(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 104639528 A
(43)申请公布日 2015.05.20

(21)申请号 201410663806.9

(22)申请日 2014.11.19

(71)申请人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号

(72)发明人 刘镝 张云勇 张尼 王笑帝

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 李丹 栗若木

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
G10L 17/08(2013.01)

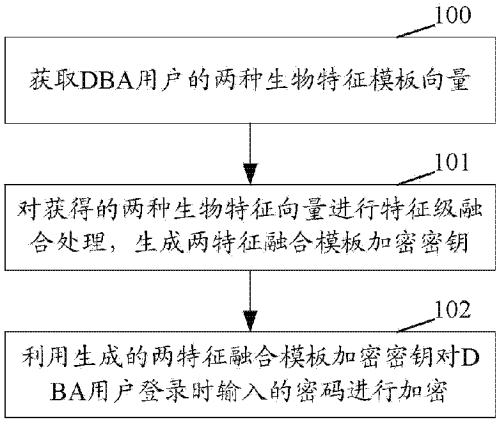
权利要求书2页 说明书11页 附图2页

(54)发明名称

一种DBA移动客户端反攻击方法及装置

(57)摘要

本发明公开了一种DBA移动客户端反攻击方法及装置，包括获取DBA用户的两种生物特征模板向量；对获得的两种生物特征向量进行特征级融合处理，生成两特征融合模板加密密钥；利用生成的两特征融合模板加密密钥对DBA用户登录时输入的密码进行加密。本发明的特征融合模板加密密钥是在云数据库管理机房中，DBA用户使用DBA移动客户端与注册系统协商生成的，不通过网络信道传输，因此，中间人代理服务器不可能同时具备DBA用户的指纹、声纹特征以及融合后的特征融合模板加密密钥；而且，特征融合模板加密密钥的空间很大，不可能破解得出整个密钥具体信息。通过本发明的DBA移动客户端反攻击方法，实现了DBA用户个人隐私信息的有效保护。



CN 104639528 A

1. 一种云平台数据库管理员 DBA 移动客户端反攻击方法，其特征在于，包括：获取 DBA 用户的两种生物特征模板向量；

对获得的两种生物特征向量进行特征级融合处理，生成两特征融合模板加密密钥；

利用生成的两特征融合模板加密密钥对 DBA 用户登录时输入的密码进行加密。

2. 根据权利要求 1 所述的 DBA 移动客户端反攻击方法，其特征在于，所述获取 DBA 用户的两种生物特征模板向量包括：

通过生物样本注册系统录入两种生物样本；根据预先设置的特征提取算法提取两种生物样本的生物特征模板向量。

3. 根据权利要求 2 所述的 DBA 移动客户端反攻击方法，其特征在于，所述两种生物样本为声纹样本，及指纹样本；

所述两种生物样本的生物特征模板向量为声纹特征模板向量、指纹关键点模板向量。

4. 根据权利要求 3 所述的 DBA 移动客户端反攻击方法，其特征在于，所述生成两特征融合模板加密密钥包括：

对所述两种生物样本对应的特征模板向量进行特征级拼接融合；

根据用户设置的密码的位数，及所述声纹特征模板向量和指纹关键点模板向量，获取两特征融合模板加密密钥。

5. 根据权利要求 1 所述的 DBA 移动客户端反攻击方法，其特征在于，对于所述两种生物样本中的指纹样本，所述获取生物特征模板向量包括：

针对预设数量 n_{finger} 张指纹样本，先按照下式提取出每张指纹交叉点的坐标 F_i，其中，$i = 1 \cdots n_{finger}$：

$$F_i = \left\{ < x_{i,1}, y_{i,1} >, < x_{i,2}, y_{i,2} >, \cdots, < x_{i,n_{fingerfeature}}, y_{i,n_{fingerfeature}} > \right\}, i = 1 \cdots n_{finger}$$；其　中，

$n_{fingerfeature}$ 为第 i 个指纹图像上的交叉点的个数，且假设每张指纹图像具备相等个数的交叉点，均为 $n_{fingerfeature}$ 个；

将上式中的每个二元组中横坐标、纵坐标的数值相加求平均，得到下式所示的一维向量：

$$F_i^{'} = \left\{ \frac{x_{i,1} + y_{i,1}}{2}, \frac{x_{i,2} + y_{i,2}}{2}, \cdots, \frac{x_{i,n_{fingerfeature}} + y_{i,n_{fingerfeature}}}{2} \right\}, i = 1 \cdots n_{finger}$$；

最终得到下式所示的 n_{finger} 张指纹交叉点的矩阵作为所示指纹关键点模板向量 $a_{template}$：

$$F = \begin{vmatrix} F_1^{'} \\ F_2^{'} \\ \vdots \\ F_{n_{finger}}^{'} \end{vmatrix} = \begin{vmatrix} \frac{x_{1,1} + y_{1,1}}{2} & \frac{x_{1,2} + y_{1,2}}{2} & \cdots & \frac{x_{1,n_{fingerfeature}} + y_{1,n_{fingerfeature}}}{2} \\ \frac{x_{2,1} + y_{2,1}}{2} & \frac{x_{2,2} + y_{2,2}}{2} & \cdots & \frac{x_{2,n_{fingerfeature}} + y_{2,n_{fingerfeature}}}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{x_{n_{finger},1} + y_{n_{finger},1}}{2} & \frac{x_{n_{finger},2} + y_{n_{finger},2}}{2} & \cdots & \frac{x_{n_{finger},n_{fingerfeature}} + y_{n_{finger},n_{fingerfeature}}}{2} \end{vmatrix}$$。

