(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 102769531 A
(43)申请公布日 2012.11.07

(21)申请号 201210285035.5

(22)申请日 2012.08.13

(71)申请人 鹤山世达光电科技有限公司
地址 529000 广东省江门市鹤山市共和镇新材料基地（鹤山市世逸电子科技有限公司H座）

(72)发明人 王国芳 程佩仪

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
G06K 9/00(2006.01)

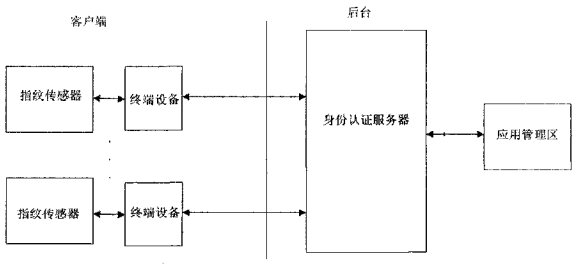
权利要求书 2 页 说明书 4 页 附图 1 页

(54)发明名称

身份认证装置及其方法

(57)摘要

一种身份认证装置，它包括客户端以及后台，客户端包括多个终端设备以及分别与每个终端设备相交互连接的指纹传感器，指纹传感器包括用于采集指纹信息的采集识别装置以及用于存储包括指纹信息以及该指纹信息相对应用户的用户信息的存储器，后台包括与终端设备相交互连接的身份认证服务器以及与身份认证服务器相交互连接的多个应用服务器，终端设备用于登记或确认指纹传感器接收到的指纹信息以辨别用户的身份，并将登记或确认的结果传递至后台的身份认证服务器，身份认证服务器根据该结果以决定用户在多个应用服务器上具有的权限。



CN 102769531 A

1. 一种身份认证装置，其特征在于，它包括客户端以及后台，所述客户端包括多个终端设备以及分别与每个终端设备相交互连接的指纹传感器，所述指纹传感器包括用于采集指纹信息的采集识别装置以及用于存储包括指纹信息以及该指纹信息相对应用户的用户信息的存储器，所述后台包括与终端设备相交互连接的身份认证服务器以及与所述身份认证服务器相交互连接的多个应用服务器，所述终端设备用于登记或确认指纹传感器接收到的指纹信息以辨别用户的身份，并将登记或确认的结果传递至所述后台的身份认证服务器，所述身份认证服务器根据该结果以决定用户在多个应用服务器上具有的权限。

2. 根据权利要求 1 所述的身份认证装置，其特征在于：所述身份认证服务器包括用于辨别用户身份的用户认证单元以及用于存放注册后的用户信息的用户档案管理单元。

3. 根据权利要求 2 所述的身份认证装置，其特征在于：每个终端设备上设置有 OTP 口令，所述用户档案管理单元中设置有 OTP 种子，所述终端设备在指纹信息确认匹配后，将 OTP 口令发送至所述身份认证服务器，所述用户认证单元对通过所述用户档案管理单元中的 OTP 种子对 OTP 口令进行匹配。

4. 根据权利要求 2 所述的身份认证装置，其特征在于：每个指纹传感器具有唯一的传感器 ID，所述用户档案管理单元中设置有传感器 ID 档案，在所述终端设备在指纹信息确认匹配后，所述终端设备将指纹传感器的传感器 ID 传送至所述身份认证服务器，所述身份认证服务器的用户认证单元通过所述用户档案管理单元的传感器 ID 档案对指纹传感器的传感器 ID 进行匹配。

5. 根据权利要求 1 所述的身份认证装置，其特征在于：所述终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

