093] 密钥文件的文件名可以采用数据文件的文件名加上特有的后缀组成。如下表所示：
- [0094] 表 1
- [0095]

文件名称	大小	类型
5-421. txt	3KB	文本文档
5-421. txt. cipher	1KB	CIPHER 文件
5-422. TIF	129KB	TIF 图像
5-422. TIF. cipher	1KB	CIPHER 文件

[0096] 上表 1 中，文件名为 5_421. txt 和 5_422. TIF 是数据文件，5_421. txt. cipher 和 5_422. TIF. cipher 分别是上述两个数据文件对应的密钥文件。

[0097] 显而易见，本发明实施例中，密钥文件和数据文件的对应规则并不局限于上述对应方式。

[0098] 在本发明实施例服务器侧的文件系统中，上述密钥文件的文件属性可以设置为隐藏，普通用户通过网络在服务器侧查找文件时，服务器侧不会显示相应的密钥文件。

[0099] 有权限的用户对服务器侧的数据文件进行修改或删除时，需要同时修改或删除其对应的密钥文件。

[0100] 与本发明实施例提供的网络存储方法中的网络数据上载流程相对应，当客户端发起网络数据下载请求时，本发明实施例提供的网络数据存储方法，在服务器侧处理流程，如图 3 所示，包括以下步骤：

[0101] 步骤 S301、服务器接收客户端发起的网络数据下载请求。

[0102] 步骤 S302、根据该请求中携带的该数据文件的 URL 和文件标识信息，在对应的存储领域中读取该数据文件。

[0103] 步骤 S303、根据该数据文件对应的密钥文件,判断该数据文件是否已签名,若是,执行步骤 S304 ;若否,执行步骤 S308。

[0104] 本步骤 S303 中,可以通过数据文件和密钥文件之间的对应规则,找到该数据文件对应的密钥文件,根据密钥文件中包含的具体内容来判断该数据文件是否签名(如果该密钥文件中仅包含了加密算法和加密后的加密密钥,那么可以判断该数据文件已加密未签名,如果该密钥文件中仅包含了签名算法和签名结果,那么可以判断该数据文件已签名未加密,如果该密钥文件中同时包含上述两类信息,那么可以判断该数据文件已加密并且已签名)。

[0105] 步骤 S304、根据该密钥文件中包含的签名算法和签名结果,对读取的数据文件验证签名。

[0106] 步骤 S305、判断验证是否通过;验证失败时,执行步骤 S306。验证通过时,执行步骤 S307。

[0107] 步骤 S306、向客户端返回出现错误的确认消息。

[0108] 步骤 S307、根据该数据文件对应的密钥文件,判断该数据文件是否已加密,若是,执行步骤 S308,若否,跳转至步骤 S310。

[0109] 步骤 S308、使用配置的私钥,对该密钥文件中的加密后的加密密钥进行解密,得到解密密钥。

[0110] 步骤 S309、使用步骤 S308 得到的解密密钥和该密钥文件中的加密算法,对数据文件的数据流进行解密,得到解密后的网络数据流。

[0111] 步骤 S310、将数据文件的数据流传输至客户端。

[0112] 步骤 S311、返回下载成功的确认消息。

[0113] 根据本发明实施例提供的网络数据存储方法,本发明实施例还提供了一种网络存储服务器,如图 4 所示,包括:判断模块 401、加密模块 402、签名模块 403 和配置信息存储模块 404 ;其中:

[0114] 判断模块 401,用于根据配置信息存储模块 404 中存储的该数据文件所属存储区域的配置信息,判断该数据文件是否需加密和 / 或是否需签名;

[0115] 加密模块 402,用于当判断模块 401 判断出数据文件需加密不需签名时,对客户端上载的网络数据流进行加密,并将加密的网络数据流写入该数据文件;以及当判断模块 401 判断出该数据文件需加密和签名时,在对读取的网络数据流进行加密并写入该数据文件后,将该数据文件传送至签名模块 403;

[0116] 签名模块 403,用于当判断模块 401 判断出该数据文件需签名不需加密时,将客户端上载的网络数据流写入该数据文件,并对该数据文件进行签名;以及接收加密模块 402 传送的数据文件,对接收的数据文件进行签名;

[0117] 配置信息存储模块 404,用于存储各存储区域的配置信息。

[0118] 本发明实施例提供的网络存储服务器,如图 4 所示,还可以包括:配置模块 405,用于对预先划分的多个存储区域分别配置其存储的数据文件是否需要加密以及加密算法和 / 或是否需要签名以及签名算法的参数信息,并将配置的参数信息存储于配置信息存储模块 404 中。

