(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116366243 A
(43)申请公布日 2023.06.30

(21)申请号 202310312819.0

(22)申请日 2023.03.28

(71)申请人 加客云科技(河北)有限公司
地址 050000 河北省石家庄市裕华区槐安路与富强大街交口怀特商务D座5楼5001室

(72)发明人 孟海彬

(74)专利代理机构 北京慕达星云知识产权代理事务所(特殊普通合伙) 11465
专利代理师 李冉

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/40(2022.01)
G06F 21/60(2013.01)

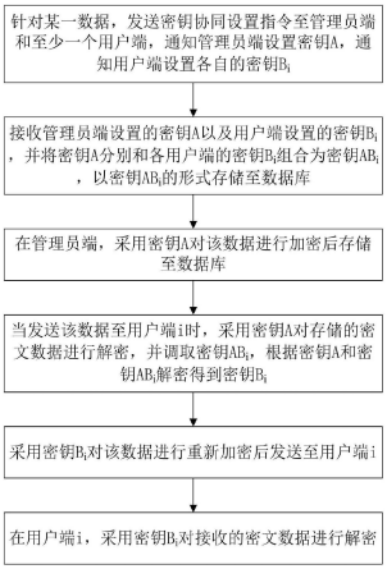
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种用于数字化协同办公的数据传输与加密方法及系统

(57)摘要

本发明公开了一种用于数字化协同办公的数据传输与加密方法及系统,方法包括:针对某一数据,通知管理员端设置密钥A,通知用户端设置密钥B_i;将密钥A和密钥B_i组合为密钥AB_i,以密钥AB_i的形式存储至数据库;在管理员端,采用密钥A对该数据进行加密后存储至数据库;当发送该数据至用户端i时,采用密钥A对存储的密文数据进行解密,并根据解密得到密钥B_i,采用密钥B_i对该数据进行重新加密后发送至用户端i;在用户端i,采用密钥B_i对接收的密文数据进行解密。本发明使管理员端和用户端协同对数据进行加密,用户端只有输对自己的秘钥后才能看到解密数据,防止因数据库外泄或网络劫持造成的数据泄露。



CN 116366243 A

1.一种用于数字化协同办公的数据传输与加密方法,其特征在于,包括:

针对某一数据,发送密钥协同设置指令至管理员端和至少一个用户端,通知管理员端设置密钥A,通知用户端设置各自的密钥B_i,i表示第i个用户端;

接收管理员端设置的密钥A以及用户端设置的密钥B_i,并将密钥A分别和各用户端的密钥B_i组合为密钥AB_i,以密钥AB_i的形式存储至数据库;

在管理员端,采用密钥A对该数据进行加密后存储至数据库;

当发送该数据至用户端i时,采用密钥A对存储的密文数据进行解密,并调取密钥AB_i,根据密钥A和密钥AB_i解密得到密钥B_i;采用密钥B_i对该数据进行重新加密后发送至用户端i;

在用户端i,采用密钥B_i对接收的密文数据进行解密。

2.根据权利要求1所述的用于数字化协同办公的数据传输与加密方法,其特征在于,还包括:

当某一数据需发送至多个用户端时,每个用户端设置的密钥各不相同,发送数据时,选择指定用户端,并采用指定用户端各自的密钥分别对该数据进行重新加密后,再分发至指定用户端。

3.根据权利要求1所述的用于数字化协同办公的数据传输与加密方法,其特征在于,在管理员端,通过密钥A对该数据进行解密,并在对该数据编辑操作后再次保存时,自动启用密钥A对该数据进行加密。

4.根据权利要求1所述的用于数字化协同办公的数据传输与加密方法,其特征在于,采用3DES算法对数据进行加密和解密操作。

5.根据权利要求1所述的用于数字化协同办公的数据传输与加密方法,其特征在于,在管理员端,执行某一操作之前,提示进行二次密码验证。

6.一种用于数字化协同办公的数据传输与加密系统,其特征在于,包括:

密钥协同设置模块,用于针对某一数据,发送密钥协同设置指令至管理员端和至少一个用户端,通知管理员端设置密钥A,通知用户端设置各自的密钥B_i,i表示第i个用户端;

密钥存储管理模块,用于接收管理员端设置的密钥A以及用户端设置的密钥B_i,并将密钥A分别和各用户端的密钥B_i组合为密钥AB_i,以密钥AB_i的形式存储至数据库;