6. 一种身份认证的方法，其特征在于，它包括以下步骤：

A) 注册阶段：

A1) 通过指纹传感器的采集识别装置提取用户的指纹，并生成一对相对应的公匙和私匙；

A2) 将私匙存储在指纹传感器的存储器内；

A3) 将公匙通过主机传送至身份认证服务器，并将公匙存储在身份认证服务器的同时生成一新的注册用户；

B) 认证阶段：

B1) 通过指纹传感器的采集识别装置提取用户的指纹信息，终端设备通过存储器进行比对，如果相匹配则进入下一步，如果不相匹配则拒绝进入下一步；

B2) 终端设备从存储器中取出私匙，并将私匙传递至身份认证服务器；

B3) 身份认证服务器通过公匙对私匙进行匹配以认证用户。

7. 根据权利要求 6 所述的身份认证方法，其特征在于：在步骤 B1) 和步骤 B2) 之间包括一步骤 B4)，终端设备上设置有 OTP 口令，身份认证服务器中设置有 OTP 种子，终端设备在确认指纹信息匹配后，将 OTP 口令传递至身份认证服务器，身份认证服务器对 OTP 口令进行匹配。

8. 根据权利要求 6 所述的身份认证方法，其特征在于：在步骤 B1) 和步骤 B2) 之间包括一步骤 B5)，每个指纹传感器具有唯一的传感器 ID，身份认证服务器中设置有传感器 ID 档案，在终端设备确认指纹信息匹配后，终端设备将指纹传感器的传感器 ID 传送至身份认证

服务器，身份认证服务器对指纹传感器的传感器 ID 通过传感器 ID 档案进行匹配。

9. 根据权利要求 6 所述的身份认证方法，其特征在于：在步骤 B3) 之后包括一步骤 B6)，当用户认证成功后，可在多个应用服务器上进行数据的加密或解密。

10. 根据权利要求 6 所述的身份认证方法，其特征在于：所述终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

身份认证装置及其方法

技术领域

[0001] 本发明涉及一种身份认证装置和身份认证方法。

背景技术

[0002] 目前的社会网络平台可以存储用户名、密码、图片、地址、身份证号码、邮件等用户信息，然而这些信息却不能反映用户的真实身份。

[0003] 网络用户可以创建不限数量的网络账户，很多用户常常会因为忘记用户名或者密码而重复创建多个不同的账户，从而造成资源的浪费。

[0004] 同时，这不仅仅会引发资源浪费，还可能会对公共安全造成损害。例如，一些网络使用者可能会利用不同的身份信息创建多个虚假账号以提供色情服务或者骗取财物。

发明内容

[0005] 本发明的目的是提供一种身份认证装置及其方法，将指纹生物信息进行归档。由于人的指纹都是唯一的，所以一个人只能在平台上创建一个具有真实身份信息的唯一账号，从而避免和排除安全以及资源浪费问题。

[0006] 本发明所采用的技术方案是：一种身份认证装置，它包括客户端以及后台，所述客户端包括多个终端设备以及分别与每个终端设备相交互连接的指纹传感器，所述指纹传感器包括用于采集指纹信息的采集识别装置以及用于存储包括指纹信息以及该指纹信息相对应用户的用户信息的存储器，所述后台包括与终端设备相交互连接的身份认证服务器以及与所述身份认证服务器相交互连接的多个应用服务器，所述终端设备用于登记或确认指纹传感器接收到的指纹信息以辨别用户的身份，并将登记或确认的结果传递至所述后台的身份认证服务器，所述身份认证服务器根据该结果以决定用户在多个应用服务器上具有的权限。

[0007] 优选地，所述身份认证服务器包括用于辨别用户身份的用户认证单元以及用于存放注册后的用户信息的用户档案管理单元。

[0008] 优选地，每个终端设备上设置有 OTP 口令，所述用户档案管理单元中设置有 OTP 种子，所述终端设备在指纹信息确认匹配后，将 OTP 口令发送至所述身份认证服务器，所述用户认证单元对通过所述用户档案管理单元中的 OTP 种子对 OTP 口令进行匹配。

