(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 111917535 A
(43)申请公布日 2020.11.10

(21)申请号 202010610020.6

(22)申请日 2020.06.30

(71)申请人 山东信通电子股份有限公司
地址 255088 山东省淄博市高新区柳毅山路18号

(72)发明人 于健 许宝进 张晓宇 邹龙跃 朱辉兵 李连亮 黄鲁 张志强

(74)专利代理机构 北京君慧知识产权代理事务所(普通合伙) 11716
代理人 董延丽

(51)Int.Cl.
H04L 9/06(2006.01)
G06F 21/60(2013.01)

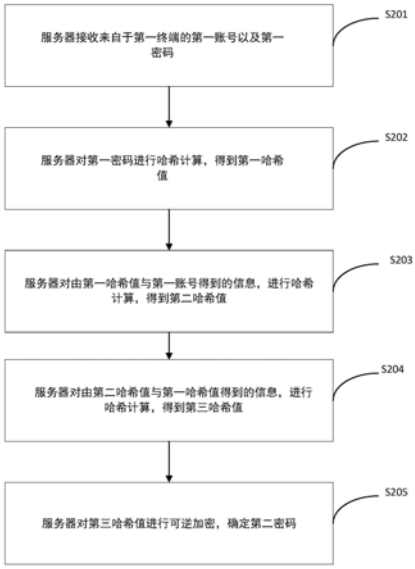
权利要求书2页 说明书7页 附图5页

(54)发明名称

一种数据加密存储方法、装置及服务器

(57)摘要

本申请公开了一种数据加密存储方法、装置及服务器。通过接收来自于第一终端的第一账号以及第一密码,所述第一密码是明文密码或者是首次加密后的密文密码;对所述第一密码进行哈希计算,得到第一哈希值;对由所述第一哈希值与所述第一账号得到的信息,进行哈希计算,得到第二哈希值;对由所述第二哈希值与所述第一哈希值得到的信息,进行哈希计算,得到第三哈希值;对所述第三哈希值进行可逆加密,以确定第二密码,所述第二密码是与所述第一账号及第一密码对应的密文密码。本发明提供的数据加密存储方法降低了数据泄露的风险,进一步增强了用户数据的安全性。



CN 111917535 A

1.一种数据加密存储方法,其特征在于,所述方法包括:

接收来自于第一终端的第一账号以及第一密码;所述第一密码是明文密码或者是首次加密后的密文密码;

对所述第一密码进行哈希计算,得到第一哈希值;

对由所述第一哈希值与所述第一账号得到的信息,进行哈希计算,得到第二哈希值;

对由所述第二哈希值与所述第一哈希值得到的信息,进行哈希计算,得到第三哈希值;

对所述第三哈希值进行可逆加密,以确定第二密码,所述第二密码是与所述第一账号及第一密码对应的密文密码。

2.根据权利要求1所述的一种数据加密存储方法,其特征在于,所述由所述第一哈希值与所述第一账号得到的信息,进行哈希计算,得到第二哈希值,具体包括:

对所述第一哈希值的M位与所述第一账号进行合并,以得到所述第一账号的加盐账号;其中,所述第一哈希值的M位是所述第一哈希值按照预设顺序的任意M位;

对所述第一账号的加盐账号进行哈希计算,得到所述第二哈希值。

3.根据权利要求2所述的一种数据加密存储方法,其特征在于,所述对所述第一哈希值的M位与所述第一账号进行合并,以得到所述第一账号的加盐账号,包括:

将所述第一账号与M位的第一哈希值进行前后拼接;或

将所述第一账号,插入到所述M位的第一哈希值任意中间位置;或

将所述M位的第一哈希值每个字符按照预设顺序逐一插入到所述第一账号中。

4.根据权利要求1所述的一种数据加密存储方法,其特征在于,所述将由所述第二哈希值与所述第一哈希值得到的信息,进行哈希计算,得到第三哈希值,具体包括:

对所述第二哈希值的N位与所述第一哈希值进行合并,以得到所述第一哈希值的加盐哈希值;其中,所述第二哈希值的N位是所述第二哈希值按照预设顺序的任意N位;

对所述第一哈希值的加盐哈希值进行哈希计算,得到所述第三哈希值。

5.根据权利要求4所述的一种数据加密存储方法,其特征在于,对所述第二哈希值的N位与所述第一哈希值进行合并,以得到所述第一哈希值的加盐哈希值,包括:

将所述第一哈希值与N位的第二哈希值进行前后拼接;或

将所述第一哈希值,插入到所述N位的第二哈希值任意中间位置;或

将所述N位的第二哈希值按照预设顺序逐一插入到所述第一哈希值中。

6.根据权利要求1所述的一种数据加密存储方法,其特征在于,所述对所述第三哈希值进行可逆加密,具体包括:

根据预设密钥,对所述第三哈希值进行可逆加密,确定所述第二密码,存储所述第二密码以及所述第三哈希值。

7.根据权利要求6所述的一种数据加密存储方法,其特征在于,所述方法还包括:

基于接收来自第二终端的第二账号以及第三密码;其中,所述第二终端与所述第一终端是同一终端,或者不同终端;

验证所述第二账号,以及所述第三密码是否与所述第一密码相同,并在验证通过后登录成功。

8.根据权利要求7所述的一种数据加密存储方法,其特征在于,验证所述第二账号,以及所述第三密码是否与所述第一密码相同,并在验证通过后登录成功,具体包括:

根据预设密钥对所述第一账号对应的第二密码解密，得到所述第三哈希值；

根据第二账号以及第二账号对应第三密码，对所述第三密码进行哈希计算，得到第四哈希值；

对由所述第四哈希值与所述第二账号得到的信息进行哈希计算，得到第五哈希值；

对由所述第五哈希值与所述第四哈希值得到的信息，进行哈希计算，得到待验证的第六哈希值；

将所述待验证的第六哈希值与所述第三哈希值进行匹配，确定对所述第二账号验证是否通过。

9.一种数据加密存储装置，其特征在于，包括：

接收模块，接收来自于第一终端的第一账号以及第一密码；

第一哈希加密模块，对对所述第一密码进行哈希计算，得到第一哈希值；

第二哈希加密模块，对由所述第一哈希值与所述第一账号得到的信息，进行哈希计算，得到第二哈希值；

第三哈希加密模块，对由所述第二哈希值与所述第一哈希值得到的信息，进行哈希计算，得到第三哈希值；

可逆加密模块，对所述第三哈希值进行可逆加密，以确定第二密码，所述第二密码是与所述第一账号及第一密码对应的密文密码。

10.一种数据加密存储服务器，其特征在于，包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行如权利要求1-8任一项所述的数据加密存储方法。

一种数据加密存储方法、装置及服务器

技术领域

[0001] 本申请涉及通信技术领域，尤其涉及一种数据加密存储方法、装置及服务器。

背景技术

[0002] 近年来，网络建设发展速度较快，数据的安全性一直是关系到企业与个人切身利益的重点，并且哈希运算由于不可逆性的特点受到了广泛的应用。但是，由于哈希运算自身特点，已出现了如彩虹表等暴力破解方式。因此，用户数据的安全性较低，数据泄露的风险较高是亟待解决的问题。

发明内容

[0003] 本申请实施例提供了一种数据加密存储方法、装置及服务器，解决了用户数据的安全性较低，数据泄露的风险较高的问题。

[0004] 一方面，本申请实施例提供了一种数据加密存储方法。服务器接收来自于第一终端的第一账号以及第一密码；所述第一密码是明文密码或者是首次加密后的密文密码；对所述第一密码进行哈希计算，得到第一哈希值；对由所述第一哈希值与所述第一账号得到的信息，进行哈希计算，得到第二哈希值；对由所述第二哈希值与所述第一哈希值得到的信息，进行哈希计算，得到第三哈希值；对所述第三哈希值进行可逆加密，以确定第二密码，所述第二密码是与所述第一账号及第一密码对应的密文密码。

[0005] 由于随机盐加密时需要将随机盐保存到数据库，一旦数据库泄露，随机盐与加密结果的对应关系也会泄露。本申请实施例通过将第一哈希值与第一账号得到的信息作为盐，从而降低了数据泄露的风险，并对第三哈希值进行可逆加密，使其直观上看起来并非哈希算法加密，达到伪装效果，进一步增强用户数据的安全性。

[0006] 在一个示例中，对所述第一哈希值的M位与所述第一账号进行合并，以得到所述第一账号的加盐账号；其中，所述第一哈希值的M位是所述第一哈希值按照预设顺序的任意M位；对所述第一账号的加盐账号进行哈希计算，得到所述第二哈希值。本申请实施例中由于第一账号的唯一性，因此，生成的第二哈希值也是唯一的。

[0007] 在一个示例中，将所述第一账号与M位的第一哈希值进行前后拼接；或将所述第一账号，插入到所述M位的第一哈希值任意中间位置；或将所述M位的第一哈希值每个字符按照预设顺序逐一插入到所述第一账号中。

[0008] 在一个示例中，对所述第二哈希值的N位与所述第一哈希值进行合并，以得到所述第一哈希值的加盐哈希值；其中，所述第二哈希值的N位是所述第二哈希值按照预设顺序的任意N位；对所述第一哈希值的加盐哈希值进行哈希计算，得到所述第三哈希值。

[0009] 在一个示例中，将所述第一哈希值与N位的第二哈希值进行前后拼接；或将所述第一哈希值，插入到所述N位的第二哈希值任意中间位置；或将所述N位的第二哈希值按照预设顺序逐一插入到所述第一哈希值中。

[0010] 在一个示例中，根据预设密钥，对所述第三哈希值进行可逆加密，确定所述第二密

码，存储所述第二密码以及所述第三哈希值。

[0011] 在一个示例中，基于接收来自第二终端的第二账号以及第三密码；其中，所述第二终端与所述第一终端是同一终端，或者不同终端；验证所述第二账号，以及所述第三密码是否与所述第一密码相同，并在验证通过后登录成功。

[0012] 在一个示例中，根据预设密钥对所述第一账号对应的第二密码解密，得到所述第三哈希值；根据第二账号以及第二账号对应第三密码，对所述第三密码进行哈希计算，得到第四哈希值；对由所述第四哈希值与所述第二账号得到的信息进行哈希计算，得到第五哈希值；对由所述第五哈希值与所述第四哈希值得到的信息，进行哈希计算，得到待验证的第六哈希值；将所述待验证的第六哈希值与所述第三哈希值进行匹配，确定对所述第二账号的验证是否通过。由于哈希加密具有不可逆性，因此，本申请实施例通过匹配存储的第三哈希值与待验证的第六哈希值是否一致，验证第二账号与第一账号是否相同，及验证第三密码与第一密码是否相同，进一步增强了用户数据的安全性。

[0013] 另一方面，本申请实施例提供了一种数据加密存储装置，该装置包括接收模块，接收来自于第一终端的第一账号以及第一密码；所述第一密码是明文密码或者是首次加密后的密文密码；第一哈希加密模块，对对所述第一密码进行哈希计算，得到第一哈希值；第二哈希加密模块，对由所述第一哈希值与所述第一账号得到的信息，进行哈希计算，得到第二哈希值；第三哈希加密模块，将由所述第二哈希值与所述第一哈希值得到的信息，进行哈希计算，得到第三哈希值；可逆加密模块，对所述第三哈希值进行可逆加密，以确定第二密码，所述第二密码是与所述第一账号及第一密码对应的密文密码。

[0014] 又一方面，本申请实施例提供了一种服务器，包括至少一个处理器；以及与所述至少一个处理器通信连接的存储器；其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行上述数据加密存储方法。