[0119] 加密模块 402,还用于根据配置信息存储模块 404 中存储的该数据文件所属存储

区域配置的加密算法,生成加密密钥;根据该加密算法和生成的加密密钥,对读取的网络数据流进行加密,生成加密的网络数据流;

[0120] 签名模块 403,还用于根据配置信息存储模块 404 存储的该数据文件所属存储区域配置的签名算法,对数据文件进行签名。

[0121] 本发明实施例提供的网络存储服务器,如图 4 所示,还可以包括:密钥文件生成模块 406 和密钥文件存储模块 407;

[0122] 密钥文件生成模块 406,用于使用公钥对加密密钥进行加密;以及将加密算法、加密后的加密密钥和 / 或所述签名算法、签名结果生成密钥文件,并与该数据文件一一对应;

[0123] 密钥文件存储模块 407,用于存储密钥文件。

[0124] 根据本发明实施例提供的一种网络数据存储方法中的网络数据下载流程,本发明实施例提供的网络存储服务器,如图 4 所示,还可以包括下面两个模块:验证模块 408 和解密模块 409;

[0125] 判断模块 401,还用于根据客户端请求下载的数据文件对应的密钥文件,判断请求下载的数据文件是否已加密和 / 或是否已签名;

[0126] 验证模块 408,用于当判断模块 401 判断该数据文件已签名未加密时,对该数据文件验证签名,并在验证通过后,将该数据文件的数据流输出到客户端;以及当判断模块 401 判断该数据文件已签名且已加密时,对该数据文件验证签名,并在验证通过后,将该数据文件发送至解密模块 409;

[0127] 解密模块 409,用于当判断模块 401 判断该数据文件已加密未签名时,对该数据文件的数据流进行解密,并将解密的数据流输出到客户端;以及接收验证模块 408 发送的数据文件,对接收的数据文件的数据流进行解密,将解密的数据流输出到客户端。

[0128] 本发明实施例提供的网络存储服务器中的验证模块 408,还用于根据该数据文件对应的密钥文件中包含的签名算法和签名结果,对读取的数据文件验证签名。

[0129] 解密模块 409,还用于使用私钥和密钥文件中包含的加密算法,对密钥文件中的加密后的加密密钥进行解密,得到解密密钥;使用解密密钥对该数据文件的数据流进行解密。

[0130] 本发明实施例提供的一种网络数据存储方法及服务器,服务器接收客户端发起的数据上载请求,创建数据文件,根据数据文件所属存储区域的配置信息,对客户端上载的网络数据流进行加密,将加密后的网络数据流写入数据文件;或将上载的网络数据流写入数据文件后,对数据文件进行签名,或对客户端上载的网络数据流进行加密后,将加密后的网络数据流写入数据文件,并对数据文件进行加密。当客户端请求进行网络数据下载时,相应地,根据数据文件所属存储区域的配置信息,对数据文件进行验证和 / 或解密的操作,将验证通过和 / 或解密后的文件数据流传送给客户端。

[0131] 本发明实施例提供的网络存储方法及服务器,由于可以将数据文件分散存储于预先划分的多个存储区域中,避免了现有技术中的安全文件系统中所有加密的文件都存储于同一个文件所带来的读 / 写访问的效率不高的问题;再者,由于不同存储区域的配置的加密和 / 或签名的参数信息可以不同,不仅提高了系统的扩展性,还进一步保证了网络存储数据的完整性和保密性。

[0132] 进一步地,本发明实施例提供的网络存储方法中,还将加密算法、加密后的加密密钥和 / 或签名算法、签名结果生成密钥文件并与数据文件一一对应,某个数据文件的密钥

文件被破解或损坏,不会对其他数据文件的安全造成影响,避免了现有网络存储服务器采用的安全文件系统将所有加密文件的密钥集中管理带来的弊端,进一步地提高了系统的健壮性。由于密钥文件的存在,使得数据文件的解密不依赖于所属存储区域的配置参数,因此随时可以根据需要修改存储区域的配置参数,进一步提高了系统的扩展性,还进一步保证了网络存储数据的完整性和保密性。

[0133] 另外,发明实施例提供的网络数据存储方法,可以直接采用现有网络服务器操作系统自身的文件系统进行数据的上载和下载的操作,由于操作系统的文件系统对上层系统而言具有统一的接口(例如标准的FTP或WEBDAV接口),保证了网络存储服务器的开放性。从读写访问的角度来说,直接访问服务器操作系统自身文件系统的效率,也优于通过服务器操作系统访问另外的安全文件系统的效率。