[0009] 优选地，每个指纹传感器具有唯一的传感器 ID，所述用户档案管理单元中设置有传感器 ID 档案，在所述终端设备在指纹信息确认匹配后，所述终端设备将指纹传感器的传感器 ID 传送至所述身份认证服务器，所述身份认证服务器的用户认证单元通过所述用户档案管理单元的传感器 ID 档案对指纹传感器的传感器 ID 进行匹配。

[0010] 优选地，所述终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

[0011] 一种身份认证的方法，它包括以下步骤：

[0012] A) 注册阶段：

[0013] A1) 通过指纹传感器的采集识别装置提取用户的指纹，并生成一对相对应的公匙和私匙；

[0014] A2) 将私匙存储在指纹传感器的存储器内；

[0015] A3) 将公匙通过主机传送至身份认证服务器，并将公匙存储在身份认证服务器的同时生成一新的注册用户；

[0016] B) 认证阶段：

[0017] B1) 通过指纹传感器的采集识别装置提取用户的指纹信息，终端设备通过存储器进行比对，如果相匹配则进入下一步，如果不相匹配则拒绝进入下一步；

[0018] B2) 终端设备从存储器中取出私匙，并将私匙传递至身份认证服务器；

[0019] B3) 身份认证服务器通过公匙对私匙进行匹配以认证用户。

[0020] 优选地，在步骤 B1) 和步骤 B2) 之间包括一步骤 B4)，终端设备上设置有 OTP 口令，身份认证服务器中设置有 OTP 种子，终端设备在确认指纹信息匹配后，将 OTP 口令传递至身份认证服务器，身份认证服务器对 OTP 口令进行匹配。

[0021] 优选地，在步骤 B1) 和步骤 B2) 之间包括一步骤 B5)，每个指纹传感器具有唯一的传感器 ID，身份认证服务器中设置有传感器 ID 档案，在终端设备确认指纹信息匹配后，终端设备将指纹传感器的传感器 ID 传送至身份认证服务器，身份认证服务器对指纹传感器的传感器 ID 通过传感器 ID 档案进行匹配。

[0022] 优选地，在步骤 B3) 之后包括一步骤 B6)，当用户认证成功后，可在多个应用服务器上进行数据的加密或解密。

[0023] 优选地，所述终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

[0024] 本发明采用以上结构或方法具有以下有益效果：

[0025] 1、在这个身份认证装置上，用户的身份是唯一且真实的，必要的时候，用户的身份是可追踪的，服务器的用户档案的是不可复制的。

[0026] 2、指纹信息储存在当地指纹设备上，且仅为用户自己拥有，因而具有高私密性。

[0027] 3、不再单独的使用密码或者指纹进行用户的身份认证，而是采用多因素认证，例如指纹，传感器 ID，一次性密码口令 (OTP) 均须匹配成功才能通过身份认证。

[0028] 4、另外这个平台里所有数据都是通过密钥进行保护的，确保了数据的安全。因此在这样的平台上，不仅解决了网络资源的浪费问题，网络的安全性也得到了极大的保证。

[0029] 说明书附图

[0030] 附图 1 为本发明中的身份认证装置的结构示意图。

具体实施方式

[0031] 下面结合附图对本发明的较佳实施例进行详细阐述，以使本发明的优点和特征能更易于被本领域技术人员理解，从而对本发明的保护范围做出更为清楚明确的界定。

[0032] 一种身份认证的方法，它包括以下步骤：

[0033] A) 注册阶段：

[0034] 通过指纹传感器的采集识别装置提取用户的指纹，并生成一对相对应的公匙和私匙；

[0035] 将私匙存储在指纹传感器的存储器内；

[0036] 将公匙通过主机传送至身份认证服务器，并将公匙存储在身份认证服务器的同时生成一新的注册用户；

[0037] 发送一个由私匙加密的确认信息；

[0038] 利用公匙鉴定发送者的信息。

[0039] B) 认证阶段：

[0040] 通过指纹传感器的采集识别装置提取用户的指纹信息，终端设备通过存储器进行比对，如果相匹配则进入下一步，如果不相匹配则拒绝进入下一步；

[0041] 终端设备上设置有 OTP 口令，身份认证服务器中设置有 OTP 种子，终端设备在确认指纹信息匹配后，将 OTP 口令传递至身份认证服务器，身份认证服务器对 OTP 口令进行匹配。