[0015] 本申请实施例提供的一种数据加密存储方法、装置及服务器，通过第一账号拼接第一哈希值的若干位作为盐来对第一密码对应的第一哈希值进行二次哈希，实现了不需要将盐存入数据库，节省了存储空间与查询成本，不存在数据库泄露即盐泄露的问题，也实现了由于第一账号是唯一的，即使第一密码相同导致第一哈希值相同，但最终得到的第二密码也是不同的，因此无法根据第二密码推出盐值。并通过对第三哈希值进行可逆加密，使直观上看起来并非哈希算法加密，达到伪装的效果。

附图说明

[0016] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0017] 图1为本申请实施例提供的一种数据加密存储示意图；

[0018] 图2为本申请实施例提供的一种数据加密存储方法流程图；

[0019] 图3为本申请实施例提供的一种数据验证方法流程图；

[0020] 图4为本申请实施例提供的一种数据加密存储装置示意图；

[0021] 图5为本申请实施例提供的一种数据加密存储服务器示意图。

具体实施方式

[0022] 为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

[0023] 图1为本申请实施例提供的一种数据加密存储示意图。

[0024] 如图1所示，数据加密存储系统至少包括服务器100、第一终端110以及第二终端120。此外，第一终端110以及第二终端120分别和服务器100通过网络连接。

[0025] 需要说明的是，本申请实施例中的第二终端120与第一终端110是不同终端。本申请实施例仅以第一终端110与第二终端120是不同终端为例。实际上，本申请实施例的第二终端120与第一终端110可以是同一终端。

[0026] 此外，第一终端110或者第二终端120具体可以是移动终端或台式终端，且移动终端具体可以手机、平板电脑、笔记本电脑等中的至少一种。服务器100可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

[0027] 用户通过第一终端110向服务器100发起注册申请，服务器100通过接收来自于第一终端110的第一账号以及第一密码，首先，对第一密码进行哈希计算，得到第一哈希值。其次，服务器100对由第一哈希值与第一账号得到的信息，进行哈希计算，得到第二哈希值。再次，服务器100对由所第二哈希值与所述第一哈希值得到的信息，进行哈希计算，得到第三哈希值。最后，服务器100对第三哈希值进行可逆加密，以确定第二密码，所述第二密码是与所述第一账号及第一密码对应的密文密码，即用户完成注册。需要说明的是，第一密码是明文密码或者是经过第一终端110首次加密后的密文密码。

[0028] 用户注册第一账号并设置第一密码之后，该用户通过输入账号、密码进行登录时，服务器100通过接收来自于第二终端120的第二账号以及第三密码，根据第二账号查询得出存储的第一账号对应的第二密码。服务器100根据预设密钥对该第二密码进行解密，得到存储的第三哈希值。服务器100根据第二账号以及第三密码，得到待验证的第六哈希值。服务器100将待验证的第六哈希值与所述第三哈希值进行匹配，从而验证第二账号，并验证第三密码是否与第一密码相同，并在验证通过后登录成功。

[0029] 在数据加密存储系统中，数据保护极其重要，每年基于帐户安全的攻击非常多，一旦黑客获取到用户的帐户密码，黑客可将用户的敏感信息进行交易获取利益。本申请实施例实现了数据保护。即使在数据库被非法访问的情况下，也能够保护敏感数据不被非法访问者直接获取。在一个应用场景中，某公司的安保系统数据库服务器100被入侵，入侵者获得了所有数据库数据的查看权限，如果管理员的口令(Password)被明文保存在数据库中，则入侵者可以进入安保系统，将整个公司的安保设施关闭，或者删除安保系统中所有的信息，将导致非常严重的后果。本申请实施例通过将口令经过特定方式的加密，使得入侵者无法获得口令明文，从而使得入侵者无法使用管理员身份进入安保系统进行非法操作。因此，本申请实施例提供了一种数据加密存储方法，通过将第一账号拼接第一哈希值的M位作为盐来对第一密码对应的第一哈希值进行二次哈希，增加了破解难度，提高了用户数据的安全性。

[0030] 下面结合图2、图3进行详细描述。

[0031] 图2为本申请实施例提供的一种数据加密存储方法流程图。

[0032] S201、服务器100接收来自于第一终端110的第一账号以及第一密码。

[0033] 在本实施例中，第一密码是明文密码或者是经过第一终端110首次加密后的密文密码。即第一密码可以为用户账号对应的账号密码，并且用户账号对应的账号密码为明文密码，也可以为第一终端110对用户账号对应的账号密码生成的密文密码。其中，密文密码的生成方法可以采用常见的加密算法。例如，用户账号为admin，用户明文密码设置为123456，而第一终端110发来的是123456经过加密后的AB12CD。

[0034] S202、服务器100对第一密码进行哈希计算，得到第一哈希值。

[0035] 用户在注册账户的时候，通常需要设置用户账号对应的账号密码，后续用户登陆时，用于进行身份验证。在本申请实施例中，为了保证用户账号的安全性，服务器100在接收到来自于第一终端110的第一密码之后，不会直接存储第一密码，通过对第一密码进行哈希计算，以得到第一哈希值。一个例子中，可以采用MD5等哈希算法，本申请对此不作特殊限制。

[0036] 举例来说，服务器100对原始密码123456采用MD5哈希算法进行运算，得到第一哈希值:49BA59ABBE56E057。

[0037] S203、服务器100对由第一哈希值与第一账号得到的信息，进行哈希计算，得到第二哈希值。

[0038] 在本实施例中，服务器100对第一哈希值的M位与第一账号进行合并，以得到第一账号的加盐账号，对第一账号的加盐账号进行哈希计算，以得到第二哈希值。其中，可以采用MD5等哈希算法，本申请对此不作特殊限制。

[0039] 此外，本申请实施例将第一哈希值的M位与第一账号合并后作为盐，并对该盐进行哈希计算，避免看出哪部分是账号以及哪部分是第一哈希值的部分哈希值，并且由于第一账号的唯一性，生成的盐也是唯一的，故而对第一密码做二次哈希时的盐都是不同的。因此，当第一账号不同时，即使第一密码相同，最终生成的第二密码也不同。