[0134] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

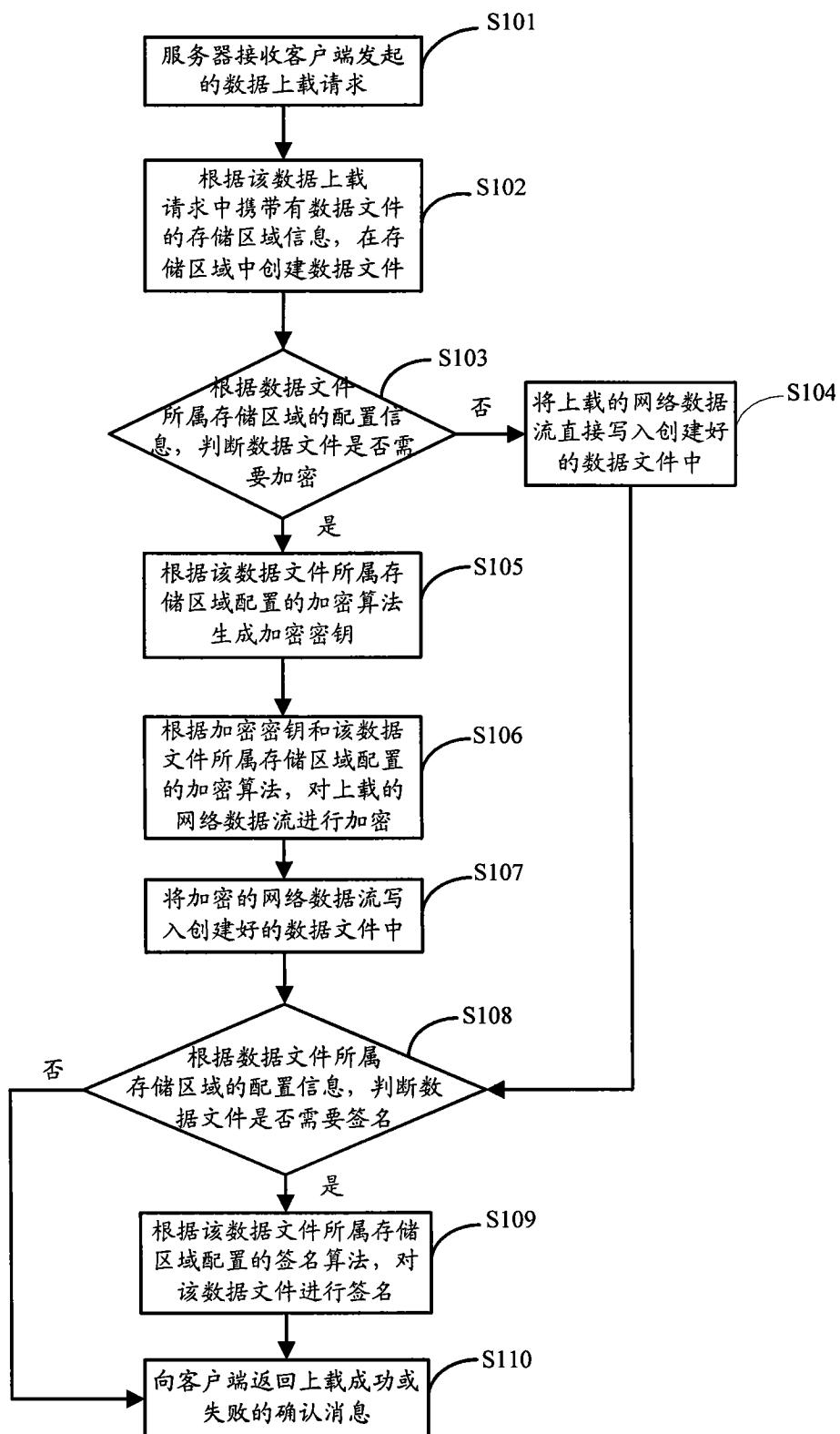