管理员端数据加密模块,用于在管理员端,采用密钥A对该数据进行加密后存储至数据库;

数据发送及重加密模块,用于当发送该数据至用户端i时,采用密钥A对存储的密文数据进行解密,并调取密钥AB_i,根据密钥A和密钥AB_i解密得到密钥B_i;采用密钥B_i对该数据进行重新加密后发送至用户端i;

用户端数据解密模块,用于在用户端i,采用密钥B_i对接收的密文数据进行解密。

7.根据权利要求6所述的用于数字化协同办公的数据传输与加密系统,其特征在于,所述数据发送及重加密模块还用于在发送数据时,选择指定用户端,并采用指定用户端各自的密钥分别对该数据进行重新加密后,再分发至指定用户端。

8.根据权利要求6所述的用于数字化协同办公的数据传输与加密系统,其特征在于,所述管理员端数据加密模块还用于在管理员端,通过密钥A对该数据进行解密,并在对该数据编辑操作后再次保存时,自动启用密钥A对该数据进行加密。

9.根据权利要求6所述的用于数字化协同办公的数据传输与加密系统,其特征在于,还

包括：

二次验证模块，用于在管理员端，执行某一操作之前，提示进行二次密码验证。

一种用于数字化协同办公的数据传输与加密方法及系统

技术领域

[0001] 本发明涉及信息安全技术领域，更具体的说是涉及一种用于数字化协同办公的数据传输与加密方法及系统。

背景技术

[0002] 目前，在众多的数字化系统办公系统当中，对于数据的存储和传输都是用明文实现的，少数系统使用了秘钥加密，将数据加密存储和传输，同时将解密秘钥存储在数据库或文件中，一定程度上保证了数据的保密性。但是，一旦秘钥和密文同时被泄露，就很容易造成密文的破译，无法真正保证数据的安全。如果不加密，系统运维人员能直接看到原始数据。如果使用秘钥加密，并且保存了秘钥，对于开发人员来说，也是无法实现真正的保密，因为程序是开发人员写的，如果将秘钥放到第三方，开发人员可以调用解密工具读取数据。

[0003] 因此，如何提供一种能够解决运维人员或开发人员获取机密数据的用于数字化协同办公的数据传输与加密方法及系统是本领域技术人员亟需解决的问题。

发明内容

[0004] 有鉴于此，本发明提供了一种用于数字化协同办公的数据传输与加密方法及系统，使管理员端和用户端协同对数据进行加密，用户端只有输对自己的秘钥后才能看到解密数据，防止因数据库外泄或网络劫持造成的数据泄露。

[0005] 为了实现上述目的，本发明采用如下技术方案：

[0006] 第一方面，本发明提供一种用于数字化协同办公的数据传输与加密方法，包括：

[0007] 针对某一数据，发送密钥协同设置指令至管理员端和至少一个用户端，通知管理员端设置密钥A，通知用户端设置各自的密钥B_i，i表示第i个用户端；

[0008] 接收管理员端设置的密钥A以及用户端设置的密钥B_i，并将密钥A分别和各用户端的密钥B_i组合为密钥AB_i，以密钥AB_i的形式存储至数据库；

[0009] 在管理员端，采用密钥A对该数据进行加密后存储至数据库；

[0010] 当发送该数据至用户端i时，采用密钥A对存储的密文数据进行解密，并调取密钥AB_i，根据密钥A和密钥AB_i解密得到密钥B_i；采用密钥B_i对该数据进行重新加密后发送至用户端i；

[0011] 在用户端i，采用密钥B_i对接收的密文数据进行解密。

[0012] 进一步的，还包括：

[0013] 当某一数据需发送至多个用户端时，每个用户端设置的密钥各不相同，发送数据时，选择指定用户端，并采用指定用户端各自的密钥分别对该数据进行重新加密后，再分发至指定用户端。

[0014] 进一步的，在管理员端，通过密钥A对该数据进行解密，并在对该数据编辑操作后再次保存时，自动启用密钥A对该数据进行加密。

[0015] 进一步的，采用3DES算法对数据进行加密和解密操作。

[0016] 进一步的，在管理员端，执行某一操作之前，提示进行二次密码验证。

[0017] 第二方面，本发明还提供一种用于数字化协同办公的数据传输与加密系统，包括：

[0018] 密钥协同设置模块，用于针对某一数据，发送密钥协同设置指令至管理员端和至少一个用户端，通知管理员端设置密钥A，通知用户端设置各自的密钥B_i，i表示第i个用户端；