6.一种 DBA 移动客户端反攻击装置，其特征在于，设置在云数据库管理机房中，至少包括获取单元、融合单元，以及加密单元；其中，

获取单元，用于获取 DBA 用户的两种生物特征模板向量；

融合单元，用于对获得的两种生物特征向量进行特征级融合处理，生成两特征融合模板加密密钥；

加密单元，用于利用生成的两特征融合模板加密密钥对 DBA 用户登录时输入的密码进行加密。

7.根据权利要求 6 所述的 DBA 移动客户端反攻击装置，其特征在于，所述获取单元具体包括采集模块，以及处理模块；其中，

采集模块，用于通过生物样本注册系统的 MIC 和指纹采集器，录入声纹样本和指纹样本两种生物样本；

处理模块，用于按照预先设置的特征提取算法，对采集到的声纹样本和指纹样本获取两种生物样本提取特征，获得声纹特征模板向量和指纹关键点模板向量两种生物特征模板向量。

8.根据权利要求 7 所述的 DBA 移动客户端反攻击装置，其特征在于，

所述融合单元，具体用于对所述两种生物样本对应的特征模板向量进行特征级拼接融合；根据用户设置的密码的位数，及所述声纹特征模板向量和指纹关键点模板向量，获取两特征融合模板加密密钥。

一种 DBA 移动客户端反攻击方法及装置

技术领域

[0001] 本发明涉及声纹特征识别技术，尤指一种云平台数据库管理员 (DBA，Database Administrator) 移动客户端反攻击方法及装置。

背景技术

[0002] 随着云计算技术的不断演进，大量云平台不断涌现，如亚马逊 (Amazon) 的 AWS，国内的阿里云，沃云等平台。这些云平台的强大的计算能力已经被广泛地用于国民生产领域，如 12306 火车票订票网站、阿里巴巴的淘宝平台等。这些云平台将海量的用户数据存储于云平台的数据库区。

[0003] 云平台的数据量极大，这无形中加重了云平台数据库管理员 (DBA，Database Administrator) 的管理、维护负担。而且，用于存放云平台的基于互联网的数据中心 (IDC，Internet Data Center) 的地理位置通常与 DBA 的办公区所在地具有一定的物理距离。为了更为方便地维护、管理云平台数据库，云平台 DBA 往往采取将数据库管理系统映射到公网上的方式，通过公网 IP 登入该地址，进行云平台数据库的管理、运维工作。但是，这种管理方法存在两方面缺陷 :一方面，黑客可通过公网 IP 地址攻击数据库管理系统，例如向该 IP 地址发起分布式拒绝服务 (DDoS，Distributed Denial of Service) 攻击，导致整个云平台数据库区，乃至整个云平台门户瘫痪 ;另一方面，由于云平台数据库承载着大量的数据，需要 DBA 时刻关注数据库态势，出于安全考虑，当 DBA 人员不在办公区域内时，无法通过办公区域内的 PC 终端实时登录访问数据库管理系统，从而不能对数据库进行实时维护控制。

[0004] 针对以上两点缺陷，目前业内已经考虑设计一种为 DBA 深度定制的移动客户端系统。由于是远程客户端登录，保障 DBA 安全登录尤为重要。虽然开发商普遍采用以安全为目标的 HTTP 通道 (HTTPS，Hyper Text Transfer Protocol over Secure Socket Layer，也称 HTTP 的安全版) 等网络传输加密协议对移动客户端至 IDC 中的后台云数据库管理服务器之间的链路进行加密。 但是，如果黑客发起中间人攻击，如中间人代理攻击方式，现有网络加密协议并不能保护 DBA 客户端输入的明文密码，也就是说这种方式仍然不能确保 DBA 在使用客户端过程中，密码不被黑客所窃取。其中，中间人代理攻击方式为 :黑客在互联网中部署一台中间人代理服务器，该中间人代理服务器可分别与 DBA 移动客户端、后台云数据库管理服务器建立两端单独的网络加密传输链路。使得后台云数据库管理服务器误认为中间人代理服务器即为 DBA 移动客户端，并与之正常交互。而 DBA 移动客户端误认为中间人代理服务器即为后台云数据库管理服务器，并与之实现正常交互。这样，中间人代理服务器通过获取的移动客户端生成密钥解密网络流量内容，从中获取 DBA 用户明文密码，最终造成用户信息泄露的严重局面。

[0005] 如果采用业内传统的密钥加密手段对用户登录输入的密码进行加密，也就是说，在 DBA 移动客户端与后台云数据库管理服务器之间建立 HTTPS 之后，再建立一套新的证书 (公钥) 远程交换协商机制。那么，这套机制同样面临着中间人代理服务器攻击，中间人代理服务器还是会采用同样的方式破解密钥，从而获取用户名、密码。

[0006] 综上所述，目前的 DBA 移动客户端反攻击方案中，不能防止中间人代理攻击，从而不能达到保证用户信息安全的目的。

发明内容

[0007] 为了解决上述技术问题，本发明提供了一种 DBA 移动客户端反攻击方法及装置，能够有效防止中间人代理攻击，从而达到保证用户信息安全的目的。

[0008] 为了达到本发明目的，本发明提供了一种云平台数据库管理员 DBA 移动客户端反攻击方法，包括：获取 DBA 用户的两种生物特征模板向量；

[0009] 对获得的两种生物特征向量进行特征级融合处理，生成两特征融合模板加密密钥；

[0010] 利用生成的两特征融合模板加密密钥对 DBA 用户登录时输入的密码进行加密。

[0011] 所述获取 DBA 用户的两种生物特征模板向量包括：

[0012] 通过生物样本注册系统录入两种生物样本；根据预先设置的特征提取算法提取两种生物样本的生物特征模板向量。

[0013] 所述两种生物样本为声纹样本，及指纹样本；

[0014] 所述两种生物样本的生物特征模板向量为声纹特征模板向量、指纹关键点模板向量。

[0015] 所述生成两特征融合模板加密密钥包括：

[0016] 对所述两种生物样本对应的特征模板向量进行特征级拼接融合；

[0017] 根据用户设置的密码的位数，及所述声纹特征模板向量和指纹关键点模板向量，获取两特征融合模板加密密钥。

[0018] 对于所述两种生物样本中的指纹样本，所述获取生物特征模板向量包括：

[0019] 针对预设数量 n_{finger} 张指纹样本，先按照下式提取出每张指纹交叉点的坐标 F_i，其中，$i = 1 \cdots n_{finger}$：

