(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114567447 B
(45)授权公告日 2022.07.19

(21)申请号 202210441338.5
(22)申请日 2022.04.26
(65)同一申请的已公布的文献号
申请公布号 CN 114567447 A
(43)申请公布日 2022.05.31
(73)专利权人 佳瑛科技有限公司
地址 410000 湖南省长沙市五一大道599号供销大厦906室
(72)发明人 杨胜 曾海波 袁平 唐必成 黄瑛
(74)专利代理机构 长沙楚为知识产权代理事务所(普通合伙) 43217
专利代理师 李大为
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 67/06(2022.01)
G06F 16/176(2019.01)
(56)对比文件
CN 113542187 A,2021.10.22
CN 105323209 A,2016.02.10
CN 113704221 A,2021.11.26
CN 104158827 A,2014.11.19
CN 113067699 A,2021.07.02
CN 102014133 A,2011.04.13
CN 105025041 A,2015.11.04
CN 103002029 A,2013.03.27
CN 113722695 A,2021.11.30
CN 106341236 A,2017.01.18
US 2018063115 A1,2018.03.01
JP 2005196614 A,2005.07.21
审查员 刘莹

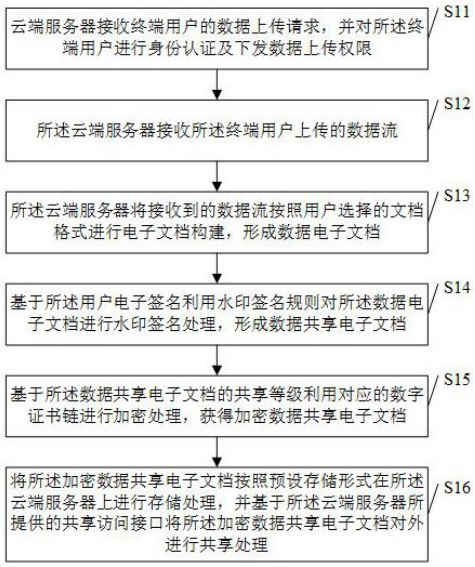
权利要求书3页 说明书10页 附图2页

(54)发明名称

一种基于云端服务器的数据共享管理方法及装置

(57)摘要

本发明公开了一种基于云端服务器的数据共享管理方法及装置,其中,所述方法包括:接收终端用户的数据上传请求,并进行身份认证及下发数据上传权限;云端服务器接收终端用户上传的数据流;将接收到的数据流按照用户选择的文档格式进行电子文档构建,形成数据电子文档;对数据电子文档进行水印签名处理,形成数据共享电子文档;对应的数字证书链进行加密处理,获得加密数据共享电子文档;将加密数据共享电子文档按照预设存储形式在云端服务器上进行存储处理,并基于云端服务器所提供的共享访问接口将加密数据共享电子文档对外进行共享处理。在本发明实施例中,可以实现对涉密数据根据相应的涉密等级进行针对性共享,保证涉密数据的安全性。



CN 114567447 B

1.一种基于云端服务器的数据共享管理方法,其特征在于,所述方法包括:

云端服务器接收终端用户的数据上传请求,并对所述终端用户进行身份认证及下发数据上传权限;

所述云端服务器接收所述终端用户上传的数据流,所述数据流包括数据信息、用户电子签名及选择对应的文档格式;

所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建,形成数据电子文档;

基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理,形成数据共享电子文档;

基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理,获得加密数据共享电子文档;

将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理,并基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理;

所述云端服务器接收终端用户的数据上传请求,并对所述终端用户进行身份认证及下发数据上传权限,包括:

所述云端服务器的授权中心接收所述终端用户的数据上传请求,并基于所述数据上传请求和终端用户身份信息生成待认证电子文档,并下发至所述终端用户;

所述终端用户基于所述待认证电子文档在所述云端服务器上的身份认证中心进行用户身份认证处理,形成身份信息认证电子文档;

所述授权中心基于所述身份信息认证电子文档向所述终端用户下发数据上传权限;

述授权中心基于所述身份信息认证电子文档向所述终端用户下发数据上传权限,包括:

所述终端用户基于所述身份信息认证电子文档中的用户特征信息生成随机数,并利用公链证书私钥进行电子签名,生成向所述授权中心提出的数据上传请求的上传请求授权申请;

所述授权中心验证所述上传请求授权申请的有效性,并在通过验证后,基于预设授权策略向所述终端用户下发数据上传权限。

2.根据权利要求1所述的数据共享管理方法,其特征在于,所述云端服务器接收所述终端用户上传的数据流,包括:

所述终端用户基于所述数据上传权限选择对应的文档格式,将所述数据信息、用户电子签名和选择对应的文档格式构建为数据流,并向所述云端服务器发送;