[0019] 密钥存储管理模块，用于接收管理员端设置的密钥A以及用户端设置的密钥B_i，并将密钥A分别和各用户端的密钥B_i组合为密钥AB_i，以密钥AB_i的形式存储至数据库；

[0020] 管理员端数据加密模块，用于在管理员端，采用密钥A对该数据进行加密后存储至数据库；

[0021] 数据发送及重加密模块，用于当发送该数据至用户端i时，采用密钥A对存储的密文数据进行解密，并调取密钥AB_i，根据密钥A和密钥AB_i解密得到密钥B_i；采用密钥B_i对该数据进行重新加密后发送至用户端i；

[0022] 用户端数据解密模块，用于在用户端i，采用密钥B_i对接收的密文数据进行解密。

[0023] 进一步的，所述数据发送及重加密模块还用于在发送数据时，选择指定用户端，并采用指定用户端各自的密钥分别对该数据进行重新加密后，再分发至指定用户端。

[0024] 进一步的，所述管理员端数据加密模块还用于在管理员端，通过密钥A对该数据进行解密，并在对该数据编辑操作后再次保存时，自动启用密钥A对该数据进行加密。

[0025] 进一步的，该系统还包括：

[0026] 二次验证模块，用于在管理员端，执行某一操作之前，提示进行二次密码验证。

[0027] 经由上述的技术方案可知，与现有技术相比，本发明公开提供了一种用于数字化协同办公的数据传输与加密方法，针对某一数据，需要管理员端和用户端协同对该数据进行加密，管理员端操作时，数据保存的都是用管理员的秘钥加密后的数据，发送给用户端的数据是用户端的秘钥加密的，发送给每个用户端的数据采用自己掌握秘钥进行解密，也能确保接收人设备遗失等原因造成数据的遗失。

[0028] 同时，未存储管理员的秘钥和用户的秘钥，采用不保留秘钥的加密方式将数据存放到数据库，数据无法被运维和技术人员解密，也能够解决通过正常或非正常手段，即使获取到数据库和劫持程序，也因无法通过技术或黑客手段获取到秘钥从而保证数据无法解密。

附图说明

[0029] 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，还可以根据提供的附图获得其他的附图。

[0030] 图1为本发明提供的用于数字化协同办公的数据传输与加密方法的流程图；

[0031] 图2为本发明提供的用于数字化协同办公的数据传输与加密系统的结构框图。

具体实施方式

[0032] 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。

[0033] 如图1所示，本发明实施例公开了一种用于数字化协同办公的数据传输与加密方法，包括以下步骤：

[0034] 针对某一数据，发送密钥协同设置指令至管理员端和至少一个用户端，通知管理员端设置密钥A，通知用户端设置各自的密钥B_i，i表示第i个用户端；

[0035] 接收管理员端设置的密钥A以及用户端设置的密钥B_i，并将密钥A分别和各用户端的密钥B_i组合为密钥AB_i，以密钥AB_i的形式存储至数据库；

[0036] 在管理员端，采用密钥A对该数据进行加密后存储至数据库；

[0037] 当发送该数据至用户端i时，采用密钥A对存储的密文数据进行解密，并调取密钥AB_i，根据密钥A和密钥AB_i解密得到密钥B_i；采用密钥B_i对该数据进行重新加密后发送至用户端i；

[0038] 在用户端i，采用密钥B_i对接收的密文数据进行解密。

[0039] 本发明实施例需要管理员端和用户端协同操作，在管理员端，管理员对数据进行操作前需要输入解密秘钥A，用秘钥A解密数据库中的加密数据，如果秘钥A不正确，将无法得到正确的解密结果，如果秘钥A正确，则可以得到解密后的数据并在页面临时展示明文，管理员端可对数据进行编辑，再次保存的时候，自动启用秘钥A将数据加密后保存到数据库。

[0040] 管理员端发起设置用户秘钥的协同工作给用户端，管理员输入秘钥A，用户输入秘钥B，提交保存时，将秘钥A和秘钥B组合得到秘钥AB，并将秘钥AB存到数据库，秘钥A和秘钥B均不保存。

[0041] 管理员端将数据发送给用户时，需输入秘钥A，通过A秘钥将数据库中加密的数据解密得到原始数据，同时取出秘钥AB，用A秘钥将AB秘钥解密得出B秘钥，再用B秘钥将原始数据加密后传送给用户端。