[0020] $$F_i = \left\{ < x_{i,1}, y_{i,1} >, < x_{i,2}, y_{i,2} >, \cdots, < x_{i,n_{fingerfeature}}, y_{i,n_{fingerfeature}} > \right\}, i = 1 \cdots n_{finger}$$；其中，$n_{fingerfeature}$ 为第 i 个指纹图像上的交叉点的个数，且假设每张指纹图像具备相等个数的交叉点，均为 $n_{fingerfeature}$ 个；

[0021] 将上式中的每个二元组中横坐标、纵坐标的数值相加求平均，得到下式所示的一维向量：

[0022] $$F_i' = \left\{ \frac{x_{i,1} + y_{i,1}}{2}, \frac{x_{i,2} + y_{i,2}}{2}, \cdots, \frac{x_{i,n_{fingerfeature}} + y_{i,n_{fingerfeature}}}{2} \right\}, i = 1 \cdots n_{finger}$$；

[0023] 最终得到下式所示的 n_{finger} 张指纹交叉点的矩阵作为所示指纹关键点模板向量 $a_{template}$：

[0024]

$$F=\left|\begin{matrix}F_1'\\F_2'\\\vdots\\F_{n_{finger}}'\end{matrix}\right|=\left|\begin{matrix}\frac{x_{1,1}+y_{1,1}}{2} & \frac{x_{1,2}+y_{1,2}}{2} & \cdots & \frac{x_{1,n_{fingerfeature}}+y_{1,n_{fingerfeature}}}{2}\\ \frac{x_{2,1}+y_{2,1}}{2} & \frac{x_{2,2}+y_{2,2}}{2} & \cdots & \frac{x_{2,n_{fingerfeature}}+y_{2,n_{fingerfeature}}}{2}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{x_{n_{finger},1}+y_{n_{finger},1}}{2} & \frac{x_{n_{finger},2}+y_{n_{finger},2}}{2} & \cdots & \frac{x_{n_{finger},n_{fingerfeature}}+y_{n_{finger},n_{fingerfeature}}}{2}\end{matrix}\right|。$$

[0025] 本发明还公开了一种 DBA 移动客户端反攻击装置，设置在云数据库管理机房中，至少包括获取单元、融合单元，以及加密单元；其中，

[0026] 获取单元，用于获取 DBA 用户的两种生物特征模板向量；

[0027] 融合单元，用于对获得的两种生物特征向量进行特征级融合处理，生成两特征融合模板加密密钥；

[0028] 加密单元，用于利用生成的两特征融合模板加密密钥对 DBA 用户登录时输入的密码进行加密。

[0029] 所述获取单元具体包括采集模块，以及处理模块；其中，

[0030] 采集模块，用于通过生物样本注册系统的 MIC 和指纹采集器，录入声纹样本和指纹样本两种生物样本；

[0031] 处理模块，用于按照预先设置的特征提取算法，对采集到的声纹样本和指纹样本获取两种生物样本提取特征，获得声纹特征模板向量和指纹关键点模板向量两种生物特征模板向量。

[0032] 所述融合单元，具体用于对所述两种生物样本对应的特征模板向量进行特征级拼接融合；根据用户设置的密码的位数，及所述声纹特征模板向量和指纹关键点模板向量，获取两特征融合模板加密密钥。

[0033] 与现有技术相比，本发明包括获取 DBA 用户的两种生物特征模板向量；对获得的两种生物特征向量进行特征级融合处理，生成两特征融合模板加密密钥；利用生成的两特征融合模板加密密钥对 DBA 用户登录时输入的密码进行加密。本发明提供的 DBA 移动客户端反攻击方法，由于特征融合模板加密密钥是在云数据库管理机房中，DBA 用户使用 DBA 移动客户端与注册系统协商生成的，不通过网络信道传输，因此，中间人代理服务器不可能同时具备 DBA 用户的指纹、声纹特征以及融合后的特征融合模板加密密钥，因此，中间代理人服务器仅能获得加密后的密码密文（即唯密文攻击场景），而且，特征融合模板加密密钥的空间很大，不可能破解得出整个密钥具体信息。因此，中间代理人服务器是不能破解得到 DBA 密码明文的，也就是说，通过本发明的 DBA 移动客户端反攻击方法，实现了 DBA 用户个人隐私信息的有效保护。

[0034] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0035] 附图用来提供对本发明技术方案的进一步理解，并且构成说明书的一部分，与本申请的实施例一起用于解释本发明的技术方案，并不构成对本发明技术方案的限制。

[0036] 图 1 为本发明 DBA 移动客户端反攻击方法的流程图；

[0037] 图 2 为本发明 DBA 移动客户端反攻击装置的组成结构示意图；

[0038] 图 3 为本发明 DBA 移动客户端反攻击方法的实施例的流程示意图。

具体实施方式

[0039] 为使本发明的目的、技术方案和优点更加清楚明白，下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0040] 在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行。并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0041] 生物模板加密技术，是利用具有唯一性的人体生物特征作为密钥，如指纹、面部、声音等，本申请发明人考虑，利用生物模板加密技术对 DBA 移动客户端用户登录时输入的密码进行加密。由于中间代理服务器不具备用户的真实生物特征。因此，在唯密文攻击即仅有加密后的用户密码，无生物模板密钥、无相关先前被破解的用户名密码明文的情况下，中间人代理服务器很难破解出用户真实密码。因此，比传统的密钥加密方式更为安全。

[0042] 生物模板加密技术具备较好的安全性，在普通环境下，可以实现用户的安全登录。但是，本申请发明人发现，在云数据库 DBA 移动客户端环境下，需要考虑到底使用哪种适当的生物样本对 DBA 移动客户端的身份信息进行 加密保护：

[0043] 如果采用面部图像进行身份认证，在手机采集到用户登录面部图像样本存在发型服饰改变、遮蔽、复杂背景等时，会造成采集时出现的误差；

[0044] 如果采用虹膜进行身份认证，保密性同样存在问题，例如隐藏的图像采集装置可能会盗拍用户的虹膜；而且，由于虹膜识别一般采集虹膜红外图像，用户接受度低，在采集过程中 DBA 用户会担心自己的眼部受到伤害；

[0045] 如果采用指纹图像进行身份认证，指纹识别作为一种成熟的生物认证手段，其精度、稳定性均已被业内广泛接受，但是，指纹识别的保密性存在一定问题，比如，攻击者可能从用户摸过的杯子等物品盗窃用户指纹，从而假冒真实身份强行登录；

