(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 106991332 A
(43)申请公布日 2017.07.28

(21)申请号 201710213681.3

(22)申请日 2017.04.01

(71)申请人 广东浪潮大数据研究有限公司
地址 510620 广东省广州市天河区黄埔大道西平云路163号A塔9层自编01单元

(72)发明人 聂东旭

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 罗满

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)

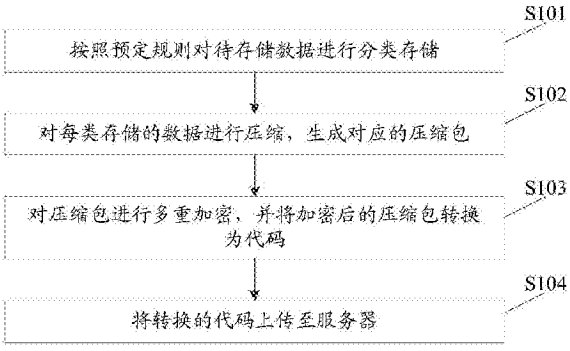
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种海量数据安全存储的方法及装置

(57)摘要

本发明公开了一种海量数据安全存储的方法，包括：按照预定规则对待存储数据进行分类存储；对每类存储的数据进行压缩，生成对应的压缩包；对压缩包进行多重加密，并将加密后的压缩包转换为代码；将转换的代码上传至服务器；可见，在本实施例中，通过多重方式高度加密，确保了数据的安全性，通过数据与代码的转换节约了磁盘空间，提高了存储量；本发明还公开了一种海量数据安全存储的装置，同样能实现上述技术效果。



