

## 一种可信终端验证方法、装置

### 技术领域

本申请涉及终端技术领域，尤其涉及一种可信终端验证方法和装置。

### 背景技术

5       对于像类似于支付宝这样的安全性要求较高的支付应用中，当用户需要进行重置密码，修改用户预留的联系手机，修改登录名等敏感操作时，由于敏感操作涉及的修改信息多为用户私密信息，因此用户在进行敏感操作时，用户身份认证过程将会更加严格。

10       例如，当用户在进行敏感操作时，可以由用户上传证件信息，并在页面上回答生成的预留问题，然后再由客服人员对用户上传的证件信息进行人工审核后做电话回访，只有上述认证都通过后才会允许用户进行上述的敏感操作。

15       然而在上述方案中，如果所有用户进行敏感操作时都需要执行上述严格的身份认证过程，那么对用户上传的证件进行审核以及电话回访都需要较大的人力成本。而且，如果用户每进行一次敏感操作都需要重新进行一次较为严格的身份认证的话，会影响用户体验。

为了解决上述问题，可以对用户所使用的登录终端进行认证，认证通过的登录终端对于该用户来说是可信终端，当用户使用可信终端登录并进行敏感操作时，可以不对该用户进行重复认证或者只进行较简单的认证。

20       当前对用户的登录终端进行认证，多是通过用户的交易信息、IP地址、登录时间段进行认证，然而对一些特殊的应用场景，比如用户之间交叉使用登录终端的应用场景中，上述方法已不能满足用户需求。

## 发明内容

为克服背景技术中存在的问题，本申请提供一种在可信终端验证方法和装置。

根据本申请实施例的第一方面，本申请提出一种可信终端验证方法，所述方法包括：

判断用户的登录终端是否匹配本地记录的该用户的可信终端；

当判断出所述登录终端不匹配本地记录的该用户的可信终端时，判断所述用户的登录账号与所述登录终端的常用登录账号是否相关联；

如果是，判定所述登录终端在本地记录为该用户的可信终端。

10 可选的，所述判断用户的登录终端是否匹配本地记录的该用户的可信终端之前，所述方法还包括：

根据所述可信终端的硬件信息识别所述可信终端的终端类型；

当识别出所述可信终端为手持终端时，将所述可信终端在本地归类为手持可信终端；

15 当识别出所述可信终端为 PC 终端时，判断所述可信终端的常用时间段是否为办公时间段或家用时间段；

当所述可信终端的常用时间段为办公时间段时，将所述可信终端在本地归类为办公可信终端；

20 当所述可信终端的常用时间段为家用时间段时，将所述可信终端在本地归类为家用可信终端。

可选的，所述判断用户的登录账号是否与所述登录终端的常用登录账号相关联之前，所述方法还包括：

判断所述用户的登录账号在所述登录终端上的登入次数是否达到阈值；

25 如果是，继续判断所述用户的登录账号是否与所述登录终端的常用登录账号相关联；

如果否，判定所述登录终端为该用户的非可信终端。

可选的，所述判断用户的登录账号与所述登录终端的常用登录账号是否相关联包括：

查询所述登录终端的常用登录账号；其中所述常用登录账号为所述登录终端的历史登录账号中登入次数达到阈值的登录账号；

- 5       判断所述用户的登录账号与所述常用登录账号是否曾在同一可信终端上登录，并且登录次数均达到阈值；

如果是，确定所述用户的登录账号与所述常用登录账号相关联，并在本地保存所述用户的登录账号与所述历史登录账号之间的关联关系。

可选的，所述同一可信终端为同一家用可信终端。

- 10       根据本申请实施例的第二方面，本申请提出一种可信终端验证装置，所述装置包括：

第一判断模块，用于判断用户的登录终端是否匹配本地记录的可信终端；

- 第二判断模块，用于在判断出所述登录终端不匹配本地记录的可信终端时，判断用户的登录账号与所述登录终端的常用登录账号是否相关联；如果  
15       是，判定所述登录终端为该用户的可信终端。