[0046] 如果采用声纹识别则是一种比较理想的选择。声纹采集器价格低廉，如手机上的麦克风 (MIC)。针对生物特征被盗取问题，如果攻击者盗录了某次用户的话语录音，系统在登录验证时，可规定测试话语内容，从而避免攻击者利用盗录录音仿冒身份录音。但是，发明人发现，传统的单模态声纹认证算法还是存在一些缺陷，主要包括：单一的声纹特征提取方式会造成系统性能下降。利用单一特征提取方法采集的特征向量，不能完全代表原始生物样本的特点，即不能完全反映出其可分性信息 (Discriminatory information)，从而导致了系统加解密时识别精度的下降。

[0047] 为了克服以上问题，信息融合思想即两种或多种生物特征认证融合技术被引入声纹特征识别领域中。以两种生物特征融合为例，该技术可以采用两种不同的传感器如 MIC 与指纹采集器，分别采集到的两种不同的生物特征信号即用户话语录音与指纹，并利用两

种不同的特征提取算法提取两种不同的特征向量，再利用一定的融合方式，如特征级融合方案，将这些提取的特征进行拼接融合，最后，通过融合后的可分性信息作为识别个人身份的关键特征，使得系统更好地实现对 DBA 移动客户端的用户密码的加密保护功能。

[0048] 图 1 为本发明 DBA 移动客户端反攻击方法的流程图，如图 1 所示，包括以下步骤：

[0049] 步骤 100：获取 DBA 用户的两种生物特征模板向量。具体包括：

[0050] 首先，待注册的 DBA 用户可以通过生物样本注册系统录入两种生物样本，比如：根据语音提示内容，DBA 用户通过注册系统的 MIC 录入长约 3-5 分钟的规定内容的语音信息作为声纹样本；通过注册系统的指纹采集器，采集预设数量 n_{finger} 如 50 张的 DBA 用户的指纹图像信息作为指纹样本。

[0051] 然后，获取两种生物样本的生物特征模板向量，即指纹关键点模板向量 $a_{template}$ 与声纹特征模板向量 $b_{template}$。具体地，生物样本注册系统可以针对注册的 DBA 用户的两种不同生物样本即指纹与声纹，根据预先设置的特征提取算法提出相应的生物特征模板向量。举例来看：

[0052] 比如，针对预设数量 n_{finger} 张指纹样本，先按照公式 (1) 提取出每张指纹交叉点的坐标 F_i，其中，$i = 1 \cdots n_{finger}$：

[0053]

$$F_i = \left\{ < x_{i,1}, y_{i,1} >, < x_{i,2}, y_{i,2} >, \cdots, < x_{i,n_{fingerfeature}}, y_{i,n_{fingerfeature}} > \right\}, i = 1 \cdots n_{finger} \quad (1)$$

[0054] 在公式 (1) 中，$n_{fingerfeature}$ 为第 i 个指纹图像上的交叉点的个数，为方便运算，可假设每张指纹图像具备相等个数的交叉点，均为 $n_{fingerfeature}$ 个。

[0055] 再将以上每个二元组中横坐标、纵坐标的数值相加求平均，即变为如公式 (2) 所示的一维向量 F_i'：

[0056]

$$F_i' = \left\{ \frac{x_{i,1} + y_{i,1}}{2}, \frac{x_{i,2} + y_{i,2}}{2}, \cdots, \frac{x_{i,n_{fingerfeature}} + y_{i,n_{fingerfeature}}}{2} \right\}, i = 1 \cdots n_{finger} \quad (2)$$

[0057] 那么，最终可以得到如公式 (3) 所示的 n_{finger} 张指纹交叉点的矩阵 F 即指纹关键点模板向量 $a_{template}$：

[0058]

$$F = \begin{vmatrix} F_1' \\ F_2' \\ \vdots \\ F_{n_{finger}}' \end{vmatrix} = \begin{vmatrix} \frac{x_{1,1} + y_{1,1}}{2} & \frac{x_{1,2} + y_{1,2}}{2} & \cdots & \frac{x_{1,n_{fingerfeature}} + y_{1,n_{fingerfeature}}}{2} \\ \frac{x_{2,1} + y_{2,1}}{2} & \frac{x_{2,2} + y_{2,2}}{2} & \cdots & \frac{x_{2,n_{fingerfeature}} + y_{2,n_{fingerfeature}}}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{x_{n_{finger},1} + y_{n_{finger},1}}{2} & \frac{x_{n_{finger},2} + y_{n_{finger},2}}{2} & \cdots & \frac{x_{n_{finger},n_{fingerfeature}} + y_{n_{finger},n_{fingerfeature}}}{2} \end{vmatrix} \quad (3)$$

[0059] 针对 DBA 用户注册录入的声纹样本，注册系统可以利用业内常用的 MFCC 特征提取算法提取 MFCC 特征 E 即声纹特征模板向量 $b_{template}$，如公式 (4) 所示：

[0060]

$$E=\begin{vmatrix}E_1\\E_2\\\vdots\\E_{n_{Frame}}\end{vmatrix}=\begin{vmatrix}e_{1,1} & e_{1,2} & \cdots & e_{1,n_{efficient}}\\e_{2,1} & e_{2,2} & \cdots & e_{2,n_{efficient}}\\\vdots & \vdots & \ddots & \vdots\\e_{n_{Frame},1} & e_{n_{Frame},2} & \cdots & e_{n_{Frame},n_{efficient}}\end{vmatrix} \quad (4)$$