[0042] 用户端收到加密数据后，每次查看需要输入秘钥B才能查看到原始数据，若秘钥错误，将无法得到解密后的数据。

[0043] 本发明实施例中，数据在数据库中是加密存储的，因未存储管理员端的秘钥和用户端的秘钥，一旦数据库被泄露，泄露的数据是无法识别的，因此数据无法被运维和技术人员解密。

[0044] 更有利的，该方法还包括：当某一数据需发送至多个用户端时，每个用户端设置的密钥各不相同，发送数据时，选择指定用户端，并采用指定用户端各自的密钥分别对该数据进行重新加密后，再分发至指定用户端。

[0045] 本发明实施例可以选择一个或多个指定用户端对数据进行选择性发送，根据各指定用户端各自的密钥对该数据进行重新加密，将重新加密的数据发送至对应的用户端，由于每个用户端的密钥是不同的，所以发送给每个用户端的数据都通过不一样的加密方式加密，加密的数据需要每个用户端用自己的秘钥，解密自己的数据，才能看到结果，即使接收人设备遗失，也不会被轻易破解造成数据的遗失。

[0046] 具体来说，无论是在管理员端采用密钥A对数据进行加解密，或采用密钥B对数据

进行加密，还是在用户端采用密钥B对数据进行解密，均可以采用3DES算法对数据进行加密和解密操作。

[0047] 更有利的，在管理员端，执行某一操作之前，提示进行二次密码验证。本发明实施例通过在进入相关页面前，提示输入二次密码验证，可以避免管理员端被其他人使用造成数据泄露的情况。

[0048] 如图2所示，本发明实施例还提供一种用于数字化协同办公的数据传输与加密系统，包括：

[0049] 密钥协同设置模块，用于针对某一数据，发送密钥协同设置指令至管理员端和至少一个用户端，通知管理员端设置密钥A，通知用户端设置各自的密钥B_i，i表示第i个用户端；

[0050] 密钥存储管理模块，用于接收管理员端设置的密钥A以及用户端设置的密钥B_i，并将密钥A分别和各用户端的密钥B_i组合为密钥AB_i，以密钥AB_i的形式存储至数据库；

[0051] 管理员端数据加密模块，用于在管理员端，采用密钥A对该数据进行加密后存储至数据库；

[0052] 数据发送及重加密模块，用于当发送该数据至用户端i时，采用密钥A对存储的密文数据进行解密，并调取密钥AB_i，根据密钥A和密钥AB_i解密得到密钥B_i；采用密钥B_i对该数据进行重新加密后发送至用户端i；

[0053] 用户端数据解密模块，用于在用户端i，采用密钥B_i对接收的密文数据进行解密。

[0054] 其中，管理员端数据加密模块还用于在管理员端，通过密钥A对该数据进行解密，并在对该数据编辑操作后再次保存时，自动启用密钥A对该数据进行加密。

[0055] 更有利的，数据发送及重加密模块还用于在发送数据时，选择指定用户端，并采用指定用户端各自的密钥分别对该数据进行重新加密后，再分发至指定用户端。

[0056] 在其他实施例中，本发明系统还包括：

[0057] 二次验证模块，用于在管理员端，执行某一操作之前，提示进行二次密码验证。

[0058] 本发明系统可以应用于各数字化协同办公软件中，提高数字化协同办公软件的安全性。

[0059] 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。对于实施例公开的装置而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。