可选的，所述装置还包括：

归类模块，用于在第一判断模块判断用户的登录终端是否匹配本地记录的该用户的可信终端之前，根据所述可信终端的硬件信息识别所述可信终端的终端类型；

- 20       当识别出所述可信终端为手持终端时，将所述可信终端在本地归类为手持可信终端；

当识别出所述可信终端为 PC 终端时，判断所述可信终端的常用时间段是否为办公时间段或家用时间段；

- 当所述可信终端的常用时间段为办公时间段时，将所述可信终端在本地  
25       归类为办公可信终端；

当所述可信终端的常用时间段为家用时间段时，将所述可信终端在本地归类为家用可信终端。

可选的，所述第二判断模块具体用于：

在判断用户的登录账号与所述登录终端的常用登录账号是否相关联之前，判断所述用户的登录账号在所述登录终端上的登入次数是否达到阈值；

如果是，继续判断所述用户的登录账号是否与所述登录终端的常用登录  
5 账号相关联；

如果否，判定所述登录终端为该用户的非可信终端。

可选的，所述第二判断模块具体用于：

查询所述登录终端的常用登录账号；其中所述常用登录账号为所述登录终端的历史登录账号中登入次数达到阈值的登录账号；

10 判断所述用户的登录账号与所述常用登录账号是否曾在同一可信终端上登录，并且登录次数均达到阈值；

如果是，确定所述用户的登录账号与所述常用登录账号相关联，并在本地保存所述用户的登录账号与所述历史登录账号之间的关联关系。

可选的，所述同一可信终端为同一家用可信终端。

15 根据本申请实施例的第三方面，本申请提出一种可信终端验证装置，包括：

处理器；用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为：

判断用户的登录终端是否匹配本地记录的该用户的可信终端；

20 当判断出所述登录终端不匹配本地记录的该用户的可信终端时，判断用户的登录账号与所述登录终端的常用登录账号是否相关联；

如果是，判定所述登录终端为该用户的可信终端。

本申请基于现有实现中对登录终端的认证方案，通过在判断用户的登录终端是否为该用户的可信终端时，引入了对登录账号与登录终端的常用登录  
25 账号之间的关联性判断，当判断出用户的登录账号与登录终端的常用登录账号相关联时，则判定该登录终端为该用户的可信终端。通过该方案，可以实现在用户之间交叉使用登录终端的应用场景中，避免对该登录终端进行复杂

的重复认证。

## 附图说明

图 1 是本申请一实施例提供的一种可信终端验证方法的流程图；

图 2 是本申请一实施例提供的另一种可信终端验证方法的流程图；

5 图 3 是本申请一实施例提供的服务器对用户的登录终端进行认证的示意图；

图 4 是本申请一实施例提供的终端分析系统的处理流程图；

图 5 是本申请一实施例提供的用户认证系统的处理流程图；

图 6 是本申请一实施例提供的一种可信终端验证装置的逻辑结构示意图。

## 10 具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

15 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目

20 目的任何或所有可能组合。

应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在...时”或“当...时”或“响应

于确定”。

对于用户之间交叉使用登录终端登录支付账号的应用场景中，目前的实现方式仍然是通过服务端，结合该登录终端的硬件信息对所有的用户的登录终端分别进行认证，当认证成功后，服务端在本地将该登录终端记录为该用户的可信终端，当用户使用可信终端进行敏感操作时，不对该用户的登录终端进行重复认证或者只进行简单的认证。

然而，上述方案中会存在如下问题：

例如，以家人之间使用共同的登录终端登录支付账号的应用场景为例，按照上述方法对登录终端进行认证时，通常是基于用户的登录信息，比如用户的交易信息、IP 地址以及登录时间段等进行认证，因此不同的家庭成员使用同一个登录终端登录自己的支付账号时，服务端会对不同的家庭成员逐一进行登录终端的认证。

然而，由于家庭成员之间的信任程度通常很高，因此当家庭成员之间使用同一个登录终端登录自己的支付账号时，服务端对不同的家庭成员对逐一进行登录终端的认证完全没有必要。

有鉴于此，本申请基于现有技术中对登录终端进行认证的技术方案，通过在对登录终端进行认证的过程中，引入对登录账号与登录终端的常用登录账号之间的关联性的判断，当判断出用户的登录账号与登录终端的常用登录账号相关联时，则判定该登录终端为该用户的可信终端。

通过该方案，实现了在用户之间交叉使用登录终端的应用场景中，可以通过用户的登录账号与登录终端的常用登录账号之间的关联性来判断该登录终端是否为该用户的可信终端，从而避免了对该登录终端进行复杂的重复认证。