[0061] 在公式(4)中，$n_{efficient}$为第j帧语音信号片段对应的MFCC系数，如公式(4)所示，共有n_{Frame}帧语音信号片段。

[0062] 本步骤中，DBA用户通过注册系统输入新创建的密码，系统自动识别密码位数为n_{cipher}，这里，一般用户设置的密码不会超过20位。因此，密码位数远小于指纹图像个数与声纹帧数的和、小于指纹向量元素个数，也小于声纹特征向量元素个数，也就是说：

$$n_{cipher} \ll n_{Frame}+n_{finger}$$

$$n_{cipher} \ll n_{fingerfeature}, \quad 。$$

$$n_{cipher} \ll n_{efficient}$$

[0063] 步骤101：对获得的两种生物特征向量进行特征级融合处理，生成两特征融合模板加密密钥。

[0064] 本步骤具体包括：将两种生物样本对应的特征模板向量进行特征级拼接融合，且系统根据用户设置的登录的密码的位数n_{cipher}，最终得到$n_{cipher}\times n_{cipher}$维度矩阵k即两特征融合模板加密密钥，如公式(5)所示：

[0065]

$$k=\begin{vmatrix}F_{cipher}\\E_{cipher}\end{vmatrix}=\begin{vmatrix}\frac{x_{1,1}+y_{1,1}}{2} & \frac{x_{1,2}+y_{1,2}}{2} & \cdots & \frac{x_{1,n_{cipher}}+y_{1,n_{cipher}}}{2}\\\vdots & \vdots & \cdots & \vdots\\\frac{x_{\frac{n_{cipher}}{2},1}+y_{\frac{n_{cipher}}{2},1}}{2} & \frac{x_{\frac{n_{cipher}}{2},2}+y_{\frac{n_{cipher}}{2},2}}{2} & \cdots & \frac{x_{\frac{n_{cipher}}{2},n_{cipher}}+y_{\frac{n_{cipher}}{2},n_{cipher}}}{2}\\e_{\frac{n_{cipher}}{2}+1,1} & e_{\frac{n_{cipher}}{2}+1,2} & \cdots & e_{\frac{n_{cipher}}{2}+1,n_{cipher}}\\\vdots & \vdots & \cdots & \vdots\\e_{n_{cipher},1} & e_{n_{cipher},1} & \cdots & e_{n_{cipher},n_{cipher}}\end{vmatrix} \quad (5)$$

[0066] 其中，特征级拼接融合属于现有技术，即将两种不同生物特征向量（维度相同）融合到一起，生成新的融合后的向量，如公式(5)所示，其具体实 现过程并不用于限定本发明的保护范围，这里不再赘述。

[0067] 根据密码学理论，密码体制中需要选择一种加密密钥，且用户获取加密密钥必须处于完全安全的环境下。目前有两种方式用户获取加密密钥：一种是，加密方与解密方在同一地点协商密钥；另一种是，使用安全信道传输密钥。由于云数据库管理移动客户端属于专业深度定制客户端，安全级别较高。因此，本发明采用加密方与解密方在同一地点协商密钥

的方式来获取加密秘钥。这样，就要求DBA用户在云数据库管理机房内，制作专属自己的上述两生物特征融合模板加密密钥。

[0068] 本发明中，DBA远程管理客户端注册系统可以通过USB接驳将生成的两特征融合模板加密密钥传至客户端并存储，同时，将生成的两特征融合模板加密密钥发送至云数据库管理服务器对应的用户数据库并保存。其中，USB接驳是指通过USB接口，一端是DBA远程管理客户端注册系统（备有USB插口），另一端是用户手机。例如，安卓手机数据充电线。

[0069] 步骤102：利用生成的两特征融合模板加密密钥对DBA用户登录时输入的密码进行加密。

[0070] 本步骤的具体实现属于本领域技术人员的惯用技术手段，并不用于限定本发明的保护范围，这里不再赘述。

[0071] 本发明提供的DBA移动客户端反攻击方法中，由于特征融合模板加密密钥是在云数据库管理机房中，DBA用户使用DBA移动客户端与注册系统协商生成的，不通过网络信道传输，因此，中间人代理服务器不可能同时具备DBA用户的指纹、声纹特征以及融合后的特征融合模板加密密钥，因此，中间代理人服务器仅能获得加密后的密码密文（即唯密文攻击场景），而且，特征融合模板加密密钥的空间很大，不可能破解得出整个密钥具体信息。因此，中间代理人服务器是不能破解得到DBA密码明文的，也就是说，通过本发明的DBA移动客户端反攻击方法，实现了DBA用户个人隐私信息的有效保护。

[0072] 需要说明的是，由于指纹和声纹两种生物特征好采集且采集器成本低、通用，因此，从实际应用角度出发，本发明采用两种生物特征向量融合，即选取指纹、声纹特征向量进行特征融合，得到融合特征向量，再生成两特征 模板生物密钥。但是，对于三种或三种以上的生物特征融合情况，理论上也是可行的，即将三种生物特征对应的特征向量进行融合，得到融合后的向量生成三特征模板生物密钥。比如再增加面部图像、虹膜以及相关采集器等，在本发明提供的发明思想的基础上，对于本领域技术人员是具有技术启示的，而且对于本领域技术人员来讲，也是不难实现的，因此，应属于本发明的保护范围。

[0073] 图2为本发明DBA移动客户端反攻击装置的组成结构示意图，本发明DBA移动客户端反攻击装置设置在云数据库管理机房中，如图2所示，至少包括获取单元、融合单元，以及加密单元；其中，

[0074] 获取单元，用于获取DBA用户的两种生物特征模板向量；

[0075] 融合单元，用于对获得的两种生物特征向量进行特征级融合处理，生成两特征融合模板加密密钥；

[0076] 加密单元，用于利用生成的两特征融合模板加密密钥对DBA用户登录时输入的密码进行加密。

[0077] 其中，获取单元具体包括采集模块，以及处理模块；具体地：

[0078] 采集模块，用于通过生物样本注册系统的MIC和指纹采集器，录入声纹样本和指纹样本两种生物样本；

[0079] 处理模块，用于按照预先设置的特征提取算法，对采集到的声纹样本和指纹样本获取两种生物样本提取特征，获得声纹特征模板向量和指纹关键点模板向量两种生物特征模板向量。

[0080] 其中，融合单元具体用于：对两种生物样本对应的特征模板向量进行特征级拼接

融合；根据用户设置的密码的位数，及声纹特征模板向量和指纹关键点模板向量，获取两特征融合模板加密密钥。

[0081] 图 3 为本发明 DBA 移动客户端反攻击方法的实施例的流程示意图，图 3 所示的实施例描述了 DBA 用户登录时，对输入密码加密、后台云平台管理服务器解密，以及当黑客发起中间人攻击，利用本发明的两特征融合模板加密密钥进行加密来保护用户登录时输入的密码，以成功避开中间人代理服务器的窃取密码的过程，如图 3 所示，包括以下步骤：