所述云端服务器接收所述终端用户上传的数据流。

3.根据权利要求1所述的数据共享管理方法,其特征在于,所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建,形成数据电子文档,包括:

所述云端服务器基于所述数据流中的选择对应的文档格式匹配到对应的匹配文件格式模板;

将所述数据流中的数据信息按照预设填写规则填写至对应的匹配文件格式模板中进行电子文档构建处理,形成数据电子文档。

4.根据权利要求1所述的数据共享管理方法，其特征在于，所述基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理，形成数据共享电子文档，包括：

获得所述水印签名规则中的水印参数，基于所述水印参数利用所述用户电子签名进行水印构建处理，获得用户电子签名水印；

将所述用户电子签名水印加载至所述数据电子文档的指定签名位置上，形成数据共享电子文档。

5.根据权利要求1所述的数据共享管理方法，其特征在于，所述基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理，获得加密数据共享电子文档，包括：

获得所述终端用户给所述数据共享电子文档划分的共享等级；

在共享等级加密数据库中匹配到所述共享等级对应的数字证书链，并利用所述共享等级利用对应的数字证书链对所述数据共享电子文档进行加密处理，获得加密数据共享电子文档。

6.根据权利要求1所述的数据共享管理方法，其特征在于，所述将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，包括：

获得所述加密数据共享电子文档中的数据上传的终端用户的用户名称和数据共享时的检索关键字；

将所述加密数据共享电子文档分别与所述用户名称、所述检索关键字之间构建索引关系；

将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，同时将所述用户名称和所述检索关键字匹配存储在索引数据库中。

7.根据权利要求1所述的数据共享管理方法，其特征在于，所述基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理，包括：

所述云端服务器获得存储在其上的所述加密数据共享电子文档的名称，并利用所述加密数据共享电子文档的名称更新当前的共享目录；

所述云端服务器将更新后的共享目录通过所述共享访问接口对外进行共享处理。

8.一种基于云端服务器的数据共享管理装置，其特征在于，所述装置包括：

权限获得模块：用于云端服务器接收终端用户的数据上传请求，并对所述终端用户进行身份认证及下发数据上传权限；

数据接收模块：用于所述云端服务器接收所述终端用户上传的数据流，所述数据流包括数据信息、用户电子签名及选择对应的文档格式；

文档构建模块：用于所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建，形成数据电子文档；

水印签名模块：用于基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理，形成数据共享电子文档；

文档加密模块：用于基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理，获得加密数据共享电子文档；

对外共享模块：用于将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，并基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理；

所述云端服务器接收终端用户的数据上传请求，并对所述终端用户进行身份认证及下发数据上传权限，包括：

所述云端服务器的授权中心接收所述终端用户的数据上传请求，并基于所述数据上传请求和终端用户身份信息生成待认证电子文档，并下发至所述终端用户；

所述终端用户基于所述待认证电子文档在所述云端服务器上的身份认证中心进行用户身份认证处理，形成身份信息认证电子文档；

所述授权中心基于所述身份信息认证电子文档向所述终端用户下发数据上传权限；

所 述授权中心基于所述身份信息认证电子文档向所述终端用户下发数据上传权限，包括：

所述终端用户基于所述身份信息认证电子文档中的用户特征信息生成随机数，并利用公链证书私钥进行电子签名，生成向所述授权中心提出的数据上传请求的上传请求授权申请；

所述授权中心验证所述上传请求授权申请的有效性，并在通过验证后，基于预设授权策略向所述终端用户下发数据上传权限。

一种基于云端服务器的数据共享管理方法及装置

技术领域

[0001] 本发明涉及数据共享技术领域，尤其涉及一种基于云端服务器的数据共享管理方法及装置。

背景技术

[0002] 在一些大企业中，存在一些涉密的数据需要进行有限范围内的共享，现有的共享方式，一般都是将这些涉密数据按照涉密等级，分别存储在不同的服务器上，然后给相应的均有查询这些涉密数据的人员分配这些服务器等登陆盾牌，对应的人员通过该登录盾牌登录相应的服务器上查看或者共享对应的涉密数据；这样一来，需要多个不同的服务器来存储这些不同等级的涉密数据，可能存在资源浪费的情况；并且这些数据在相关服务器上不对涉密数据进行单独的加密处理，容易被人冒充登录盾牌登录对应的服务器，造成涉密数据的泄密问题。

发明内容

[0003] 本发明的目的在于克服现有技术的不足，本发明提供了一种基于云端服务器的数据共享管理方法及装置，可以在一个服务器上实现对涉密数据根据相应的涉密等级进行针对性存储和共享，保证涉密数据的安全性。