下面通过具体实施例并结合不同应用实例对本申请进行描述。

请参考图 1，图 1 是本申请一实施例提供的一种可信终端验证方法，该方法的执行主体可以为服务端；所述方法包括以下步骤：

步骤 101，判断用户的登录终端是否匹配本地记录的该用户的可信终端；

在该步骤中，在判断该用户的登录终端是否为该用户的可信终端时，服务端可以通过获取该登录终端的硬件信息，然后将该终端的硬件信息与数据库中记录的该用户的可信终端的硬件信息依次进行匹配，如果匹配上了，表明当前该登录终端对于该用户为可信终端；相反，如果没有匹配上，表明该登录终端对于该用户为非可信终端，服务端对于非可信终端可以只记录该终端的硬件信息以及用户使用该终端进行登录的次数。

其中，服务端在针对用户进行登录终端的认证时，仍然可以根据用户的登录信息，比如用户的交易信息、IP 地址以及登录时间段等进行认证，当认证通过后，可以在本地将该登录终端记录为用户的可信终端。另外，服务端对于已在本地记录的可信终端，还可以根据终端类型进行分类。

例如，服务端可以根据终端类型以及该可信终端的常用时间段，将本地记录的可信终端划分为手持可信终端，家用可信终端和办公可用终端。如果所述可信终端为手持终端时，服务端可以直接将该类可信终端在本地归类为手持可信终端；当识别出所述可信终端为 PC 终端时，服务端可以进一步判断该类可信终端的常用时间段是否为办公时间段或家用时间段；如果为家用时间段，服务端可以直接将该类可信终端在本地归类为家用可信终端；如果为办公时间段，服务端可以直接将该类可信终端在本地归类为办公可信终端。

所述登录终端的硬件信息，根据登录终端的终端类型的不同可以包含不同的信息；例如，如果所述登录终端为 PC 终端，那么所述硬件信息可以包括 PC 的主板 MAC，网卡 MAC，操作系统等信息；如果所述登录终端为手机终端，那么所述硬件信息可以包括手机配件的硬件信息，手机系统等信息。

步骤 102，当判断出所述登录终端不匹配本地记录的该用户的可信终端时，判断所述用户的登录账号与所述登录终端的常用登录账号是否相关联；

步骤 103，如果是，判定所述登录终端为该用户的可信终端。

在以上步骤中，当用户的登录终端为服务端在本地记录的该用户的可信终端时，可以不对该登录终端进行复杂的重复认证或者只进行简单的认证；相反，当用户的登录终端不是服务端在本地记录的该用户的可信终端时，服

务端可以进一步获取该用户的登录账号,以及所述登录终端的历史登陆账号,通过判断该用户的登录账号与该登录终端的历史登录账号是否关联,来进一步确认该登录终端是否为该用户的可信终端。

具体的,服务端可以在获取到的历史登录账号中确定出常用登录账号;

- 5 例如,可以将所述历史登录账号中登录次数达到阈值的登录账号作为常用登录账号。当确认出常用登录账号时,服务端可以通过查询本地的数据库,判断该常用登录账号是否与该用户本次登录所使用的登录账号是否曾在同一可信终端上登录,并且登录次数达到阈值;如果是,表明该用户本次登录所使用的登录账号与该登录终端的常用登录账号具有极高的关联性,那么服务端
- 10 可以直接判定该登录终端为该用户可信终端。

- 在一种优选的实施方式中,在判断所述常用登录账号与所述用户本次登录所使用的登录账号是否曾在同一可信终端上登录时,所述同一可信终端可以为同一家用可信终端。当所述常用登录账号与所述用户本次登录所使用的登录账号曾在同一家用可信终端上登录,并且登录次数达到阈值时,所述用
- 15 户与所述常用登录账号对应的用户之间很可能是家人关系,因此对于这种情况,可以直接判定所述登录终端为该用户的可信终端。

- 在实现时,服务端可以分别获取本地记录的各家用可信终端的常用登录账号,然后根据获取到的常用登录账号来建立家人关系数据,当对登入用户进行认证时,可以直接查询已建立的家人关系数据来确认当前登入的用户与
- 20 经常使用该登录终端的用户之间是否为家人关系。

当然,在具体应用中,在判断该常用登录账号与该用户本次登录所使用的登录账号曾在同一可信终端上登录时,所述同一可信终端也可以是同一手持可信终端或办公可信终端。

- 另外,服务端在进行上述登录账号之间的关联性判断之前,服务端还可
- 25 以对用户进行进一步的筛选以确定出所述登录终端的常用用户,只针对常用用户进行上述登录账号之间的关联性判断。