[0082] 步骤 300：DBA 用户使用 DBA 移动客户端发起接入云数据库管理服务器的请求。

[0083] 步骤 301：中间人代理服务器发起拦截攻击，拦截到 DBA 发送的请求后，向 DBA 移动客户端返回响应，在响应中携带有中间人代理服务器的公钥。

[0084] 步骤 302 ～步骤 303：移动 DBA 客户端内部验证中间人代理服务器发送的公钥，并在验证成功后，随机生成新公钥。

[0085] 步骤 304：DBA 移动客户端利用中间人代理服务器的公钥加密新公钥。

[0086] 步骤 305：DBA 移动客户端传输加密后的新公钥至中间人代理服务器。

[0087] 步骤 306：中间人代理服务器利用其自身的公钥对收到的加密后的新公钥进行解密，获取 DBA 移动客户端新生成的新公钥。

[0088] 步骤 307：中间人代理服务器发送响应反馈信息，并采用新公钥加密。

[0089] 步骤 308：中间人代理服务器与 DBA 移动客户端建立加密信道，向 DBA 移动客户端反馈交互信息。

[0090] 步骤 309：至此，DBA 移动客户端与中间人代理服务器之间利用新公钥加密解密交互数据。

[0091] 步骤 310：中间人代理服务器发起接入云数据库管理服务器的请求。

[0092] 步骤 311：云数据库管理服务器向中间人代理服务器返回响应，在响应中携带有云数据库管理服务器公钥。

[0093] 步骤 312 ～步骤 313：中间人代理服务器验证云数据库管理服务器公钥可用性，并在云数据库管理服务器公钥可用时，随机生成一个新公钥。

[0094] 步骤 314：中间人代理服务器利用云数据库管理服务器公钥加密随机生成的新公钥。

[0095] 步骤 315：中间人代理服务器向云数据库管理服务器传输加密后的新公钥。

[0096] 步骤 316：云数据库管理服务器利用自身公钥解密获得的来自中间人代理服务器的加密后的新公钥。

[0097] 步骤 317：云数据库管理服务器反馈响应信息，并采用新公钥加密。

[0098] 步骤 318 ～步骤 319：至此，中间人代理服务器与云数据库管理服务器之间建立起加密信道，向中间人代理服务器反馈交互信息；

[0099] 步骤 320：云数据库管理 DBA 移动客户端，当 DBA 用户登录输入密码时，利用在注册过程中获取的两特征融合生物模板特征向量作为加密密钥 k，加密传输输入的用户密码信息，具体加密过程如下：

[0100] 首先，DBA 移动客户端利用预先设置的密码置换表，如表 1 所示，对 DBA 用户输入的用户密码明文进行置换，得到置换后的密码置换向量。

[0101]

字符	A	B	C	D	E	F	G	H	I	J
对应码	1	2	3	4	5	6	7	8	9	10
字符	K	L	M	N	O	P	Q	R	S	T
对应码	11	12	13	14	15	16	17	18	19	20
字符	U	V	W	X	Y	Z	A	b	c	d
对应码	21	22	23	24	25	26	27	28	29	30
字符	e	f	g	h	i	j	K	l	m	n
对应码	31	32	33	34	35	36	37	38	39	40
字符	o	p	q	r	s	t	U	v	w	x
对应码	41	42	43	44	45	46	47	48	49	50
字符	y	z	1	2	3	4	5	6	7	8
对应码	51	52	53	54	55	56	57	58	59	60
字符	9	0	～	!	@	#	$	%	^	&
对应码	61	62	63	64	65	66	67	68	69	70
字符	*	(	)	_	+	=	[	]	{	}
对应码	71	72	73	74	75	76	77	78	79	80

[0102] 表 1

[0103] 举例来看，比如用户登录 DBA 移动客户端时输入的密码为 :Asd12345，则根据表 1 置换后得到的向量为 (1,45,30,53,54,55,56,57)。这里，DBA 用户输入 密码明文对应的码表向量采用 $a = (a_1, a_2, \cdots, a_m)$ 表示，利用两生物特征模块加密后的密文采用 $s = (s_1, s_2, \cdots, s_m)$ 表示，两生物特征融合模板加密密钥采用 $k = \begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix}$ 表示，那么，利用两生物特征模块加密后的密文 s 如公式 (6) 所示 :

[0104]

$$s = a \cdot k = (a_1, a_2, \cdots, a_m) \begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix} \tag{6}$$

[0105] 将注册过程中生成的两生物特征融合模板加密密钥，如式 (5) 代入上公式 (6) 中，得到公式 (7) :

[0106]

$$s=(a_1,a_2,\cdots,a_m)\begin{vmatrix} \frac{x_{1,1}+y_{1,1}}{2} & \frac{x_{1,2}+y_{1,2}}{2} & \cdots & \frac{x_{1,n_{cipher}}+y_{1,n_{cipher}}}{2} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{x_{n_{cipher},1}+y_{n_{cipher},1}}{2} & \frac{x_{n_{cipher},2}+y_{n_{cipher},2}}{2} & \cdots & \frac{x_{n_{cipher},n_{cipher}}+y_{n_{cipher},n_{cipher}}}{2} \\ e_{n_{cipher}+1,1} & e_{n_{cipher}+1,2} & \cdots & e_{n_{cipher}+1,n_{cipher}} \\ \vdots & \vdots & \cdots & \vdots \\ e_{n_{cipher},1} & e_{n_{cipher},1} & \cdots & e_{n_{cipher},n_{cipher}} \end{vmatrix} \quad (7)$$

[0107] 步骤 321：由于中间人代理服务器没有 DBA 用户的指纹特征向量、声纹特征向量，且处于唯密文攻击场景下，因此，中间人代理服务器是不能破解两特征融合生物模板特征向量加密密钥的，从而无法获取用户的加密密码，只能将加密后的密码传输至云数据库管理服务器。

