(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 105553980 A
(43)申请公布日 2016.05.04

(21)申请号 201510946531.4

(22)申请日 2015.12.18

(71)申请人 北京理工大学
地址 100081 北京市海淀区中关村南大街5号
申请人 中国人民解放军91655部队

(72)发明人 曹文强 张子剑 王峰 李帅 刘嵩

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

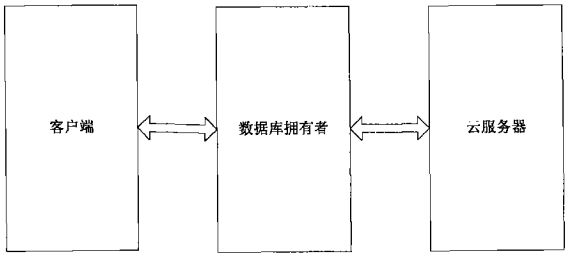
权利要求书2页 说明书6页 附图1页

(54)发明名称

基于云计算的安全指纹识别系统和方法

(57)摘要

本发明公开了一种基于云计算的安全指纹识别系统和方法，该系统包括客户端、数据库拥有者和云服务器三部分，其中，客户端，通过指纹向量提取算法API，将指纹图像提取为固定长度的向量并将其上传至数据库拥有者；数据库拥有者，当从客户端接收样本指纹向量时，将其加密并上传至云服务器进行存储；当接收到待验证指纹向量时，将其进行加密并上传至云服务器；云服务器，当接收到加密后的样本指纹信息时将其进行存储；当接收到加密后的待验证指纹信息时，将该信息中的数据与存储的待验证指纹信息中的数据进行匹配计算，返回索引，数据库拥有者根据该索引找出对应的样本指纹向量，向客户端返回结果。



CN 105553980 A

1.一种基于云计算的安全指纹识别系统，包括客户端、数据库拥有者和云服务器三部分，其中，

客户端，配置有向量提取模块，通过指纹向量提取算法API，将指纹图像提取为固定长度的向量并将其上传至数据库拥有者；

数据库拥有者，配置有指纹向量加密模块，该模块包括样本指纹加密子模块与待验证指纹加密子模块，当从客户端接收到样本指纹向量时，利用样本指纹加密子模块将其加密并上传至云服务器进行存储；当接收到待验证指纹向量时，利用待验证指纹加密子模块将其进行加密并上传至云服务器；

云服务器，配置有信息存储与匹配计算模块，当从数据库拥有者接收到加密后的样本指纹向量信息时将其进行存储；当接收到加密后的待验证指纹向量信息时，将接收到的该待验证指纹向量信息中的数据与存储的待验证指纹向量信息中的数据进行匹配计算，返回索引，数据库拥有者根据该索引找出对应的样本指纹向量，与待验证指纹向量进行欧几里得距离运算，并且与阈值进行比较，向客户端返回结果。

2.根据权利要求1所述的系统，所述客户端首先由提取算法API对指纹图像进行处理得到样本指纹向量b＝[b_1,b_2,,,b_n]，将其第(n+1)位进行扩展为$b_{n+1}=-0.5\sum_{i=1}^{n}b_i^2$，得到向量$b_s$，随机生成(n+1)×(n+1)的矩阵A，令D＝[A_1*b_{s1},A_2*b_{s2},,,$A_{n+1}*b_{s(n+1)}$]，由此样本指纹向量便被隐藏于矩阵D中。

3.根据权利要求1所述的系统，所述数据库拥有者模块利用样本指纹加密子模块将其加密并上传至云服务器进行存储，具体包括：

$$\begin{cases} C_{hi}=C_R\times C_i=H\times M_1^{-1}\times M_1\times D\times M_2=H\times D\times M_2 \\ C_R=M_2^{-1}\times R^T \\ Index \\ Index \end{cases}$$

其中M_1,M_2,H,R为系统的密钥，M_1,M_2为(n+1)×(n+1)的矩阵，H,R为(n+1)的随机向量，Index为样本指纹向量对应的索引，将这些信息(C_{hi},C_R,Index)打包后上传至云服务器进行存储。

4.一种基于云计算的安全指纹识别方法，该方法包括如下步骤：

客户端，通过指纹向量提取算法API，将指纹图像提取为固定长度的向量并将其上传至数据库拥有者；

当从客户端接收到样本指纹向量时，数据库拥有者利用样本指纹加密子模块将其加密并上传至云服务器进行存储；当从客户端接收到待验证指纹向量时，数据库拥有者利用待验证指纹加密子模块将其进行加密并上传至云服务器；