例如,服务端还可以判断所述用户的登录账号在所述登录终端上的登入

次数是否达到阈值；如果是，表明该用户为常用用户，可以继续判断所述用户的登录账号是否与所述登录终端的常用登录账号相关联；如果否，表明该用户为非常用用户，可以直接判定所述登录终端为该用户的非可信终端。例如，以所述同一可信终端为同一家用可信终端为例，如果某一用户使用所述家用可信登录终端的登录次数小于阈值时，比如只有一次，那么该用户很可能仅仅是造访的访客，对于这类用户，服务端执行上述登录账号之间的关联性判断没有意义，因此可以直接判定所述登录终端为该用户的非可信终端。

在本实施例中，服务端通过在对登录终端进行认证的过程中，引入对登录账号与登录终端的常用登录账号之间的关联性的判断，当判断出用户的登录账号与登录终端的常用登录账号相关联时，则判定该登录终端为该用户的可信终端。

通过该方案，实现了在用户之间交叉使用登录终端的应用场景中，可以通过用户的登录账号与登录终端的常用登录账号之间的关联性来判断该登录终端是否为该用户的可信终端，从而避免了对该登录终端进行复杂的重复认证。

请参考图 2，图 2 是本申请一实施例提供的一种可信终端验证方法，该方法的执行主体可以为服务器；所述方法包括以下步骤：

步骤 201、判断用户的登录终端是否匹配本地记录的该用户的可信终端；

步骤 202、当判断出所述登录终端不匹配本地记录的该用户的可信终端时，查询所述登录终端的常用登录账号；其中所述常用登录账号为所述登录终端的历史登录账号中登入次数达到阈值的登录账号；

步骤 203，判断所述用户的登录账号与所述常用登录账号是否曾在同一可信终端上登录，并且登录次数均达到阈值；如果是，确定所述用户的登录账号与所述常用登录账号相关联，并在本地保存所述用户的登录账号与所述历史登录账号之间的关联关系。

步骤 204、当确定所述用户的登录账号与所述常用登录账号相关联时，

判定所述登录终端为该用户的可信终端。

在本实施例中，服务器在判断该用户的登录终端是否为该用户的可信终端时，可以通过获取该登录终端的硬件信息，然后将该终端的硬件信息与数据库中记录的该用户的可信终端的硬件信息依次进行匹配，如果匹配上了，  
5 表明当前该登录终端对于该用户为可信终端；相反，如果没有匹配上，表明该登录终端对于该用户为非可信终端。对于非可信终端，服务器可以只记录该终端的硬件信息以及用户使用该终端进行登录的次数。

其中，服务器在针对用户进行登录终端的认证时，仍然可以基于现有实现中对用户进行登录终端的认证方案。例如，服务器仍然可以根据用户的登  
10 录信息，比如用户的交易信息、IP 地址以及登录时间段等信息对用户的登录终端进行认证，当认证通过后，可以在本地将该登录终端记录为用户的可信终端。

在实现时，服务器可以通过将本地的认证系统划分为不同的子系统，不同的子系统互相配合，来完成以上对用户的登录终端的认证的过程。

15 例如，请参见图 3，服务器的认证系统划分完成后的子系统可以包括用户操作系统、用户认证系统和终端分析系统。值得说明的是，以上对服务器的认证系统进行子系统的划分仅为示例性，并不用于限定本发明。

### 1) 用户操作系统

所述用户操作系统，用于记录用户的操作，比如用户登录支付宝系统的  
20 登录、退出、转账、用户信息修改、登入次数等操作，并将记录的用户操作保存到数据库中；所述用户操作系统还用于获取用户的操作环境，比如用户的登录终端的硬件信息，并将获取到的用户的登录终端的硬件信息传给终端分析系统进行分析。

例如，用户操作系统可以在用户操作的时候分析用户的操作环境，获取  
25 用户的登录终端的硬件信息，根据获取到的硬件信息进行建模，并将建模完成的硬件信息模型传给终端分析系统进行分析。其中，所述登录终端的硬件信息，根据登录终端的终端类型的不同可以包含不同的信息；例如，如果所