[0004] 为了解决上述技术问题，本发明实施例提供了一种基于云端服务器的数据共享管理方法，所述方法包括：

[0005] 云端服务器接收终端用户的数据上传请求，并对所述终端用户进行身份认证及下发数据上传权限；

[0006] 所述云端服务器接收所述终端用户上传的数据流，所述数据流包括数据信息、用户电子签名及选择对应的文档格式；

[0007] 所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建，形成数据电子文档；

[0008] 基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理，形成数据共享电子文档；

[0009] 基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理，获得加密数据共享电子文档；

[0010] 将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，并基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理。

[0011] 可选的，所述云端服务器接收终端用户的数据上传请求，并对所述终端用户进行身份认证及下发数据上传权限，包括：

[0012] 所述云端服务器的授权中心接收所述终端用户的数据上传请求，并基于所述数据上传请求和终端用户身份信息生成待认证电子文档，并下发至所述终端用户；

[0013] 所述终端用户基于所述待认证电子文档在所述云端服务器上的身份认证中心进行用户身份认证处理，形成身份信息认证电子文档；

[0014] 所述授权中心基于所述身份认证电子文档向所述终端用户下发数据上传权限。

[0015] 可选的，所述授权中心基于所述身份认证电子文档向所述终端用户下发数据上传权限，包括：

[0016] 所述终端用户基于所述身份信息认证电子文档中的用户特征信息生成随机数，并利用公链证书私钥进行电子签名，生成向所述授权中心提出的数据上传请求的上传请求授权申请；

[0017] 所述授权中心验证所述上传请求授权申请的有效性，并在通过验证后，基于预设授权策略向所述终端用户下发数据上传权限。

[0018] 可选的，所述云端服务器接收所述终端用户上传的数据流，包括：

[0019] 所述终端用户基于所述数据上传权限选择对应的文档格式，将所述数据信息、用户电子签名和选择对应的文档格式构建为数据流，并向所述云端服务器发送；

[0020] 所述云端服务器接收所述终端用户上传的数据流。

[0021] 可选的，所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建，形成数据电子文档，包括：

[0022] 所述云端服务器基于所述数据流中的选择对应的文档格式匹配到对应的匹配文件格式模板；

[0023] 将所述数据流中的数据信息按照预设填写规则填写至对应的匹配文件格式模板中进行电子文档构建处理，形成数据电子文档。

[0024] 可选的，所述基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理，形成数据共享电子文档，包括：

[0025] 获得所述水印签名规则中的水印参数，基于所述水印参数利用所述用户电子签名进行水印构建处理，获得用户电子签名水印；

[0026] 将所述用户电子签名水印加载至所述数据电子文档的指定签名位置上，形成数据共享电子文档。

[0027] 可选的，所述基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理，获得加密数据共享电子文档，包括：

[0028] 获得所述终端用户给所述数据共享电子文档划分的共享等级；

[0029] 在共享等级加密数据库中匹配到所述共享等级对应的数字证书链，并利用所述共享等级利用对应的数字证书链对所述数据共享电子文档进行加密处理，获得加密数据共享电子文档。

[0030] 可选的，所述将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，包括：

[0031] 获得所述加密数据共享电子文档中的数据上传的终端用户的用户名称和数据共享时的检索关键字；

[0032] 将所述加密数据共享电子文档分别与所述用户名称、所述检索关键字之间构建索引关系；

[0033] 将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储

处理,同时将所述用户名称和所述检索关键字匹配存储在索引数据库中。

[0034] 可选的,所述基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理,包括:

[0035] 所述云端服务器获得存储在其上的所述加密数据共享电子文档的名称,并利用所述加密数据共享电子文档的名称更新当前的共享目录;

[0036] 所述云端服务器将更新后的共享目录通过所述共享访问接口对外进行共享处理。

[0037] 另外,本发明实施例还提供了一种基于云端服务器的数据共享管理装置,所述装置包括:

[0038] 权限获得模块:用于云端服务器接收终端用户的数据上传请求,并对所述终端用户进行身份认证及下发数据上传权限;

[0039] 数据接收模块:用于所述云端服务器接收所述终端用户上传的数据流,所述数据流包括数据信息、用户电子签名及选择对应的文档格式;

[0040] 文档构建模块:用于所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建,形成数据电子文档;

[0041] 水印签名模块:用于基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理,形成数据共享电子文档;

[0042] 文档加密模块:用于基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理,获得加密数据共享电子文档;

[0043] 对外共享模块:用于将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理,并基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理。

[0044] 在本发明实施例中,通过给终端用户的数据上传权限来实现数据的上传,同时在云端服务器形成数据电子文档,并依次进行水印签名和加密处理,形成加密数据共享电子文档,然后进行相应的存储处理,最后进行对外共享处理,可以在一个服务器上实现对涉密数据根据相应的涉密等级进行针对性存储和共享,保证涉密数据的安全性。