[0060] 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。

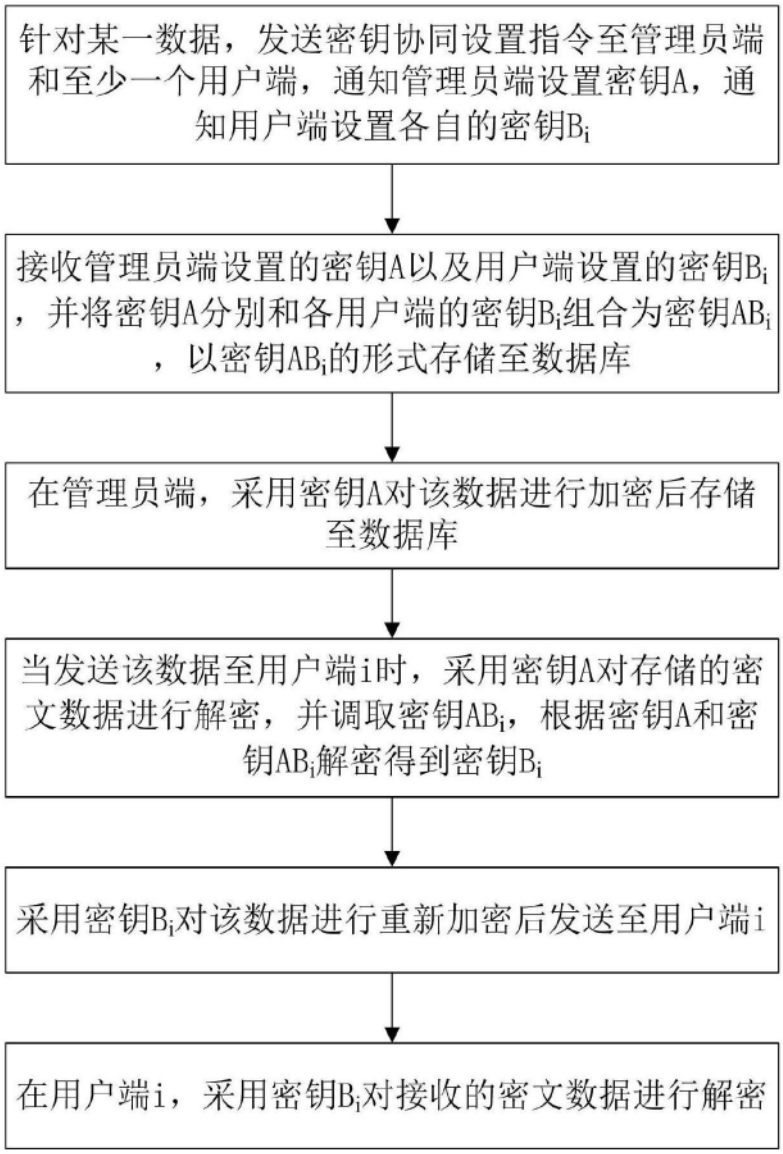

针对某一数据，发送密钥协同设置指令至管理员端和至少一个用户端，通知管理员端设置密钥A，通知用户端设置各自的密钥B_i
接收管理员端设置的密钥A以及用户端设置的密钥B_i，并将密钥A分别和各用户端的密钥B_i组合为密钥AB_i，以密钥AB_i的形式存储至数据库
在管理员端，采用密钥A对该数据进行加密后存储至数据库
当发送该数据至用户端i时，采用密钥A对存储的密文数据进行解密，并调取密钥AB_i，根据密钥A和密钥AB_i解密得到密钥B_i
采用密钥B_i对该数据进行重新加密后发送至用户端i
在用户端i，采用密钥B_i对接收的密文数据进行解密

图1

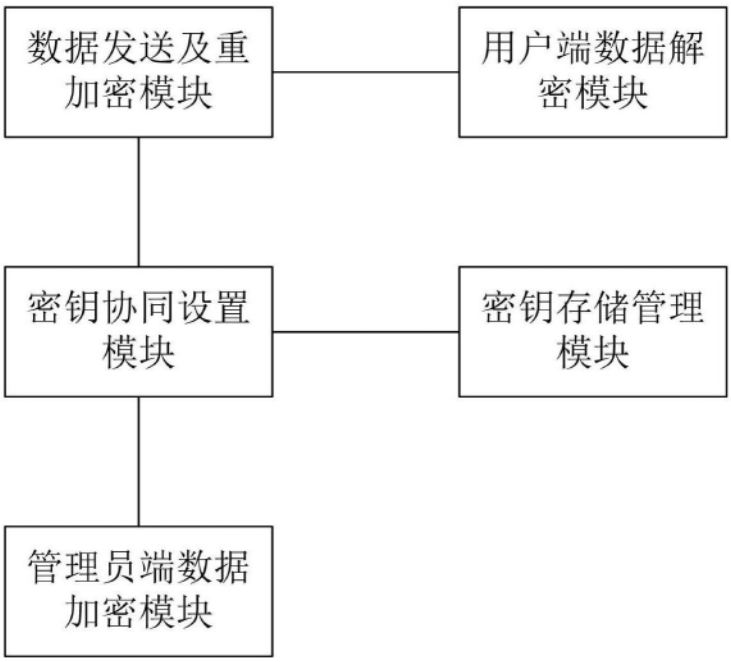


图2