[0042] 每个指纹传感器具有唯一的传感器 ID，身份认证服务器中设置有传感器 ID 档案，在终端设备确认指纹信息匹配后，终端设备将指纹传感器的传感器 ID 传送至身份认证服务器，身份认证服务器对指纹传感器的传感器 ID 通过传感器 ID 档案进行匹配。

[0043] 终端设备从存储器中取出私匙，并将私匙传递至身份认证服务器；

[0044] 身份认证服务器通过公匙对私匙进行匹配以认证用户。

[0045] 当用户认证成功后，可在多个应用服务器上进行数据的加密或解密。

[0046] 如附图 1 所示，一种身份认证装置，它包括客户端以及后台。

[0047] 客户端包括多个终端设备以及分别与每个终端设备相交互连接的指纹传感器，指纹传感器包括用于采集指纹信息的采集识别装置以及用于存储包括指纹信息以及该指纹信息相对应用户的用户信息的存储器。

[0048] 后台包括与终端设备相交互连接的身份认证服务器以及与所述身份认证服务器相交互连接的多个应用服务器。

[0049] 终端设备用于登记或确认指纹传感器接收到的指纹信息以辨别用户的身份，并将登记或确认的结果传递至所述后台的身份认证服务器，所述身份认证服务器根据该结果以决定用户在多个应用服务器上具有的权限

[0050] 身份认证服务器包括用于辨别用户身份的用户认证单元以及用于存放注册后的用户信息的用户档案管理单元。

[0051] 每个终端设备上设置有 OTP 口令，所述用户档案管理单元中设置有 OTP 种子，所述终端设备在指纹信息确认匹配后，将 OTP 口令发送至所述身份认证服务器，所述用户认证单元对通过所述用户档案管理单元中的 OTP 种子对 OTP 口令进行匹配。

[0052] 每个指纹传感器具有唯一的传感器 ID，所述用户档案管理单元中设置有传感器 ID 档案，在所述终端设备在指纹信息确认匹配后，所述终端设备将指纹传感器的传感器 ID 传送至所述身份认证服务器，所述身份认证服务器的用户认证单元通过所述用户档案管理单元的传感器 ID 档案对指纹传感器的传感器 ID 进行匹配。

[0053] 终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

[0054] 指纹传感器包含存储器和采集识别装置两部分。在用户注册和认证时，该设备提取用户生物指纹数据，连同私钥以及用户的其他信息储存在存储器上。私钥以及其对应的

公钥，是根据用户注册的指纹信息所生成的加密和解密的算法。私钥存储在指纹传感器的存储器上，而公钥则被上传到身份认证服务器上。一旦用户身份被服务认证通过，密钥匹配成功则可在不用的应用中进行数据加密和解密。

[0055] 终端设备可以是电脑、平板电脑或者手机等。在身份注册和认证中，终端设备负责指纹的登记与确认。同时，一次性口令 (OTP) 也存储于终端设备中，在指纹确认之后用于身份认证。一次性口令 (OTP) 在不同的情形生成不同的密码。这样的话，指纹传感设备的 ID、一次性口令以及其他被私钥加密的信息一并发送至到身份认证服务器确认。一旦用户被认证，在服务器的不同应用就可以使用而且数据受加密保护。

[0056] 身份认证服务器包括用户认证单元和用户档案管理单元。

[0057] 用户认证单元通过匹配主机中的一次性口令、传感器 ID、以及解密其他加密信息完成用户的认证。以上信息一旦匹配成功，可以鉴定用户的身份是真实的，而且允许用户使用平台的应用。