附图说明

[0045] 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,显而易见的,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它的附图。

[0046] 图1是本发明实施例中的基于云端服务器的数据共享管理方法的流程示意图;

[0047] 图2是本发明实施例中的基于云端服务器的数据共享管理装置的结构组成实体图。

具体实施方式

[0048] 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它

实施例，都属于本发明保护的范围。

[0049] 实施例一

[0050] 请参阅图1，图1是本发明实施例中的基于云端服务器的数据共享管理方法的流程示意图。

[0051] 如图1所示，一种基于云端服务器的数据共享管理方法，所述方法包括：

[0052] S11：云端服务器接收终端用户的数据上传请求，并对所述终端用户进行身份认证及下发数据上传权限；

[0053] 在本发明具体实施过程中，所述云端服务器接收终端用户的数据上传请求，并对所述终端用户进行身份认证及下发数据上传权限，包括：所述云端服务器的授权中心接收所述终端用户的数据上传请求，并基于所述数据上传请求和终端用户身份信息生成待认证电子文档，并下发至所述终端用户；所述终端用户基于所述待认证电子文档在所述云端服务器上的身份认证中心进行用户身份认证处理，形成身份信息认证电子文档；所述授权中心基于所述身份认证电子文档向所述终端用户下发数据上传权限。

[0054] 进一步的，所述授权中心基于所述身份认证电子文档向所述终端用户下发数据上传权限，包括：所述终端用户基于所述身份信息认证电子文档中的用户特征信息生成随机数，并利用公链证书私钥进行电子签名，生成向所述授权中心提出的数据上传请求的上传请求授权申请；所述授权中心验证所述上传请求授权申请的有效性，并在通过验证后，基于预设授权策略向所述终端用户下发数据上传权限。

[0055] 具体的，在该云端服务器上创建一个模块，该模块为授权中心，主要用于给访问该云端服务器的用户进行授权，包括数据上传时的授权和收据查询授权和数据管理授权等；在该云端服务器的授权中心接收到终端用户的数据上传请求时，根据该数据上传请求和终端用户身份信息生成待认证电子文档，并将该待认证电子文档下发至该终端用户上，在该终端用户上根据待认证电子文档在该云端服务器上的身份认证中心来进行用户身份认证处理，从而在终端用户身份认证通过时，形成身份信息认证电子文档；最后该授权中心根据该身份认证电子文档向该终端用户下发数据上传权限。

[0056] 其中，在该终端用户上根据待认证电子文档在该云端服务器上的身份认证中心来进行用户身份认证处理具体包括双重身份认证处理，首先进行用户的账户密码认证处理，在终端用户上根据所提供的账号输入框和对应的密码输入框输入相应的账号信息和对应的密码信息，并上传至云端服务器中的身份认证中心进行第一次身份认证处理，在身份认证通过之后，云端服务器的身份认证中心调用终端用户所在的终端的摄像设备采集用户的人脸信息或者活体指纹信息进行二次身份认证处理，在两次身份认证均通过的情况下，即可形成身份信息认证电子文档。

[0057] 在授权中心根据身份认证电子文档向终端用户下发数据上传权限时，该终端用户首先根据该身份信息认证电子文档中的用户特征信息生成一个随机数，并且利用公链证书的私钥来进行电子签名处理，并生成向授权中心提出的数据上传请求的上传请求授权申请；然后该授权中心通过验证该上传请求授权申请的有效性，并在验证通过之后，根据预设的授权策略向终端用户下发数据上传权限。

[0058] 其中，预设授权策略包括该用户的身份在云端服务器上所拥有的最高权限，并且所授予权限不能高于最高权限。

[0059] S12:所述云端服务器接收所述终端用户上传的数据流,所述数据流包括数据信息、用户电子签名及选择对应的文档格式;

[0060] 在本发明具体实施过程中,所述云端服务器接收所述终端用户上传的数据流,包括:所述终端用户基于所述数据上传权限选择对应的文档格式,将所述数据信息、用户电子签名和选择对应的文档格式构建为数据流,并向所述云端服务器发送;所述云端服务器接收所述终端用户上传的数据流。

[0061] 具体的,该终端用户根据数据上传权限进行对应的文档格式的选择,并将该数据信息、用户电子签名和选择对应的文档格式构建为数据流,同时向云端服务器发送;该云端服务器接收云端服务器接收;即该数据流包括数据信息、用户电子签名及选择对应的文档格式。

[0062] S13:所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建,形成数据电子文档;