CN 106991332 A

1.一种海量数据安全存储的方法，其特征在于，包括：

按照预定规则对待存储数据进行分类存储；

对每类存储的数据进行压缩，生成对应的压缩包；

对压缩包进行多重加密，并将加密后的压缩包转换为代码；

将转换的代码上传至服务器。

2.根据权利要求1所述的海量数据安全存储的方法，其特征在于，所述对压缩包进行多重加密，包括：

利用用户输入的身份信息对压缩包进行身份加密；

确定与压缩包对应的关联终端，通过向所述关联终端发送的验证码，对压缩包进行验证码加密；

根据用户输入的加密密码对压缩包进行密码加密。

3.根据权利要求2所述的海量数据安全存储的方法，其特征在于，所述按照预定规则对待存储数据进行分类存储，包括：

根据待存储数据的文件类型对待存储数据进行分类，并将分类后的数据进行存储。

4.根据权利要求3所述的海量数据安全存储的方法，其特征在于，所述按照预定规则对待存储数据进行分类存储，包括：

根据待存储数据的存储方式对待存储数据进行分类，并将分类后的数据进行存储。

5.根据权利要求3所述的海量数据安全存储的方法，其特征在于，所述按照预定规则对待存储数据进行分类存储，包括：

根据待存储数据的文件力度对待存储数据进行分类，并将分类后的数据进行存储。

6.一种海量数据安全存储的装置，其特征在于，包括：

存储模块，用于按照预定规则对待存储数据进行分类存储；

压缩模块，用于对每类存储的数据进行压缩，生成对应的压缩包；

加密模块，用于对压缩包进行多重加密；

转换模块，用于将加密后的压缩包转换为代码；

上传模块，用于将转换的代码上传至服务器。

7.根据权利要求6所述的海量数据安全存储的装置，其特征在于，所述加密模块包括：

第一加密单元，用于利用用户输入的身份信息对压缩包进行身份加密；

第二加密单元，用于确定与压缩包对应的关联终端，通过向所述关联终端发送的验证码，对压缩包进行验证码加密；

第三加密单元，用于根据用户输入的加密密码对压缩包进行密码加密。

8.根据权利要求7所述的海量数据安全存储的装置，其特征在于，所述存储模块包括：

第一存储单元，用于根据待存储数据的文件类型对待存储数据进行分类，并将分类后的数据进行存储。

9.根据权利要求8所述的海量数据安全存储的装置，其特征在于，所述存储模块包括：

第二存储单元，用于根据待存储数据的存储方式对待存储数据进行分类，并将分类后的数据进行存储。

10.根据权利要求9所述的海量数据安全存储的装置，其特征在于，所述存储模块包括：

第三存储单元，用于根据待存储数据的文件力度对待存储数据进行分类，并将分类后

的数据进行存储。

一种海量数据安全存储的方法及装置

技术领域

[0001] 本发明涉及数据存储技术领域，更具体地说，涉及一种海量数据安全存储的方法及装置。

背景技术

[0002] 随着存储系统向着网络化和分布式的方向发展，共享存储等使存储系统变得更易受到攻击，相对静态的存储系统往往成为攻击者的首选目标，窃取、篡改或破坏数据往往成为黑客们的常用伎俩。存储安全变得至关重要，安全存储主要包括存储安全技术、重复数据删除技术、数据备份及灾难恢复技术等。各种应用系统的存储设备上，信息正以数据存储的方式高速增长着，不断推进着全球信息化的进程。随之而来的是海量信息存储的需求不断增加。虽然文件服务器和数据库服务器的存储容量在不断扩充，可还是会碰到空间虽在成倍增长，用户仍会抱怨容量不足的情况，也正是用户对存储空间需求的不断增加，推动海量信息存储技术的不断发展。

[0003] 因此，如何实现海量数据的存储，确保数据的安全性，是本领域技术人员需要解决的问题。

发明内容

[0004] 本发明的目的在于提供一种海量数据安全存储的方法及装置，以实现海量数据的存储，确保数据的安全性。

[0005] 为实现上述目的，本发明实施例提供了如下技术方案：

[0006] 一种海量数据安全存储的方法，包括：

[0007] 按照预定规则对待存储数据进行分类存储；

[0008] 对每类存储的数据进行压缩，生成对应的压缩包；

[0009] 对压缩包进行多重加密，并将加密后的压缩包转换为代码；

[0010] 将转换的代码上传至服务器。

[0011] 其中，所述对压缩包进行多重加密，包括：

[0012] 利用用户输入的身份信息对压缩包进行身份加密；

[0013] 确定与压缩包对应的关联终端，通过向所述关联终端发送的验证码，对压缩包进行验证码加密；

[0014] 根据用户输入的加密密码对压缩包进行密码加密。

[0015] 其中，所述按照预定规则对待存储数据进行分类存储，包括：

[0016] 根据待存储数据的文件类型对待存储数据进行分类，并将分类后的数据进行存储。

[0017] 其中，所述按照预定规则对待存储数据进行分类存储，包括：

[0018] 根据待存储数据的存储方式对待存储数据进行分类，并将分类后的数据进行存储。

[0019] 其中，所述按照预定规则对待存储数据进行分类存储，包括：

[0020] 根据待存储数据的文件力度对待存储数据进行分类，并将分类后的数据进行存储。

[0021] 一种海量数据安全存储的装置，包括：

[0022] 存储模块，用于按照预定规则对待存储数据进行分类存储；

[0023] 压缩模块，用于对每类存储的数据进行压缩，生成对应的压缩包；

[0024] 加密模块，用于对压缩包进行多重加密；

[0025] 转换模块，用于将加密后的压缩包转换为代码；

[0026] 上传模块，用于将转换的代码上传至服务器。

[0027] 其中，所述加密模块包括：

[0028] 第一加密单元，用于利用用户输入的身份信息对压缩包进行身份加密；

[0029] 第二加密单元，用于确定与压缩包对应的关联终端，通过向所述关联终端发送的验证码，对压缩包进行验证码加密；

[0030] 第三加密单元，用于根据用户输入的加密密码对压缩包进行密码加密。

[0031] 其中，所述存储模块包括：

[0032] 第一存储单元，用于根据待存储数据的文件类型对待存储数据进行分类，并将分类后的数据进行存储。

[0033] 其中，所述存储模块包括：

[0034] 第二存储单元，用于根据待存储数据的存储方式对待存储数据进行分类，并将分类后的数据进行存储。

[0035] 其中，所述存储模块包括：

[0036] 第三存储单元，用于根据待存储数据的文件力度对待存储数据进行分类，并将分类后的数据进行存储。

[0037] 通过以上方案可知，本发明实施例提供的一种海量数据安全存储的方法，包括：按照预定规则对待存储数据进行分类存储；对每类存储的数据进行压缩，生成对应的压缩包；对压缩包进行多重加密，并将加密后的压缩包转换为代码；将转换的代码上传至服务器；可见，在本实施例中，通过多重方式高度加密，确保了数据的安全性，通过数据与代码的转换节约了磁盘空间，提高了存储量；本发明还公开了一种海量数据安全存储的装置，同样能实现上述技术效果。

附图说明

[0038] 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，下面描述中的附图仅仅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。