[0040] 具体的，服务器100将第一账号与M位的第一哈希值进行前后拼接。例如，第一账号在前，M位的第一哈希值直接拼接在第一账号的后面。又例如，M位的第一哈希值在前，第一账号直接拼接在M位的第一哈希值的后面。或服务器100将第一账号插入到M位的第一哈希值任意中间位置。例如，截取M位的第一哈希值的前$\frac{1}{2}$部分字符，再拼接第一账号，最后拼接M位的第一哈希值的后$\frac{1}{2}$字符。或服务器100将M位的第一哈希值每个字符按照预设顺序逐一插入到第一账号中。例如，先取一个第一账号的字符，再取一个M位的第一哈希值的字符，如此依次反复。若M位的第一哈希值或第一账号其中一方已取完所有字符，但另一方尚未取完，则将另一方的剩余字符全部取出并拼接到完成上述步骤中的拼接字符串的后面。

[0041] 需要说明的是，第一哈希值的M位为基于固定规则选取得到，即第一哈希值按照预设顺序的任意M位。一个例子中，第一哈希值的M位是第一哈希值任意连续M位，本申请对此不作特殊限制。

[0042] 举例来说，服务器100从第一哈希值中取前8位拼接到第一账号后，得到加盐账号：admin49BA59AB，对加盐账号进行哈希运算，得到第二哈希值:70D5B30EFC819390。

[0043] S204、服务器100对由第二哈希值与第一哈希值得到的信息，进行哈希计算，得到第三哈希值。

[0044] 在本实施例中，服务器100对第二哈希值的N位与第一哈希值进行合并，以得到第一哈希值的加盐哈希值，对第一哈希值的加盐哈希值进行哈希计算，得到第三哈希值。

[0045] 需要说明的是，本实施例中可以采用与上述S202或上述S203相同的哈希算法对第一哈希值的加盐哈希值进行计算，也可以采用与上述S202或上述S203的不同的哈希算法对第一哈希值的加盐哈希值进行计算。也就是说，本申请实施例的S202、S203以及S204中采用的哈希算法可以相同，也可以不同，本申请不作特殊限制。

[0046] 具体的，服务器100将第一哈希值与N位的第二哈希值进行前后拼接。例如，第一哈希值在前，N位的第二哈希值直接拼接在第一哈希值的后面。又例如，N位的第二哈希值在前，第一哈希值直接拼接在N位的第二哈希值的后面。或服务器100将第一哈希值插入到N位的第二哈希值任意中间位置。例如，截取的前$\frac{1}{2}$部分字符，再拼接第一哈希值，最后拼接N位的第二哈希值的后$\frac{1}{2}$字符。或服务器100将N位的第二哈希值每个字符按照预设顺序逐一插入到第一哈希值中。例如，先取一个第一哈希值的字符，再取一个N位的第二哈希值的字符，如此依次反复。若N位的第二哈希值或第一哈希值其中一方已取完所有字符，但另一方尚未取完，则将另一方的剩余字符全部取出并拼接到完成上述步骤中的拼接字符串的后面。

[0047] 需要说明的是，第二哈希值的N位为基于固定规则选取得到，即第二哈希值按照预设顺序的任意N位。一个例子中，第二哈希值N位是第二哈希值任意连续N位，本申请对此不作特殊限制。

[0048] 由上述S201-S204可知，本申请实施例通过加入盐的方式对第一哈希值进行二次加密，进行数据的二次加密，减少数据被破解的可能性，从而提高数据的安全性。此外，使用的盐不是随机盐，而是可以通过第一账号拼接第一哈希值的M位作为盐来得到，不需要保存到数据库，数据库泄露不会导致盐与第二密码的对应关系泄露。并且使用的盐也不会混入到第二密码中，无法根据第二密码以及整个流程方法逆推出盐值。

[0049] 举例来说，服务器100从第二哈希值中取前8位拼接到第一哈希值后，得到加盐第一哈希值：49BA59ABBE56E05770D5B30E，对加盐第一哈希值进行哈希运算，得到第三哈希值：337ED0227FE88A88。

[0050] S205、服务器100对第三哈希值进行可逆加密，确定第二密码。

[0051] 在本实施例中，服务器100根据预设密钥，对第三哈希值进行可逆加密，确定所述第二密码，第二密码是与所述第一账号及第一密码对应的密文密码，并存储第二密码以及第三哈希值。由于常用的哈希运算结果是由英文字符和数字组成，从外观上可直接判断出一个字符串是否为哈希字符串，本申请实施例通过加密算法对第三哈希值进行可逆加密，以进一步封装数据，增加数据安全性。具体的，加密算法可以为非对称或对称加密算法，本申请对此不作特殊限制。一个例子中，加密算法为AES对称加密算法。

[0052] 举例来说，服务器100使用密钥aeskey对上述S204中的第三哈希值做AES可逆加密，得到加密结果：

[0053] U2FsdGVkX1/HfJr/b/bfnMvJ/R3+N7aTjWPMNBWbba5/onVOtHUYNKtGSZq1ZkfU，将加

密结果保存到数据库中。

[0054] 服务器100接收到来自于第二终端120用户的登录请求时，登录请求包括第二账号、第二账号对应的第三密码等，验证第二账号，以及第三密码是否与第一密码相同，并在验证通过后登录成功。

[0055] 本申请实施例提供的验证过程将通过图3及相关内容进行描述。

[0056] S301、服务器100接收来自于第二终端120的第二账号以及第三密码。

[0057] 在本实施例中，用户注册时，若第一终端110对第一密码进行加密后，发送服务器100。那么用户登录验证时，第二终端120对该用户的账号对应的密码，采用相同算法进行加密，发送服务器100。例如，用户注册时，第一终端110将第一密码123456，下次验证时第二终端120依然发来123456，服务器才通过。若第一终端110发来的是123456加密后的AB12CD，那么下次验证第二终端120依然需要发来AB12CD，服务器100才能通过。