[0063] 在本发明具体实施过程中,所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建,形成数据电子文档,包括:所述云端服务器基于所述数据流中的选择对应的文档格式匹配到对应的匹配文件格式模板;将所述数据流中的数据信息按照预设填写规则填写至对应的匹配文件格式模板中进行电子文档构建处理,形成数据电子文档。

[0064] 具体的,该云端服务器根据该数据流中的选择对应的文档格式匹配到对应的匹配文件格式模板,让后将该数据流中的数据信息按照预设填写规则填写至对应的匹配文件格式模板中进行电子文档构建处理,形成数据电子文档。

[0065] S14:基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理,形成数据共享电子文档;

[0066] 在本发明具体实施过程中,所述基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理,形成数据共享电子文档,包括:获得所述水印签名规则中的水印参数,基于所述水印参数利用所述用户电子签名进行水印构建处理,获得用户电子签名水印;将所述用户电子签名水印加载至所述数据电子文档的指定签名位置上,形成数据共享电子文档。

[0067] 具体的,首先在该云端服务器上根据预先设置来获得该水印签名规则中的水印参数,并且根据该水印参数利用该用户电子签名来进行水印构建处理,然后得到用户电子签名水印,在水印构建时,主要是利用水印参数中的水印类型,水印大小、水印透明度等参数来对用户电子签名进行水印构建处理;最后,将该用户电子签名水印加载至该数据电子文档的指定签名位置上,形成数据共享电子文档;通过加载签名水印的方式,实现对形成的数据共享电子文档进行签名,使得该数据共享电子文档更具有有消息,同时该水印签名无法进行更改,保障数据安全性。

[0068] S15:基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理,获得加密数据共享电子文档;

[0069] 在本发明具体实施过程中,所述基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理,获得加密数据共享电子文档,包括:获得所述终端用户给所述数据共享电子文档划分的共享等级;在共享等级加密数据库中匹配到所述共享等级对应的

数字证书链，并利用所述共享等级利用对应的数字证书链对所述数据共享电子文档进行加密处理，获得加密数据共享电子文档。

[0070] 具体的，通过获得该终端用户给该数据共享电子文档划分的共享等级；然后通过利用该共享等级在共享等级加密数据库中匹配到该共享等级对应的数字证书链，并利用共享等级利用对应的数字证书链对数据共享电子文档进行加密处理，获得加密数据共享电子文档；其中，该数字证书链为安全不同的共享等级创建的证书，同时还包括对应的根CA证书；该对应的根CA证书用户在后续被共享用户在身份认证通过后，服务器根据该被共享用户的查询权限等级，授权其查询权限时，安全期查询权限等级下发对应的根CA证书；即可查询相应的加密据共享电子文档。

[0071] S16：将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，并基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理。

[0072] 在本发明具体实施过程中，所述将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，包括：获得所述加密数据共享电子文档中的数据上传的终端用户的用户名称和数据共享时的检索关键字；将所述加密数据共享电子文档分别与所述用户名称、所述检索关键字之间构建索引关系；将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，同时将所述用户名称和所述检索关键字匹配存储在索引数据库中。

[0073] 进一步的，所述基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理，包括：所述云端服务器获得存储在其上的所述加密数据共享电子文档的名称，并利用所述加密数据共享电子文档的名称更新当前的共享目录；所述云端服务器将更新后的共享目录通过所述共享访问接口对外进行共享处理。

[0074] 具体的，首先是获得该加密数据共享电子文档中的数据上传的终端用户的用户名称和数据共享时的检索关键字；然后将加密数据共享电子文档分别与用户名称、所述检索关键字之间构建索引关系；即可以通过该用户名称和数据共享时的检索关键字查询到该加密数据共享电子文档；然后将该密数据共享电子文档按照预设存储形式在云端服务器上进行存储处理，同时将用户名称和检索关键字匹配存储在索引数据库中。这样子，可以方便后续被共享用户对该密数据共享电子文档的查询检索，使得被共享用户能迅速的查找到相关的稳定数据，减少查询时间，提供用户的使用体验。

[0075] 进一步的，该云端服务器在获得存储在其上的加密数据共享电子文档的名称之后，利用加密数据共享电子文档的名称更新当前的共享目录；然后通过该云端服务器将更新后的共享目录通过共享访问接口对外进行共享处理。

[0076] 另外，在终端用户需要对已共享的加密数据共享电子文档进行管理时，需要向云端服务器的授权中心发出管理申请，通过授权中心按照步骤一中的授权方式，给终端用户发出相应的授权管理权限，才可以对现有的加密数据共享电子文档进行相应的管理，其中包括编辑、删除等权限；被共享用户也需要向该授权中心进行查询权限申请，该授权中心需要根据该被共享用户的权限向该被共享用户下发查询权限，该查询权限中包含具有时效限制的与该查询权限相对于的根CA证书，使得该被共享用户在相应时效能，可利用该跟CA证书对其具有查询权限的加密数据共享电子文档进行查询，阅读等操作。