[0039] 图1为本发明实施例公开的一种海量数据安全存储的方法流程示意图；

[0040] 图2为本发明实施例公开的一种海量数据安全存储的装置结构示意图。

具体实施方式

[0041] 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，所描述的实施例仅仅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作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。

[0042] 本发明实施例公开了一种海量数据安全存储的方法及装置，以实现海量数据的存储，确保数据的安全性。

[0043] 参见图1，本发明实施例提供的一种海量数据安全存储的方法，包括：

[0044] S101、按照预定规则对待存储数据进行分类存储；

[0045] 其中，所述按照预定规则对待存储数据进行分类存储，包括：

[0046] 根据待存储数据的文件类型对待存储数据进行分类，并将分类后的数据进行存储；或者，根据待存储数据的存储方式对待存储数据进行分类，并将分类后的数据进行存储；或者，根据待存储数据的文件力度对待存储数据进行分类，并将分类后的数据进行存储。

[0047] 具体的，在本实施例中，需要将待存储的各类数据输入计算机，计算机按照用户的选择将所有数据进行分类，在分类时，可以根据数据的存储方式、文件类型及文件力度作为标准进行分类；这样在分类后，可以通过对多个数据执行S102-S104，从而加快了数据处理速度。

[0048] S102、对每类存储的数据进行压缩，生成对应的压缩包；

[0049] 具体的，在本实施例中，通过计算机将待存储文件进行分类存储后，可对分类后的数据自动压缩成多个压缩包，以便对数据进行加密及装换等操作；并且通过对数据的压缩，可以减小数据的大小，提高后续步骤对数据的处理速度。

[0050] S103、对压缩包进行多重加密，并将加密后的压缩包转换为代码；

[0051] S104、将转换的代码上传至服务器。

[0052] 其中，所述对压缩包进行多重加密，包括：

[0053] 利用用户输入的身份信息对压缩包进行身份加密；

[0054] 确定与压缩包对应的关联终端，通过向所述关联终端发送的验证码，对压缩包进行验证码加密；

[0055] 根据用户输入的加密密码对压缩包进行密码加密。

[0056] 具体的，在本实施例中，可通过多重方式对数据进行高度加密，确保了数据的安全性；在对数据进行多重机密时，可通过下述加密方式进行加密：1、通过用户的身份信息进行加密；2、通过多个终端接收的验证码进行加密；3、通过密码进行加密。这样，用户在解析该压缩包时，便需要依次进行身份验证、通过数个终端的验证码进行验证，以及通过不同的密码验证。

[0057] 具体的，对数据进行加密处理后，可见加密后的压缩包通过转换软件转换为代码，将代码上传至服务器即可；由于代码的存储量小，这样便可通过数据与代码的转换节约了磁盘空间，提高了存储容量。

[0058] 下面对本发明实施例提供的安全存储的装置进行介绍，下文描述的安全存储的装置与上文描述的安全存储的方法可以相互参照。

[0059] 参见图2，本发明实施例提供的一种海量数据安全存储的装置，包括：

[0060] 存储模块100，用于按照预定规则对待存储数据进行分类存储；

[0061] 压缩模块200，用于对每类存储的数据进行压缩，生成对应的压缩包；

[0062] 加密模块300，用于对压缩包进行多重加密；

[0063] 转换模块400，用于将加密后的压缩包转换为代码；

[0064] 上传模块500，用于将转换的代码上传至服务器。

[0065] 基于上述实施例，所述加密模块300包括：

[0066] 第一加密单元，用于利用用户输入的身份信息对压缩包进行身份加密；

[0067] 第二加密单元，用于确定与压缩包对应的关联终端，通过向所述关联终端发送的验证码，对压缩包进行验证码加密；

[0068] 第三加密单元，用于根据用户输入的加密密码对压缩包进行密码加密。

[0069] 基于上述实施例，所述存储模块100包括：

[0070] 第一存储单元，用于根据待存储数据的文件类型对待存储数据进行分类，并将分类后的数据进行存储。

[0071] 基于上述实施例，所述存储模块100包括：

[0072] 第二存储单元，用于根据待存储数据的存储方式对待存储数据进行分类，并将分类后的数据进行存储。

[0073] 基于上述实施例，所述存储模块100包括：

[0074] 第三存储单元，用于根据待存储数据的文件力度对待存储数据进行分类，并将分类后的数据进行存储。

[0075] 综上可见，本发明实施例提供的一种海量数据安全存储的方法及装置，包括：按照预定规则对待存储数据进行分类存储；对每类存储的数据进行压缩，生成对应的压缩包；对压缩包进行多重加密，并将加密后的压缩包转换为代码；将转换的代码上传至服务器；可见，通过多重方式高度加密，确保了数据的安全性，通过数据与代码的转换节约了磁盘空间，提高了存储量；并且，本方案面向云计算、大数据应用的大容量、高可靠、高扩展的多控海量统一存储系统平台，满足了政府、企业、科研机构需要的大容量、高带宽、高可靠、横向扩展的云存储系统，提高了存储系统的扩展能力。