[0108] 步骤 322：云数据库管理服务器利用用户注册时获得的两生物融合特征向量加密秘钥对加密传输的 DBA 用户输入的用户密码信息进行解密，具体解密过程如下：

[0109] 云数据库管理服务器获取利用两生物特征模板密钥加密后的用户输入密 码密文 $s=(s_1,s_2,\cdots,s_m)$ 后，利用对应用户数据库内存储的 DBA 用户对应的两生物特征模板密钥对密文对其进行解密，将 $s=a\cdot k$ 公式改写后得到公式 (8)：

[0110] $a=s\cdot k^{-1}$ (8)

[0111] 在公式 (8) 中，k^{-1}表示加密密钥 k 的逆矩阵，将公式 (8) 展开后得到如下公式 (9)：

[0112]

$$a = s \cdot k^{-1} = (s_1, s_2 \cdots s_m) \cdot \begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix}^{-1}$$

$$= (s_1, s_2 \cdots s_m) \cdot \begin{vmatrix} \frac{x_{1,1}+y_{1,1}}{2} & \frac{x_{1,2}+y_{1,2}}{2} & \cdots & \frac{x_{1,n_{cipher}}+y_{1,n_{cipher}}}{2} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{x_{\frac{n_{cipher}}{2},1}+y_{\frac{n_{cipher}}{2},1}}{2} & \frac{x_{\frac{n_{cipher}}{2},2}+y_{\frac{n_{cipher}}{2},2}}{2} & \cdots & \frac{x_{\frac{n_{cipher}}{2},n_{cipher}}+y_{\frac{n_{cipher}}{2},n_{cipher}}}{2} \\ e_{\frac{n_{cipher}}{2}+1,1} & e_{\frac{n_{cipher}}{2}+1,2} & \cdots & e_{\frac{n_{cipher}}{2}+1,n_{cipher}} \\ \vdots & \vdots & \cdots & \vdots \\ e_{n_{cipher},1} & e_{n_{cipher},1} & \cdots & e_{n_{cipher},n_{cipher}} \end{vmatrix}^{-1} \quad (9)$$

[0113] 利用公式 (9)，可以获得 DBA 用户输入的密码对应的码表数字，再通过表 1 对 a 进行转换，最终转换为真实密码，最后利用得到的真实密码与对应的用户名进行登录验证，以完成登录过程。从图 3 所示的流程来看，及时中间服务器与云数据库管理服务器之间建立起了加密信道，但是，由于本发明中 DBA 用户输入的登录密码是采用 DBA 用户使用 DBA 移动客户端与注册系统在云数据库管理机房协商生成的特征融合模板加密密钥进行加密的，中间人代理服务器是无法获得 DBA 用户的指纹特征向量、声纹特征向量的，因此，整个过程确保了 DBA 用户密码不被中间人代理服务器窃取。

[0114] 之后，DBA 移动客户端与云数据库管理服务器登录交互的安全分析：当 DBA 用户在 DBA 移动客户端上登录输入用户名、密码时，DBA 移动客户端利用已获取的特征融合模板加密密钥对用户输入密码进行加密。虽然中间人代理服务器分别与 DBA 移动客户端、云数据库管理服务器建立两段传输加 密通道，中间人代理服务器可获取 DBA 用户名明文信息，但是，由于中间人服务器不具备注册系统分别利用某种特定算法提取到的生物特征，比如指纹交叉点坐标与声纹 MFCC 特征向量融合后的特征融合向量即两生物特征融合模板加密密钥，因此，中间人服务器仅可获取 DBA 用户加密后的密码密文，此种情况属于唯密文攻击场景，在此场景下，由于密文矩阵属于实数矩阵，实数矩阵的每一个元素空间很大 R = (1, 2, 3, …, z)，中间人服务器采用暴力破解 (brute-force) 方法精确地破解出生物模板加密密钥的元素值的概率微乎其微。因此，本发明提供的 DBA 移动客户端反攻击方法，成功地保护了 DBA 用户个人隐私，防止了中间人代理服务器窃取、破坏 DBA 用户信息。进一步放置了以冒用 DBA 身份的方式入侵云数据库管理平台的可能。

[0115] 虽然本发明所揭露的实施方式如上，但所述的内容仅为便于理解本发明而采用的实施方式，并非用以限定本发明。任何本发明所属领域内的技术人员，在不脱离本发明所揭露的精神和范围的前提下，可以在实施的形式及细节上进行任何的修改与变化，但本发明的专利保护范围，仍须以所附的权利要求书所界定的范围为准。

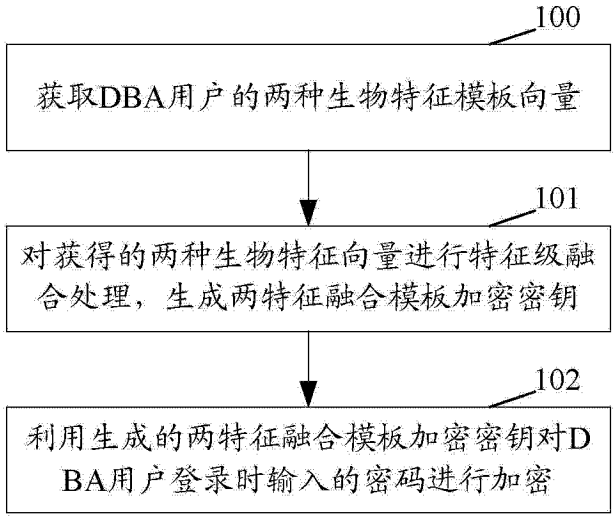

100
获取DBA用户的两种生物特征模板向量
101
对获得的两种生物特征向量进行特征级融合处理，生成两特征融合模板加密密钥
102
利用生成的两特征融合模板加密密钥对DBA用户登录时输入的密码进行加密