[0077] 在本发明实施例中，通过给终端用户的数据上传权限来实现数据的上传，同时在云端服务器形成数据电子文档，并依次进行水印签名和加密处理，形成加密数据共享电子文档，然后进行相应的存储处理，最后进行对外共享处理，可以在一个服务器上实现对涉密数据根据相应的涉密等级进行针对性存储和共享，保证涉密数据的安全性。

[0078] 实施例二

[0079] 请参阅图2，图2是本发明实施例中的基于云端服务器的数据共享管理装置的结构组成实体图。

[0080] 如图2所示，一种基于云端服务器的数据共享管理装置，所述装置包括：

[0081] 权限获得模块21：用于云端服务器接收终端用户的数据上传请求，并对所述终端用户进行身份认证及下发数据上传权限；

[0082] 在本发明具体实施过程中，所述云端服务器接收终端用户的数据上传请求，并对所述终端用户进行身份认证及下发数据上传权限，包括：所述云端服务器的授权中心接收所述终端用户的数据上传请求，并基于所述数据上传请求和终端用户身份信息生成待认证电子文档，并下发至所述终端用户；所述终端用户基于所述待认证电子文档在所述云端服务器上的身份认证中心进行用户身份认证处理，形成身份信息认证电子文档；所述授权中心基于所述身份认证电子文档向所述终端用户下发数据上传权限。

[0083] 进一步的，所述授权中心基于所述身份认证电子文档向所述终端用户下发数据上传权限，包括：所述终端用户基于所述身份信息认证电子文档中的用户特征信息生成随机数，并利用公链证书私钥进行电子签名，生成向所述授权中心提出的数据上传请求的上传请求授权申请；所述授权中心验证所述上传请求授权申请的有效性，并在通过验证后，基于预设授权策略向所述终端用户下发数据上传权限。

[0084] 具体的，在该云端服务器上创建一个模块，该模块为授权中心，主要用于给访问该云端服务器的用户进行授权，包括数据上传时的授权和收据查询授权和数据管理授权等；在该云端服务器的授权中心接收到终端用户的数据上传请求时，根据该数据上传请求和终端用户身份信息生成待认证电子文档，并将该待认证电子文档下发至该终端用户上，在该终端用户上根据待认证电子文档在该云端服务器上的身份认证中心来进行用户身份认证处理，从而在终端用户身份认证通过时，形成身份信息认证电子文档；最后该授权中心根据该身份认证电子文档向该终端用户下发数据上传权限。

[0085] 其中，在该终端用户上根据待认证电子文档在该云端服务器上的身份认证中心来进行用户身份认证处理具体包括双重身份认证处理，首先进行用户的账户密码认证处理，在终端用户上根据所提供的账号输入框和对应的密码输入框输入相应的账号信息和对应的密码信息，并上传至云端服务器中的身份认证中心进行第一次身份认证处理，在身份认证通过之后，云端服务器的身份认证中心调用终端用户所在的终端的摄像设备采集用户的人脸信息或者活体指纹信息进行二次身份认证处理，在两次身份认证均通过的情况下，即可形成身份信息认证电子文档。

[0086] 在授权中心根据身份认证电子文档向终端用户下发数据上传权限时，该终端用户首先根据该身份信息认证电子文档中的用户特征信息生成一个随机数，并且利用公链证书的私钥来进行电子签名处理，并生成向授权中心提出的数据上传请求的上传请求授权申请；然后该授权中心通过验证该上传请求授权申请的有效性，并在验证通过之后，根据预设

的授权策略向终端用户下发数据上传权限。

[0087] 其中，预设授权策略包括该用户的身份在云端服务器上所拥有的最高权限，并且所授予权限不能高于最高权限。

[0088] 数据接收模块22：用于所述云端服务器接收所述终端用户上传的数据流，所述数据流包括数据信息、用户电子签名及选择对应的文档格式；

[0089] 在本发明具体实施过程中，所述云端服务器接收所述终端用户上传的数据流，包括：所述终端用户基于所述数据上传权限选择对应的文档格式，将所述数据信息、用户电子签名和选择对应的文档格式构建为数据流，并向所述云端服务器发送；所述云端服务器接收所述终端用户上传的数据流。

[0090] 具体的，该终端用户根据数据上传权限进行对应的文档格式的选择，并将该数据信息、用户电子签名和选择对应的文档格式构建为数据流，同时向云端服务器发送；该云端服务器接收云端服务器接收；即该数据流包括数据信息、用户电子签名及选择对应的文档格式。

[0091] 文档构建模块23：用于所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建，形成数据电子文档；