[0076] 本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。

[0077] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

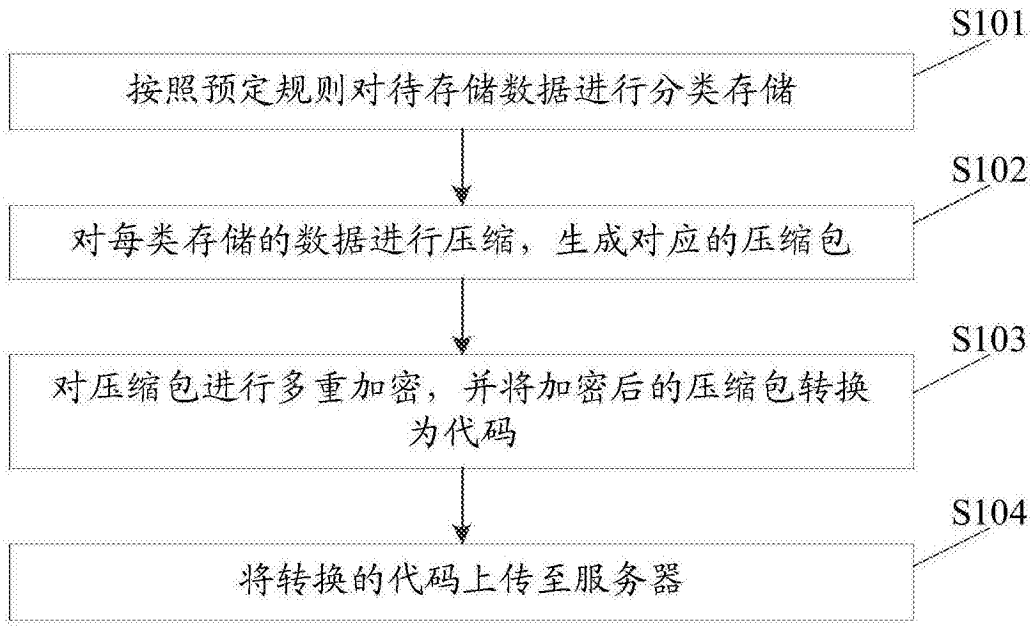

S101
按照预定规则对待存储数据进行分类存储
S102
对每类存储的数据进行压缩，生成对应的压缩包
S103
对压缩包进行多重加密，并将加密后的压缩包转换为代码
S104
将转换的代码上传至服务器

图1

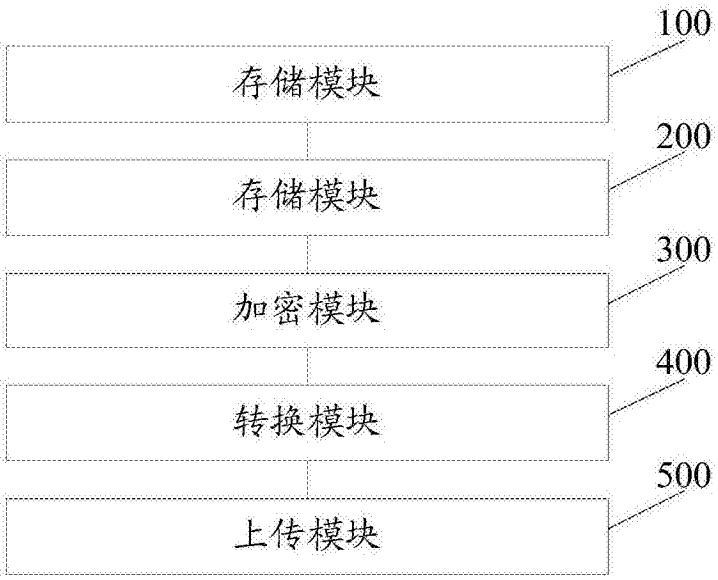

100
存储模块
200
存储模块
300
加密模块
400
转换模块
500
上传模块

图2