当从数据库拥有者接收到加密后的样本指纹向量信息时，云服务器将其进行存储；当接收到加密后的待验证指纹向量信息时，云服务器将接收到的该待验证指纹向量信息中的数据与存储的待验证指纹向量信息中的数据进行匹配计算，返回索引，数据库拥有者根据该索引找出对应的样本指纹向量，与待验证指纹向量进行欧几里得距离运算，并且与阈值进行比较，向客户端返回结果。

5.根据权利要求4所述的系统，所述客户端首先由提取算法API对指纹图像进行处理得到样本指纹向量b＝[b_1,b_2,,,b_n]，将其第(n+1)位进行扩展为$b_{n+1}=-0.5\sum_{i=1}^{n}b_i^2$，得到向量

b_s，随机生成(n+1)×(n+1)的矩阵A，令D＝[A_1*b_{s1}，A_2*b_{s2}，，，$A_{n+1}*b_{s(n+1)}$]，由此样本指纹向量便被隐藏于矩阵D中。

6.根据权利要求5所述的系统，所述数据库拥有者模块利用样本指纹加密子模块将其加密并上传至云服务器进行存储，具体包括：

$$\begin{cases} C_{hi=}\ C_H \times C_i = H \times M_1^{-1} \times M_1 \times D \times M_2 = H \times D \times M_2 \\ C_R = M_2^{-1} \times R^T \\ Index \\ Index \end{cases}$$

其中M_1，M_2，H，R为系统的密钥，M_1，M_2为(n+1)×(n+1)的矩阵，H，R为(n+1)的随机向量，Index为样本指纹向量对应的索引，将这些信息(C_{hi}，C_R，Index)打包后上传至云服务器进行存储。

基于云计算的安全指纹识别系统和方法

技术领域

[0001] 本发明涉及一种基于云计算的安全指纹识别系统，尤其涉及一种在大规模应用环境中兼顾指纹隐私保护和识别效率的系统。

背景技术

[0002] 随着生物特征识别技术的飞速发展，指纹识别技术已经成为当今社会的主要研究方向之一。但由于目前的指纹识别技术千差万别，这极大地限制了该技术向大规模应用的发展。近年来，随着基于Fingercode指纹特征向量提取算法的日益成熟，人们可以利用该算法将指纹图像提取为固定长度的指纹向量，实现不同设备之间的兼容，为指纹识别技术的大规模应用提供了基础。云平台具有强大的计算与存储能力，考虑到大规模应用中数量庞大的指纹向量，越来越多的企业倾向于将指纹识别中的存储与计算工作外包给云平台。

[0003] 然而，随之而来的安全问题也威胁着指纹信息的安全，使企业在选择指纹识别技术时对使用云计算望而却步。由于云计算将指纹向量存放于不可信的环境中，由不可信云服务商进行指纹向量的计算与验证结果的反馈，对指纹的安全性和机密性带来了严重的威胁。如果能够采用安全高效的加密技术在指纹向量上传到云服务器之前对其进行加密，可以很好地保障指纹向量的安全性和机密性，不论是窃听敌手还是不可信的云计算提供商均不能窃取指纹向量信息。在云计算环境下，如何在保证指纹隐私保护的同时提高指纹识别的效率，这已经成为指纹识别走向大规模应用的瓶颈之一。

[0004] 由于不能妥善解决云计算下指纹的隐私保护与效率问题，目前已有的指纹识别系统，均未使用云计算来对指纹向量进行有效的存储和计算。

发明内容

[0005] 本发明的目的是针对现有指纹识别系统在使用云计算时存在的缺陷，提出一种基于云计算的安全指纹识别系统。通过使用安全高效的加密方案和有效的指纹识别方案，在保障指纹向量安全的同时解决了密文环境下指纹的验证识别，使云计算能够服务于指纹识别系统。该系统可以为企事业单位提供保障指纹隐私与效率的指纹识别技术。

[0006] 本发明的目的是通过下述技术方案实现的。

[0007] 基于云计算的安全指纹识别系统，包括客户端、数据库拥有者和云服务器三部分。其中客户端是可扩展的第三方，用以提取指纹向量，可安装在多台主机上；数据库拥有者是可信的本地模块，负责与客户端和云服务器的通信，可以完成指纹向量的加密与上传；云服务器是不可信的第三方，负责存储加密后的样本指纹信息，针对待验证的指纹信息完成指纹的识别验证功能。