[0092] 在本发明具体实施过程中，所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建，形成数据电子文档，包括：所述云端服务器基于所述数据流中的选择对应的文档格式匹配到对应的匹配文件格式模板；将所述数据流中的数据信息按照预设填写规则填写至对应的匹配文件格式模板中进行电子文档构建处理，形成数据电子文档。

[0093] 具体的，该云端服务器根据该数据流中的选择对应的文档格式匹配到对应的匹配文件格式模板，让后将该数据流中的数据信息按照预设填写规则填写至对应的匹配文件格式模板中进行电子文档构建处理，形成数据电子文档。

[0094] 水印签名模块24：用于基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理，形成数据共享电子文档；

[0095] 在本发明具体实施过程中，所述基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理，形成数据共享电子文档，包括：获得所述水印签名规则中的水印参数，基于所述水印参数利用所述用户电子签名进行水印构建处理，获得用户电子签名水印；将所述用户电子签名水印加载至所述数据电子文档的指定签名位置上，形成数据共享电子文档。

[0096] 具体的，首先在该云端服务器上根据预先设置来获得该水印签名规则中的水印参数，并且根据该水印参数利用该用户电子签名来进行水印构建处理，然后得到用户电子签名水印，在水印构建时，主要是利用水印参数中的水印类型，水印大小、水印透明度等参数来对用户电子签名进行水印构建处理；最后，将该用户电子签名水印加载至该数据电子文档的指定签名位置上，形成数据共享电子文档；通过加载签名水印的方式，实现对形成的数据共享电子文档进行签名，使得该数据共享电子文档更具有有消息，同时该水印签名无法进行更改，保障数据安全性。

[0097] 文档加密模块25：用于基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理，获得加密数据共享电子文档；

[0098] 在本发明具体实施过程中，所述基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理，获得加密数据共享电子文档，包括：获得所述终端用户给所述数据共享电子文档划分的共享等级；在共享等级加密数据库中匹配到所述共享等级对应的数字证书链，并利用所述共享等级利用对应的数字证书链对所述数据共享电子文档进行加密处理，获得加密数据共享电子文档。

[0099] 具体的，通过获得该终端用户给该数据共享电子文档划分的共享等级；然后通过利用该共享等级在共享等级加密数据库中匹配到该共享等级对应的数字证书链，并利用共享等级利用对应的数字证书链对数据共享电子文档进行加密处理，获得加密数据共享电子文档；其中，该数字证书链为安全不同的共享等级创建的证书，同时还包括对应的根CA证书；该对应的根CA证书用户在后续被共享用户在身份认证通过后，服务器根据该被共享用户的查询权限等级，授权其查询权限时，安全期查询权限等级下发对应的根CA证书；即可查询相应的加密据共享电子文档。

[0100] 对外共享模块26：用于将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，并基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理。

[0101] 在本发明具体实施过程中，所述将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，包括：获得所述加密数据共享电子文档中的数据上传的终端用户的用户名称和数据共享时的检索关键字；将所述加密数据共享电子文档分别与所述用户名称、所述检索关键字之间构建索引关系；将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，同时将所述用户名称和所述检索关键字匹配存储在索引数据库中。

[0102] 进一步的，所述基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理，包括：所述云端服务器获得存储在其上的所述加密数据共享电子文档的名称，并利用所述加密数据共享电子文档的名称更新当前的共享目录；所述云端服务器将更新后的共享目录通过所述共享访问接口对外进行共享处理。

[0103] 具体的，首先是获得该加密数据共享电子文档中的数据上传的终端用户的用户名称和数据共享时的检索关键字；然后将加密数据共享电子文档分别与用户名称、所述检索关键字之间构建索引关系；即可以通过该用户名称和数据共享时的检索关键字查询到该加密数据共享电子文档；然后将该密数据共享电子文档按照预设存储形式在云端服务器上进行存储处理，同时将用户名称和检索关键字匹配存储在索引数据库中。这样子，可以方便后续被共享用户对该密数据共享电子文档的查询检索，使得被共享用户能迅速的查找到相关的稳定数据，减少查询时间，提供用户的使用体验。

[0104] 进一步的，该云端服务器在获得存储在其上的加密数据共享电子文档的名称之后，利用加密数据共享电子文档的名称更新当前的共享目录；然后通过该云端服务器将更新后的共享目录通过共享访问接口对外进行共享处理。

[0105] 另外，在终端用户需要对已共享的加密数据共享电子文档进行管理时，需要向云端服务器的授权中心发出管理申请，通过授权中心按照步骤一中的授权方式，给终端用户发出相应的授权管理权限，才可以对现有的加密数据共享电子文档进行相应的管理，其中包括编辑、删除等权限；被共享用户也需要向该授权中心进行查询权限申请，该授权中心需