[0058] S302、服务器100验证第二账号。

[0059] 在本实施例中，第二账号可以为正确的用户账号，即与第一账号相同。也可以为错误的用户账号，错误的用户账号可能不存在，也可能是存在的。例如，张三输入李四的帐号，但输入了自己账号对应的密码，服务器100通过用户名数据库验证第二账号不存在，执行S303。服务器100通过用户名数据库验证第二账号存在，查询得出第一账号对应的第二密码，执行S304。

[0060] 举例来说，服务器100根据第一账号admin查询出保存第二密码:U2FsdGVkX1/HfJr/b/bfnMvJ/R3+N7aTjWPMNBWbba5/onVOtHUYNKtGSZqlZkfU。

[0061] S303、服务器100结束验证流程。

[0062] 服务100返回验证失败的消息至第二终端120，以使第二终端120返回登录失败的提示至该终端对应的用户。

[0063] S304、服务器100根据预设密钥对第一账号对应的第二密码进行解密，得到存储的第三哈希值。

[0064] 举例来说，服务器100使用密钥aeskey对第二密码进行AES解密，得到保存的第三哈希值:337ED0227FE88A88。

[0065] S305、服务器100对第三密码进行哈希计算，得到第四哈希值。

[0066] 本实施例中，服务器100采用与S202中相同的哈希算法，对第三密码进行哈希计算，得到第四哈希值。

[0067] S306、服务器100对由第四哈希值与第二账号得到的信息，进行哈希计算，得到第五哈希值。

[0068] 本实施例中，服务器100对第四哈希值的M位与第二账号进行合并，以得到第二账号的加盐账号，对第二账号的加盐账号进行哈希计算，以得到第四哈希值。需要说明的是，第四哈希值的M位采用与上述S203中第一哈希值的M位相同的选取规则，并且第四哈希值的M位与第二账号拼接的位置和上述S203中第一哈希值的M位与第一账号的拼接位置相同，避免因为拼接位置错误，导致第二账号验证不通过的问题。

[0069] S307、服务器100对由第五哈希值与第四哈希值得到的信息，进行哈希计算，得到待验证的第六哈希值。

[0070] 在本实施例中，服务器100对第五哈希值的N位与第四哈希值进行合并，以得到第

四哈希值的加盐哈希值，对第四哈希值的加盐哈希值进行哈希计算，得到待验证的第六哈希值。需要说明的是，第五哈希值的N位采用与上述S204中第二哈希值的N位相同的选取规则，并且第五哈希值的N位与第四哈希值拼接的位置和上述S204中第二哈希值的N位与第一哈希值的拼接位置相同，避免因为拼接位置错误，导致第二账号验证不通过的问题。

[0071] S308、服务器100将待验证的第六哈希值与第三哈希值进行匹配，确定第二账号验证是否通过。

[0072] 若待验证的第六哈希值与第三哈希值相同，表示验证成功，即第二账号与第一账号相同以及第三密码与第一密码相同，返回验证成功的消息至第二终端120，若待验证的第六哈希值与第三哈希值不同，表示验证失败，返回验证失败的消息至第二终端120，以使第二终端120返回登录失败的提示至该终端对应的用户。

[0073] 举例来说，服务器100得到需要验证的第六哈希值：337ED0227FE88A88，与上述S304中的第三哈希值相同，则验证成功。

[0074] 在本申请的一个实施例中，如图4所示，提供了一种数据加密存储装置400，包括：接收模块410、哈希加密模块420及可逆加密模块430。哈希加密模块420包括第一哈希加密模块421、第二哈希加密模块422以及第三哈希加密模块423。

[0075] 接收模块410，接收来自于第一终端的第一账号以及第一密码，所述第一密码是明文密码或者是首次加密后的密文密码。

[0076] 第一哈密加密模块421，对第一密码进行哈希计算，得到第一哈希值。第二哈希加密模块422，对由第一哈希值与第一账号得到的信息，进行哈希计算，得到第二哈希值；第三哈希加密模块423，对由第二哈希值与第一哈希值得到的信息，进行哈希计算，得到第三哈希值。

[0077] 可逆加密模块430，对第三哈希值进行可逆加密，以确定第二密码，所述第二密码是与所述第一账号及第一密码对应的密文密码。

[0078] 在本申请的一个实施例中，如图5所示，提供了一种数据加密存储服务器100，包括：处理器510、存储器520及存储在存储器上并可在处理器上运行的计算机程序。

[0079] 处理器510和存储器520建立通信连接，处理器510用于读取存储器中的程序，处理器510执行计算机程序时实现以下步骤：

[0080] 接收来自于第一终端110的第一账号以及第一密码，所述第一密码是明文密码或者是首次加密后的密文密码，对第一密码进行哈希计算，得到第一哈希值，对由第一哈希值与第一账号得到的信息，进行哈希计算，得到第二哈希值，对由第二哈希值与第一哈希值得到的信息，进行哈希计算，得到第三哈希值，对第三哈希值进行可逆加密，以确定第二密码，第二密码是与第一账号及第一密码对应的密文密码。

[0081] 在本申请的一个实施例中，处理器510执行计算机程序时还实现以下步骤：

[0082] 基于接收来自第二终端120的第二账号以及第三密码；其中，第二终端120与第一终端110是同一终端，或者不同终端；验证第二账号，以及第三密码是否与所述第一密码相同，并在验证通过后登录成功。