图 1

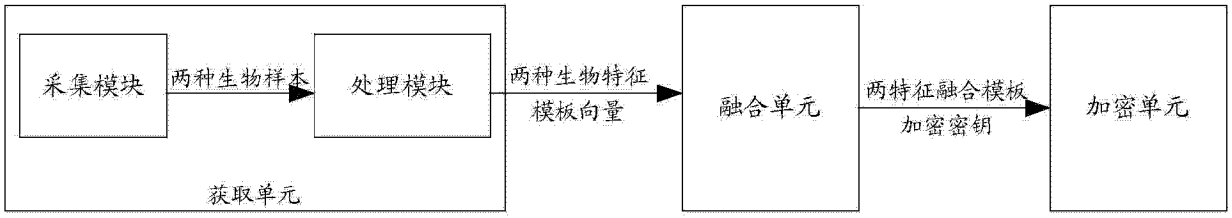

采集模块
两种生物样本
处理模块
获取单元
两种生物特征模板向量
融合单元
两特征融合模板加密密钥
加密单元

图 2

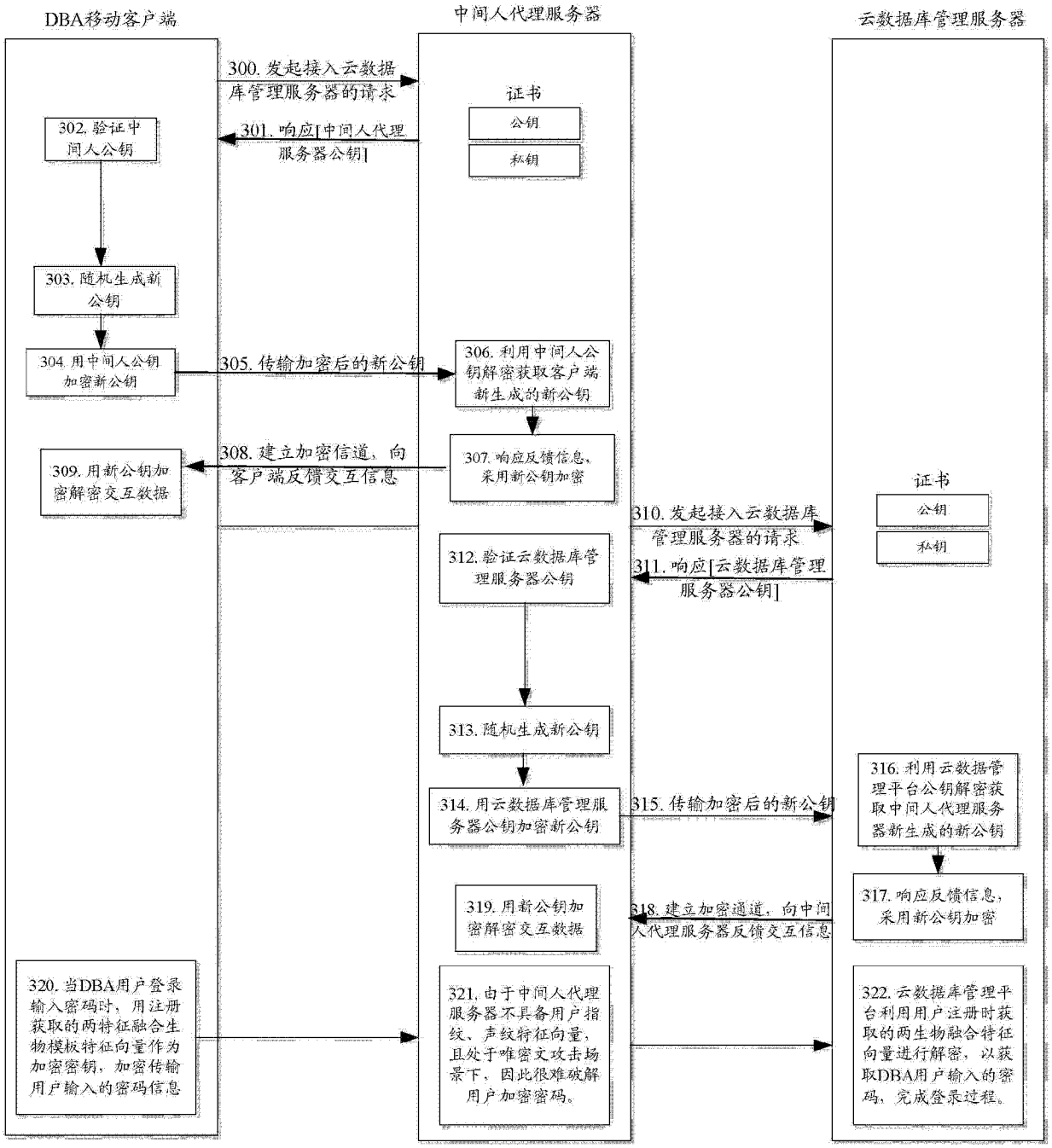

DBA移动客户端
中间人代理服务器
云数据库管理服务器
300. 发起接入云数据库管理服务器的请求
301. 响应[中间人代理服务器公钥]
证书
公钥
私钥
302. 验证中间人公钥
303. 随机生成新公钥
304. 用中间人公钥加密新公钥
305. 传输加密后的新公钥
306. 利用中间人公钥解密获取客户端新生成的新公钥
307. 响应反馈信息，采用新公钥加密
308. 建立加密信道，向客户端反馈交互信息
309. 用新公钥加密解密交互数据
310. 发起接入云数据库管理服务器的请求
311. 响应[云数据库管理服务器公钥]
证书
公钥
私钥
312. 验证云数据库管理服务器公钥
313. 随机生成新公钥
314. 用云数据库管理服务器公钥加密新公钥
315. 传输加密后的新公钥
316. 利用云数据管理平台公钥解密获取中间人代理服务器新生成的新公钥
317. 响应反馈信息，采用新公钥加密
318. 建立加密通道，向中间人代理服务器反馈交互信息
319. 用新公钥加密解密交互数据
320. 当DBA用户登录输入密码时，用注册获取的两特征融合生物模板特征向量作为加密密钥，加密传输用户输入的密码信息
321. 由于中间人代理服务器不具备用户指纹、声纹特征向量，且处于唯密文攻击场景下，因此很难破解用户加密密码。
322. 云数据库管理平台利用用户注册时获取的两生物融合特征向量进行解密，以获取DBA用户输入的密码，完成登录过程。

图 3