图 1

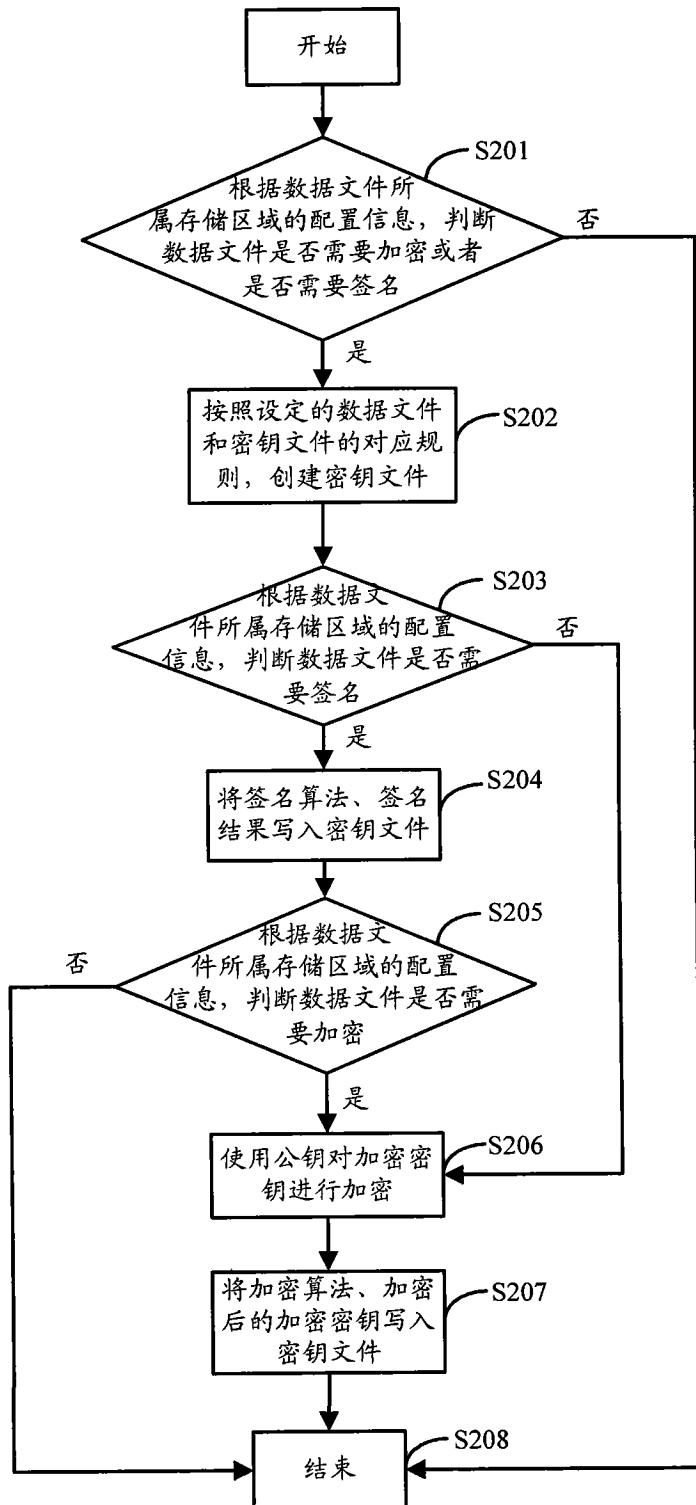


图 2