[0083] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

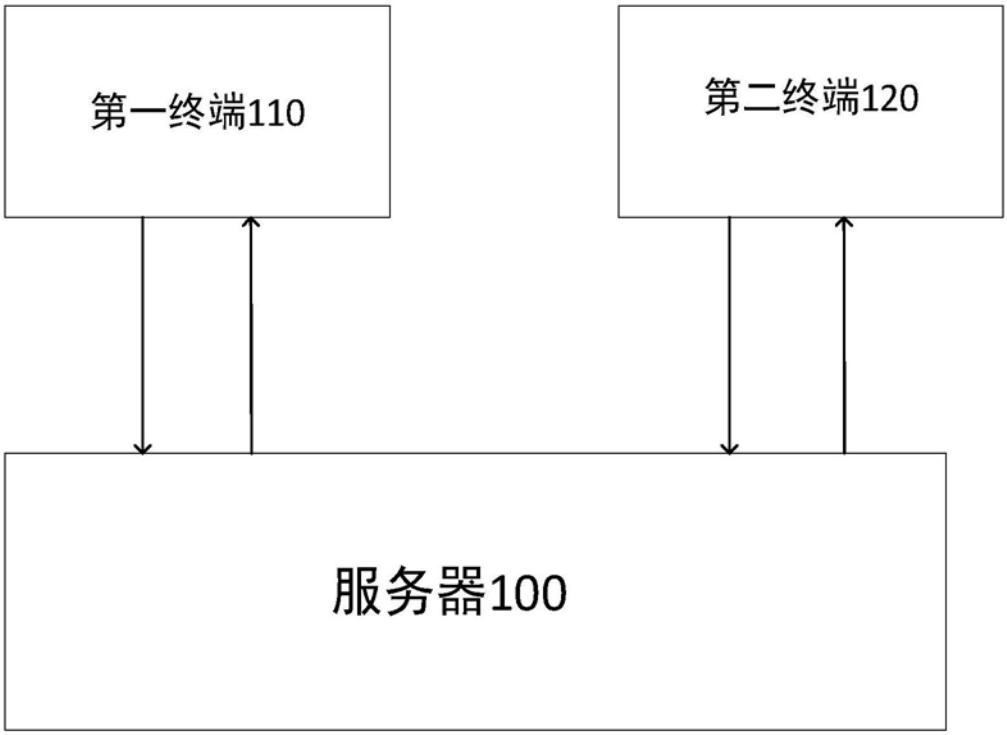


图1

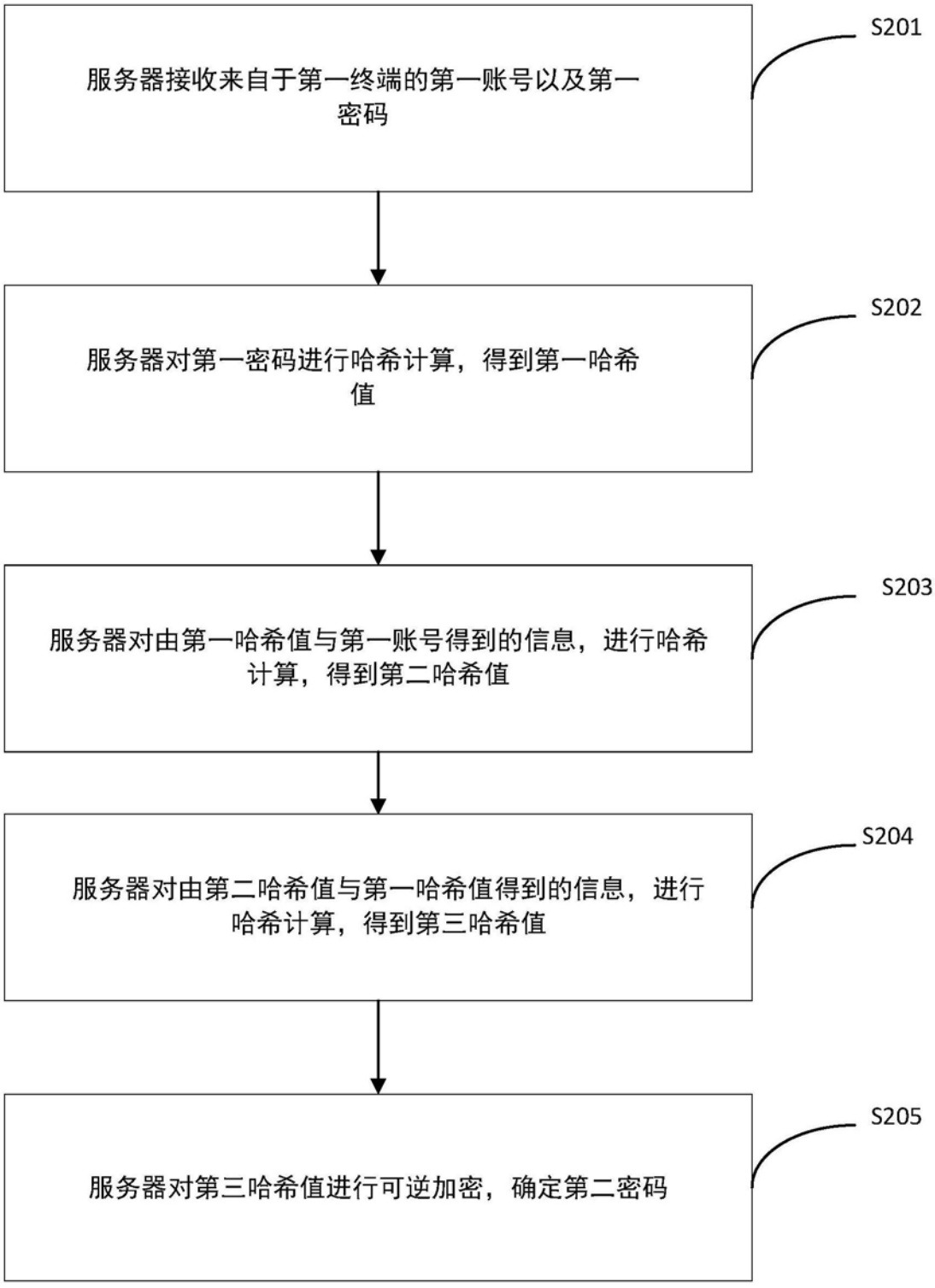

服务器接收来自于第一终端的第一账号以及第一密码
S201
服务器对第一密码进行哈希计算，得到第一哈希值
S202
服务器对由第一哈希值与第一账号得到的信息，进行哈希计算，得到第二哈希值
S203
服务器对由第二哈希值与第一哈希值得到的信息，进行哈希计算，得到第三哈希值
S204
服务器对第三哈希值进行可逆加密，确定第二密码
S205