要根据该被共享用户的权限向该被共享用户下发查询权限，该查询权限中包含具有时效限制的与该查询权限相对于的根CA证书，使得该被共享用户在相应时效能，可利用该跟CA证书对其具有查询权限的加密数据共享电子文档进行查询，阅读等操作。

[0106] 在本发明实施例中，通过给终端用户的数据上传权限来实现数据的上传，同时在云端服务器形成数据电子文档，并依次进行水印签名和加密处理，形成加密数据共享电子文档，然后进行相应的存储处理，最后进行对外共享处理，可以在一个服务器上实现对涉密数据根据相应的涉密等级进行针对性存储和共享，保证涉密数据的安全性。

[0107] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：只读存储器(ROM，Read Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁盘或光盘等。

[0108] 另外，以上对本发明实施例所提供的一种基于云端服务器的数据共享管理方法及装置进行了详细介绍，本文中应采用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

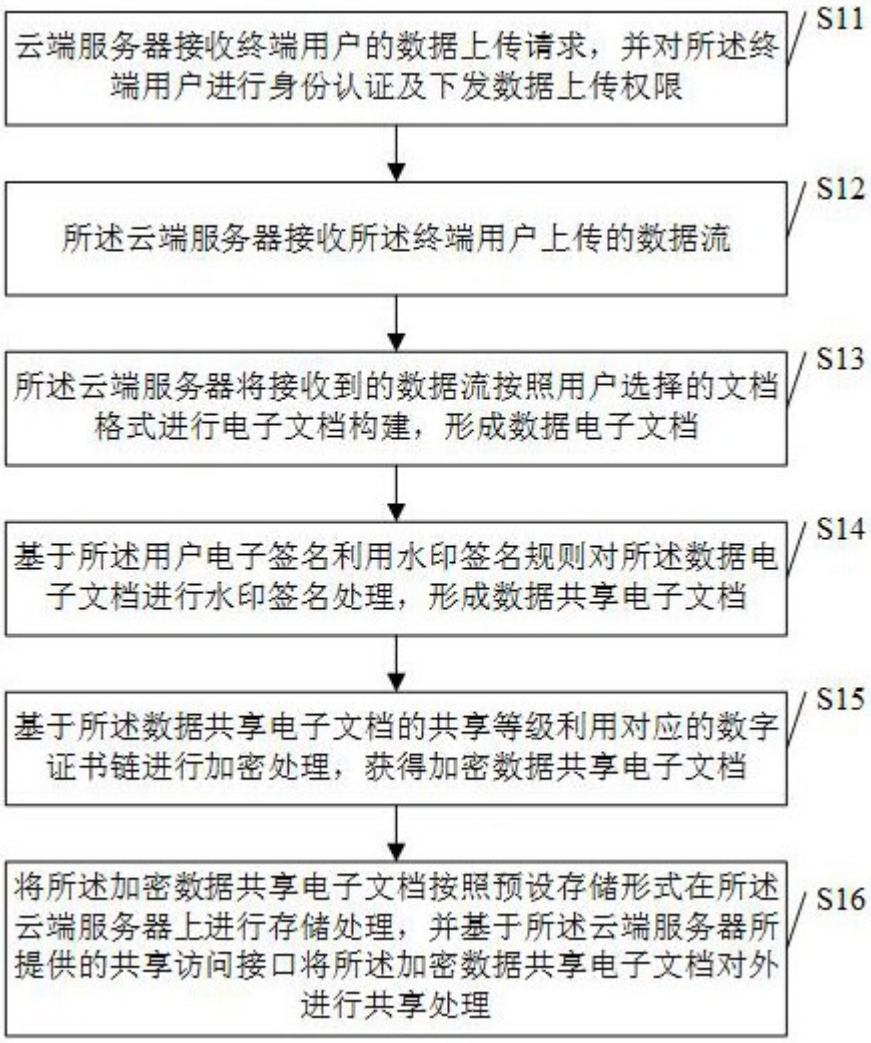

云端服务器接收终端用户的数据上传请求，并对所述终端用户进行身份认证及下发数据上传权限
S11
所述云端服务器接收所述终端用户上传的数据流
S12
所述云端服务器将接收到的数据流按照用户选择的文档格式进行电子文档构建，形成数据电子文档
S13
基于所述用户电子签名利用水印签名规则对所述数据电子文档进行水印签名处理，形成数据共享电子文档
S14
基于所述数据共享电子文档的共享等级利用对应的数字证书链进行加密处理，获得加密数据共享电子文档
S15
将所述加密数据共享电子文档按照预设存储形式在所述云端服务器上进行存储处理，并基于所述云端服务器所提供的共享访问接口将所述加密数据共享电子文档对外进行共享处理
S16

图1

图2