[0008] 客户端，配置有向量提取模块，通过指纹向量提取算法API，将指纹图像提取为固定长度的向量并将其上传至数据库拥有者；

[0009] 数据库拥有者，配置有指纹向量加密模块，该模块包括样本指纹加密子模块与待验证指纹加密子模块，当从客户端接收到样本指纹向量时，利用样本指纹加密子模块将其

加密并上传至云服务器进行存储;当接收到待验证指纹向量时,利用待验证指纹加密子模块将其进行加密并上传至云服务器;云服务器,配置有信息存储与匹配计算模块,当从数据库拥有者接收到加密后的样本指纹向量信息时将其进行存储;当接收到加密后的待验证指纹向量信息时,将接收到的该待验证指纹向量信息中的数据与存储的待验证指纹向量信息中的数据进行匹配计算,返回索引,数据库拥有者根据该索引找出对应的样本指纹向量,与待验证指纹向量进行欧几里得距离运算,并且与阈值进行比较,向客户端返回结果。

[0010] 所述指纹向量加密模块使用由Jiawei Yuan等人于2013年提出的云计算下的生物识别信息隐私保护方案(Efficient Privacy-Preserving Biometric Identification in Cloud Computing)对指纹向量的加密方案包含样本指纹向量的加密方案与待验证指纹向量的加密方案。

[0011] 当进行指纹注册时,首先由提取算法对指纹图像进行处理得到样本指纹向量b=[b_1,b_2,,,b_n],将其第(n+1)位进行扩展为$b_{n+1}=-0.5\sum_{i=1}^{n}b_i^2$,得到向量$b_s$。随机生成(n+1)×(n+1)的矩阵A,令D=[A_1*b_{s1},A_2*b_{s2},,,$A_{n+1}*b_{s(n+1)}$],由此样本指纹向量便被隐藏于矩阵D中。数据库拥有者模块对其样本指纹信息进行以下操作:

[0012] $$\begin{cases} C_{hi}=C_H\times C_i=H\times M_1^{-1}\times M_1\times D\times M_2=H\times D\times M_2 \\ C_R=M_2^{-1}\times R^T \\ Index \\ Index \end{cases}$$

[0013] 其中M_1,M_2,H,R为系统的密钥。M_1,M_2为(n+1)×(n+1)的矩阵,H,R为(n+1)维的随机向量,Index为样本指纹向量对应的索引。将这些信息(C_{hi},C_R,Index)打包后上传至云服务器进行存储。

[0014] 当进行指纹验证时,首先由提取算法对指纹图像进行处理得到待验证指纹向量b=[b_1,b_2,,,b_n],将其第(n+1)位进行扩展为$b_{n+1}=1$,得到向量b_c。随机生成(n+1)×(n+1)的矩阵E,令F_e=[E_1*b_{c1},E_2*b_{c2},...,$E_{n+1}*b_{c(n+1)}$],由此待验证指纹向量被隐藏在矩阵F_c中。在数据库拥有者模块对加密后的待验证指纹信息进行如下操作:

[0015] $$C_F=M_1^{-1}\times k\times F_c\times M_2$$

[0016] 其中M_1,M_2为系统的密钥,k为每次验证时所生成的随机常数。当验证时,将C_F上传至云服务器,与存储的样本指纹信息进行匹配计算。

[0017] 当进行指纹的验证识别时,定义相对距离:

[0018] $P_{se}=C_{hi}\times C_F\times C_R$

[0019] 对于云服务器存储的每一个样本指纹信息,由此公式都可以得到一个相对距离,计算任意两个相对距离之差:

[0020] $P_{ic}-P_{zc}=0.5k(dist_{zc}-dist_{ic})$

[0021] 可知相对距离之差即为0.5倍的欧几里得距离之差的相反值。因此可知相对距离最大的样本指纹向量即为欧几里得距离最小的样本指纹向量。

[0022] 所述数据库拥有者方加密模块负责将所有的指纹向量按照注册与验证进行不同的加密并上传至云服务器。

[0023] 所述云服务器的解密模块负责将加密后的待验证指纹信息与云服务器存储的加密后的样本指纹信息进行匹配计算,找出最接近待验证指纹的样本指纹的索引。

[0024] 上述组成部分的连接关系为:

[0025] 客户端对指纹图像提取指纹向量，上传至数据库拥有者进行指纹向量的加密，加密完成后将加密后的信息上传至云服务器，云服务器根据不同的需求完成数据的存储或者匹配计算，并将索引反馈给数据库拥有者。数据库拥有者按照索引找出对应的样本指纹向量，与待验证指纹向量计算欧几里得距离并与阈值相比较，最终将结果反馈给客户端。

[0026] 有益效果

[0027] 与普通的指纹识别系统相比，本发明使用云计算技术对指纹注册和识别过程进行方便有效的存储和管理，通过使用安全高效的加密方案，保障了指纹信息的安全性和机密性，同时使用云计算提高了验证识别的效率，为企业提供了安全高效的指纹识别系统。

附图说明

[0028] 图1是系统架构图；

[0029] 图2是系统的具体组成框图。

具体实施方式

[0030] 下面结合附图，对本发明的具体实施方式做进一步详实说明。

[0031] 基于云计算的安全指纹加密系统，包括客户端、数据库拥有者和云服务器。其中，客户端作为可扩展的第三方，对指纹图像提取指纹向量的功能并将其上传，可以安装在多台主机上，增加系统的可扩展性。

[0032] 数据库拥有者模块为可信的本地模块，配置有指纹向量的加密模块，完成指纹向量的加密功能，实现与客户端和云服务器的通信。

[0033] 云服务器配置有解密模块，与客户端拥有者进行通信，实现加密样本指纹的存储与加密待验证指纹的识别验证功能。

[0034] 本系统的工作过程如下：

[0035] 首先是指纹的注册过程。

[0036] 用户通过安装在本地的数据库拥有者进行指纹的注册。具体的，输入指纹图像后，数据库拥有者先从指纹图片中提取出固定长度的指纹向量，将该样本指纹向量存储在该模块，并且通过样本指纹加密算法对该向量进行加密。加密完成后将信息(C_{hi},C_R,Index)打包上传至云服务器，同时用户可以录入自己的基本信息。

[0037] 云服务器在接收到数据库拥有者上传的打包信息后将其进行存储，并将对应的操作状态返回给数据库拥有者。

[0038] 通过以上操作将多个加密后的指纹信息上传至云服务器，实现指纹的注册。

[0039] 然后是指纹的验证过程。

[0040] 用户可以通过安装在多台主机上的客户端进行指纹的验证。具体的，输入指纹图像后，客户端通过向量提取算法API提取出固定长度的指纹向量，并将信息上传至数据库拥有者。数据库拥有者接收后，调用待验证指纹向量加密算法对其进行加密得到C_F并上传至云服务器。云服务器接收到该信息后，调用解密模块，分别与存储的样本指纹信息进行匹配计算，向数据库拥有者返回索引。

[0041] 所述解密过程包括以下步骤：

[0042] 假设云服务器已经存储了n个加密后的样本指纹信息，现在要选取一个指纹图像

进行验证。客户端利用向量提取算法可提取待验证指纹向量为$b=[b_1,b_2,,,b_n]$，调用待验证指纹信息的加密算法可以得到C_F，将其上传至云服务器进行匹配计算。具体的匹配过程如下：

[0043] 首先将待验证指纹信息C_F与云服务器存储的每一个样本指纹信息(C_{hs},C_R,Index)都计算其相对距离，计算公式如下：

$$P_{Fi}=C_{hi}\times C_F\times C_R$$

$$=H\times D_i\times M_1$$

[0044] $$\times M_1^{-1}\times k\times F_c\times M_2\times M_2^{-1}\times R^T$$

$$=H\times D_i\times k\times F_c\times R^T$$

$$=k\sum_{j=1}^{n+1}b_{zj}*b_{cj}$$

[0045] 假设在云服务器存有m个指纹样本，指纹b_c为待验证指纹。则b_c会与样本库中的指纹信息生成m个相对距离为P_{ic}，其中($1\le i\le m$)

[0046] 则在匹配计算时，假设样本指纹库有b_i和b_z，其中($1\le i,z\le m$，且$i\neq z$)，则与b_c相对距离分别为P_{ic}和P_{zc}，计算其差可知：

$$P_{ic}-P_{zc}$$

[0047]

$$=k\left(\sum_{j=1}^{n}b_{ij}*b_{cj}-0.5\left(\sum_{j=1}^{n}b_{ij}^2\right)\right)$$

$$-k\left(\sum_{j=1}^{n}b_{zj}*b_{cj}-0.5\left(\sum_{j=1}^{n}b_{zj}^2\right)\right)$$