图2

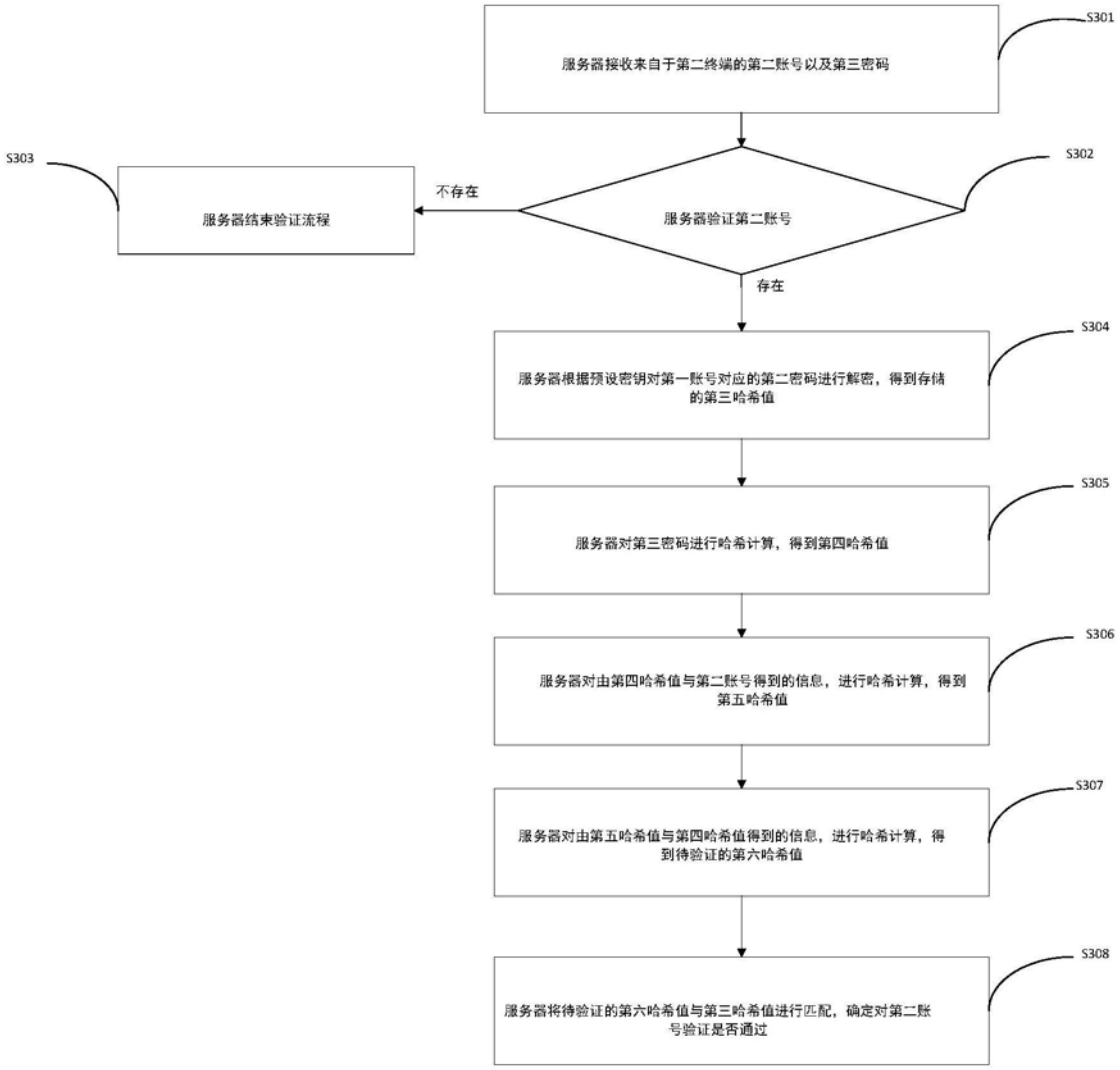

服务器接收来自于第二终端的第二账号以及第三密码
S301
服务器验证第二账号
S302
不存在
S303
服务器结束验证流程
存在
服务器根据预设密钥对第一账号对应的第二密码进行解密，得到存储的第三哈希值
S304
服务器对第三密码进行哈希计算，得到第四哈希值
S305
服务器对由第四哈希值与第二账号得到的信息，进行哈希计算，得到第五哈希值
S306
服务器对由第五哈希值与第四哈希值得到的信息，进行哈希计算，得到待验证的第六哈希值
S307
服务器将待验证的第六哈希值与第三哈希值进行匹配，确定对第二账号验证是否通过
S308