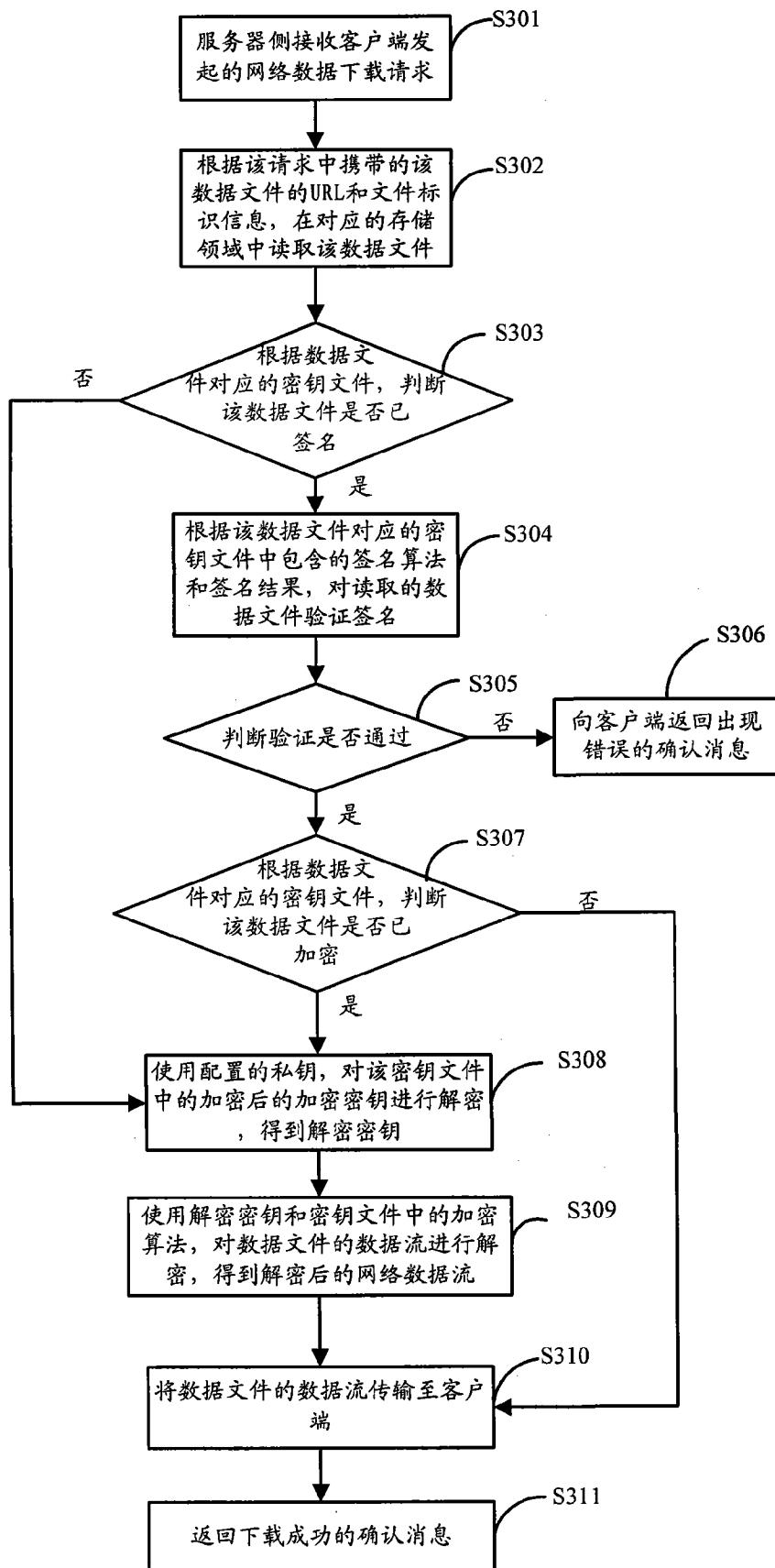


图 3

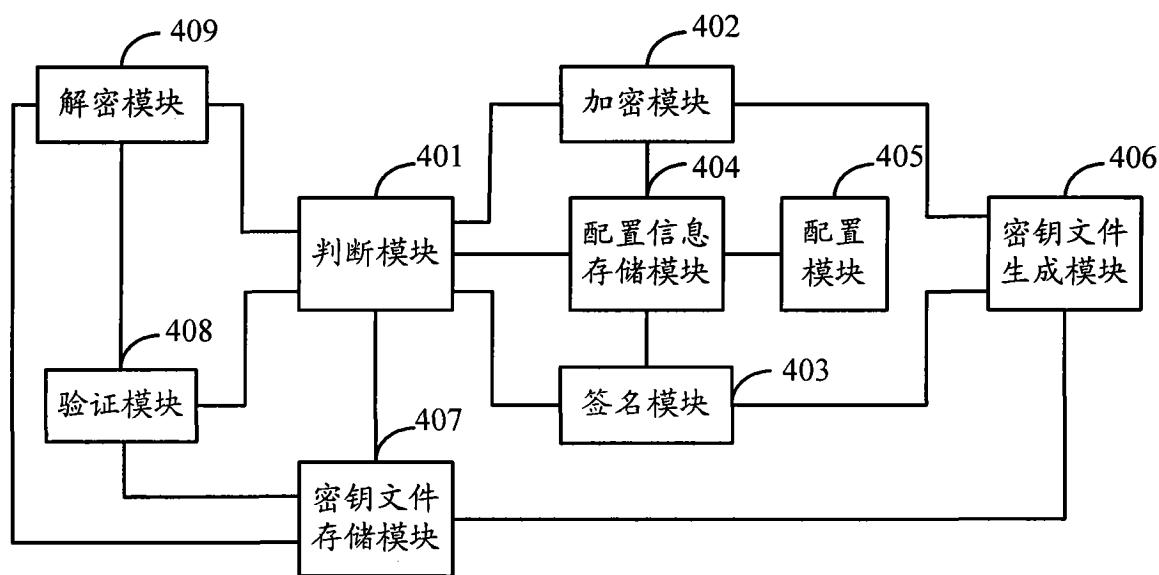


图 4