[0048]

$$=0.5k(dist_{zc}-dist_{ic})$$

[0049] 由上式可知，通过相对距离之差，可以将其转化为0.5k倍的真实距离之差的相反值。如果$P_{iG}-P_{zc}>0$，则意为着$dist_{zc}-dist_{ic}>0$，即P_i与P_F相比，P_i与待验证指纹更加接近。因此在匹配时，只需找到相对距离最大的$P_{i_{max}}$，其中($1\le i\le m$)，即可得到最接近待验证指纹的样本指纹向量为b_i。因为云服务器存储的是b_i对应的指纹信息(C_i,C_H,C_R,Index)，通过匹配计算可以得到最接近指纹b_i的索引Index。

[0050] 数据库拥有者根据索引找到对应的样本指纹向量与待验证的指纹向量计算欧几里得距离，并且与事先设定的阈值进行比较，最终将结果反馈给客户端。

[0051] 如果欧几里得距离小于或等于阈值，就将用户的信息显示出来，如果大于阈值，则提示验证失败。

[0052] 至此，一次完整的指纹识别过程完成。

[0053] 下面对本发明所采用的指纹识别加解密安全算法的正确性进行证明描述。为了验证本系统的安全性，假定存在威胁模型为攻击者是否与云服务器合谋。

[0054] 首先假定攻击者不与云服务器合谋：

[0055] 当攻击者不与云服务器合谋时，此时攻击者攻击数据库拥有者，可以获得(C_{hi},C_R)，如果攻击者可以通过已知量得到密钥M_1,M_2,H,R，则该算法被视为不安全的。通过上文中已述已知量的相关等式，可知：

[0056] $$\begin{cases} C_{hi} = H \times D_i \times M_1 \\ C_R = M_2^{-1} \times R^T \\ Index \end{cases}$$

[0057] $$\begin{cases} U = M_1 \times M_1^{-1} \\ U = M_2 \times M_2^{-1} \end{cases}$$

[0058] 下面分析是否可以通过已知量求出密钥。

[0059] 如果要尝试解出密钥M_1,则将文中出现的关于M_1等式列出。

[0060] $$\begin{cases} C_{hi} = H \times D_i \times M_1 \\ U = M_1 \times M_1^{-1} \end{cases}$$

[0061] 由前提的攻击条件,已知C_{hi}(为(n+1)×(n+1)矩阵)、U(为(n+1)×(n+1)单位矩阵),已知量为2(n+1)×(n+1)。

[0062] 未知D_i(为(n+1)×(n+1)矩阵)、M_1^{-1}(为(n+1)×(n+1)矩阵),未知量为2(n+1)×(n+1)+(n+1)。

[0063] 由已知量<未知量,根据数学常识,可知通过上述公式解出M_1是不可能的,因此密钥M_1是安全的。

[0064] 同理,对于M_2可以列出等式:

[0065] $$\begin{cases} C_R = M_2^{-1} \times R^T \\ U = M_2 \times M_2^{-1} \end{cases}$$

[0066] 都可以通过与上述类似的分析得到已知量<未知量,因此M_2均无法求出。

[0067] 对于密钥H,可以列出等式$C_{hi}=H\times D_i\times M_i$,已知$C_{hi}$(为(n+1)向量),已知量为(n+1)。

[0068] 未知D_i,M_1(为(n+1)×(n+1)矩阵),未知量为2(n+1)×(n+1)。

[0069] 已知量<未知量,可证解不出H。

[0070] 同理,对于密钥R,有等式$C_R = M_2^{-1} \times R^T$,根据对密钥H的分析,同样解不出R。

[0071] 由上分析,当攻击者不与云服务器合谋时,仅根据数据库拥有者中的数据是不可能解出本算法中的密钥。

[0072] 其次是假设攻击者与云服务器合谋:

[0073] 此时攻击者已知样本指纹库中(C_{hi},C_R,Index)和待验证指纹C_p,假设一种更加极端的情况,攻击者可以作为一个合法的客户端,那么攻击者可以构造i个待验证指纹C_{Fi},对于每一次的验证指纹C_{Fi},都会引入一个新的未知量k_i。不妨假设合谋t次(t≥n+2),利用矩阵与方程组的关系可得:

[0074] $$P = M_2^{-1} \times [k_1 \times b_{c1}^T, \ldots, k_t \times b_{ct}^T] = M_2^{-1} \times [b_{c1}^T, \ldots, b_{ct}^T] \times \begin{bmatrix} k_1 & 0 & \cdots & 0 \\ 0 & k_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & k_t \end{bmatrix}$$

$$= M_2^{-1} \times BC \times K$$

[0075] 其中,$P_i=C_{Fi}\times C_R$,P_i为P的第i个列向量,1≤i≤t。在本方案中,P、$[b_{c1}^T, \ldots, b_{ct}^T]$已知,若要解出$M_2^{-1}$,我们需要知道$K^{-1}$,但K的非零元是随机产生的,所以枚举R在多项式时间内是无法完成的。因此攻击者无法解出M_2^{-1},不能恢复出任何私密指纹特征数据。

[0076] 由上述实施实例可见,在整个指纹识别过程中,涉及指纹隐私的指纹向量在云服

务器以及传输过程中均不曾以明文形式出现，从而保障了指纹的安全性和机密性。并提供了安全有效的指纹验证识别功能，从而，将云计算技术安全地应用在了指纹识别系统中。

[0077] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进，或者对其中部分技术特征进行等同替换，这些改进和替换也应视为本发明的保护范围。

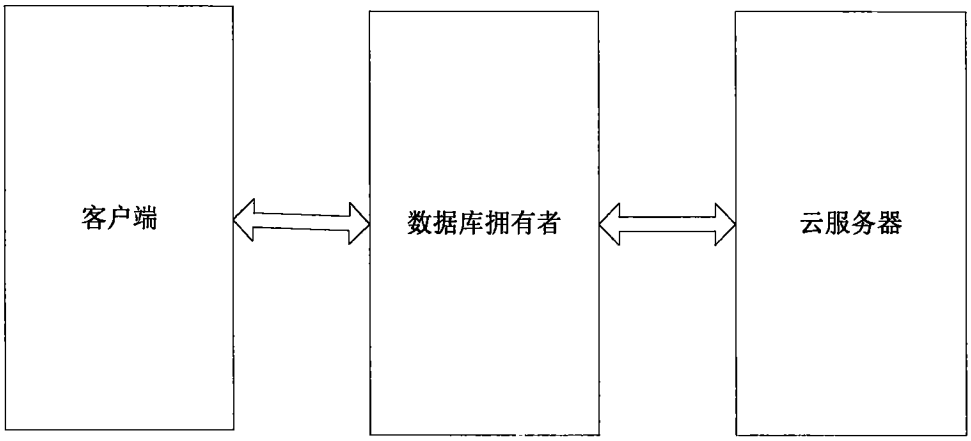

客户端
数据库拥有者
云服务器

图1

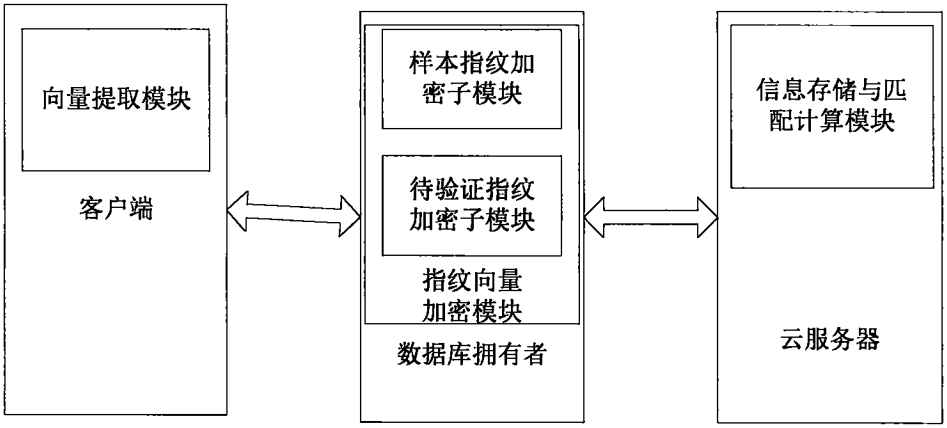

向量提取模块
客户端
样本指纹加密子模块
待验证指纹加密子模块
指纹向量加密模块
数据库拥有者
信息存储与匹配计算模块
云服务器

图2