图3

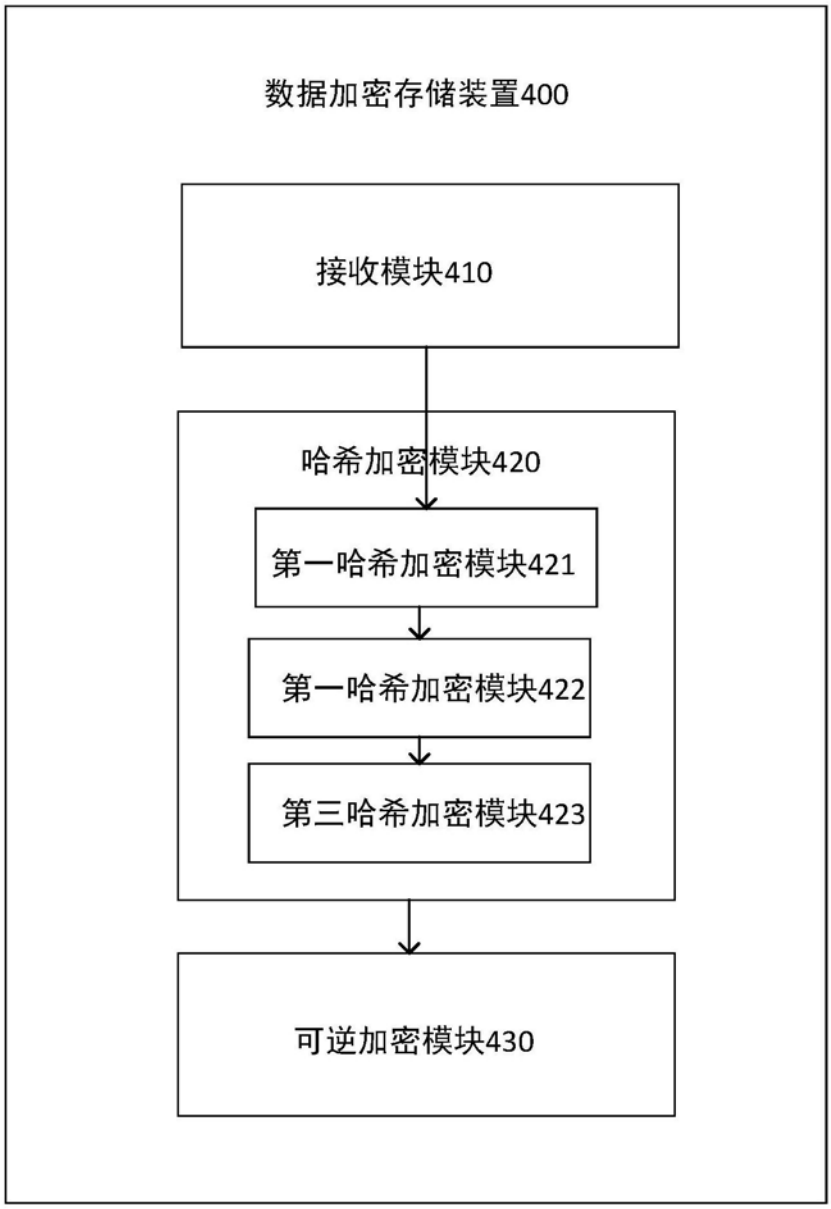

数据加密存储装置400
接收模块410
哈希加密模块420
第一哈希加密模块421
第一哈希加密模块422
第三哈希加密模块423
可逆加密模块430

图4

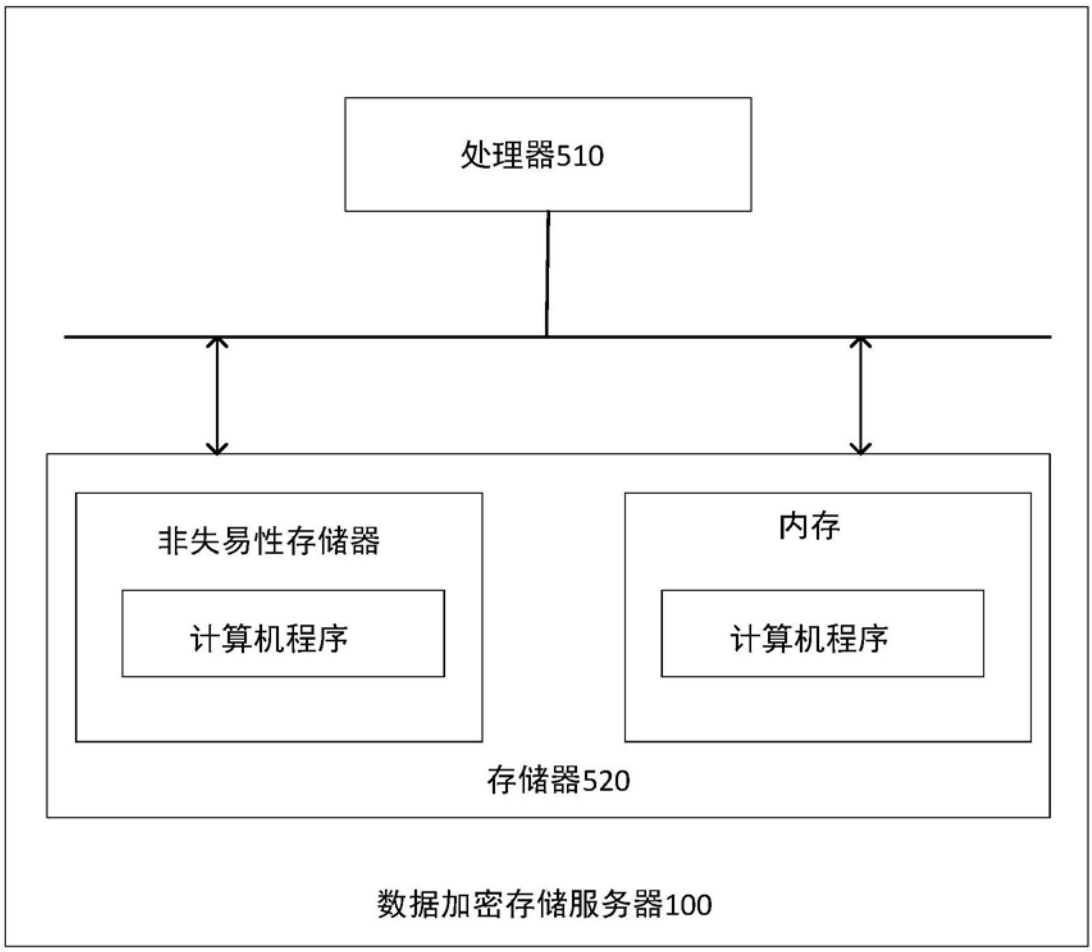


图5