[0058] 用户档案管理单元管理注册用户的档案。所有档案由系统储存及管理。这些档案包括 OTP 种子、传感器 ID，指纹数据信息（如注册者的指纹号码）、公钥、用户群以及用户特权等等。这些档案用于进行认证以及不同应用的服务器间的沟通。

[0059] 为了使该身份认证装置具有不同的功能，需要许多不同的应用服务器。这些应用服务器可以是邮件、聊天、文件共享等等。身份认证服务器认证用户的真实身份，身份认证装置上的所有用户都是实际注册的那个人。从而注册用户与其他用户安全的交谈。邮件的发件人是被认可的。只有注册用户可以读取他们自己的邮件。此外，身份认证装置的注册用户可以根据身份认证服务器档案里的群组信息与不同的用户组成不同的群。同一群里的人可以共享他们的秘密文件，音乐文件或者视频文件，只有被认证的实际注册的用户才能访问这些文件。因此在这个身份认证装置中，所有的注册用户的身份都是被认可的。

[0060] 在这个身份认证装置上，用户的身份是唯一且真实的，必要的时候，用户的身份是可追踪的，服务器的用户档案的是不可复制的。指纹信息储存在当地指纹设备上，且仅为用户自己拥有，因而具有高私密性。不再单独的使用密码或者指纹进行用户的身份认证，而是采用多因素认证，例如指纹，传感器 ID，一次性密码口令 (OTP) 均须匹配成功才能通过身份认证。另外这个平台里所有数据都是通过密钥进行保护的，确保了数据的安全。因此在这样的平台上，不仅解决了网络资源的浪费问题，网络的安全性也得到了极大的保证。

[0061] 以上对本发明的特定实施例结合图示进行了说明，很明显，在不离开本发明的范围和精神的基础上，可以对现有技术和工艺进行很多修改。在本发明的所属技术领域中，只要掌握通常知识，就可以在本发明的技术要旨范围内，进行多种多样的变更。

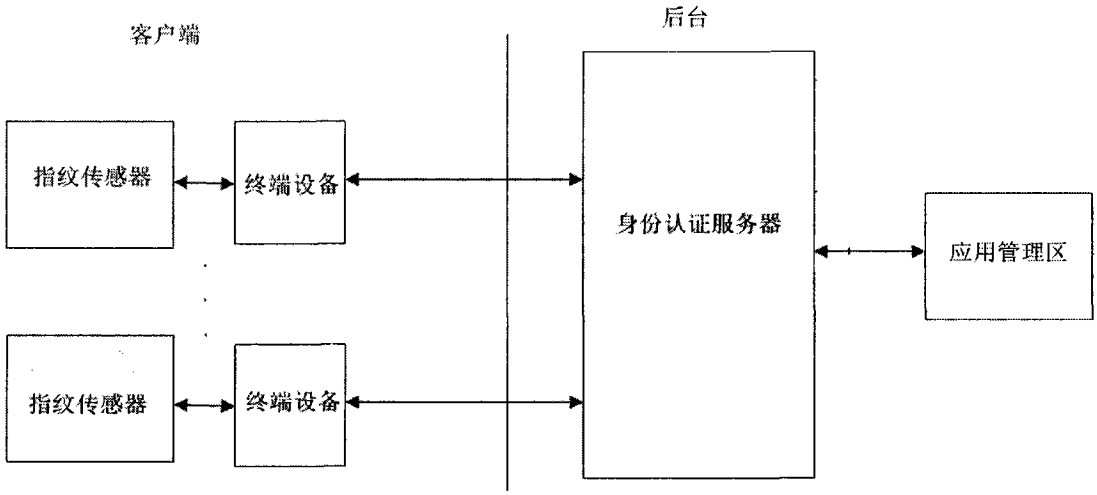


图 1