述登录终端为 PC 终端，那么所述硬件信息可以包括 PC 的主板 MAC，网卡 MAC，操作系统等信息；如果所述登录终端为手机终端，那么所述硬件信息可以包括手机配件的硬件信息，手机系统等信息。

## 2) 终端分析系统

5 所述终端分析系统，用于根据用户操作系统传来的硬件信息模型对用户的登录终端进行分析，根据分析结果对用户的登录终端进行认证，并将认证出的该用户的可信终端在数据库中进行保存。同时，终端分析系统还可以根据终端类型对数据库中记录的可信终端进行分类。

例如，请参见图 3 和图 4，终端分析系统仍然可以根据用户的登录信息，  
10 比如用户的交易信息、IP 地址以及登录时间段等对登录终端进行分析，根据分析结果对用户的登录终端进行认证，当认证通过后，可以在本地将该登录终端在本地的数据库中记录为用户的可信终端。对于数据库中记录的可信终端，还可以由终端分析系统根据终端类型划分为手持可信终端，家用可信终端和办公可用终端。

15 具体的，如果根据硬件信息识别出所述可信终端为手持终端时，终端分析系统可以直接将该类可信终端在本地归类为手持可信终端；如果根据硬件信息识别出所述可信终端为 PC 终端时，终端分析系统可以进一步判断该类可信终端的常用时间段是否为办公时间段或家用时间段；如果为家用时间段，终端分析系统可以直接将该类可信终端在本地归类为家用可信终端；如果为  
20 办公时间段，终端分析系统可以直接将该类可信终端在本地归类为办公可信终端。

其中，对于不隶属于家用可信终端、办公可信终端以及手持可信终端中任何一种的登录终端，可以在本地将此类登录终端归类为其他终端。由于此时所述其他终端还不是可信终端，因此可以不存入所述数据库。

## 25 3) 用户认证系统

所述用户认证系统，用于调用所述数据库，对用户的登录终端进行认证。

具体的，用户认证系统可以调用所述数据库，将用户的登录终端的硬件

信息与所述数据库中记录的该用户的可信终端的硬件信息进行匹配，如果匹配到了对应的信息，可以确定该登录终端为该用户的可信终端，那么该用户登录时可以不对该登录终端进行重复认证或只进行简单认证。

请参见图 5，如果未匹配到任何信息，可以进一步确定该登录终端是否匹配由终端分析系统记录的所述其他终端。如果通过查询获悉，该登录终端为终端分析系统记录的所述其他终端，用户认证系统可以进一步调用数据库，获取该用户的登录账号，以及所述登录终端的历史登陆账号，通过判断该用户的登录账号与该登录终端的历史登录账号是否关联来判断该登录终端是否为该用户的可信终端。

具体的，用户认证系统可以将所述历史登录账号中登录次数达到阈值的登录账号作为常用登录账号，然后通过向数据库查询，来判断该常用登录账号是否与该用户本次登录所使用的登录账号是否曾在同一可信终端上登录，并且登录次数达到阈值；如果是，表明该用户本次登录所使用的登录账号与该登录终端的常用登录账号具有极高的关联性，那么服务端可以直接判定该登录终端为该用户可信终端，当该用户通过该终端登录后，进行敏感操作时，可以不对该用户进行重复认证或者只进行简单认证。

在一种优选的实施方式中，在判断所述常用登录账号与所述用户本次登录所使用的登录账号是否曾在同一可信终端上登录时，所述同一可信终端可以为同一家用可信终端。

当所述常用登录账号与所述用户本次登录所使用的登录账号曾在同一家用可信终端上登录，并且登录次数达到阈值时，所述用户与所述常用登录账号对应的用户之间很可能是家人关系，因此对于这种情况，用户认证系统可以直接判定该登录终端为该用户的可信终端。

其中，判断所述用户与所述常用登录账号对应的用户之间是否为家人关系，在具体实现时，用户认证系统可以分别向数据库查询各家用可信终端的常用登录账号，然后根据获取到的常用登录账号建立家人关系数据，当对登录用户进行认证时，可以直接查询已建立的家人关系数据来确认当前登入的

用户与经常使用该登录终端的用户之间是否为家人关系。

另外，在判断所述常用登录账号与所述用户的登录账号是否曾在同一可信终端上登录时，所述同一可信终端也可以是同一手持可信终端或办公可信终端。当判断初所述常用登录账号与所述用户的登录账号曾在同一手持可信终端或者办公可信终端上登录时，用户认证系统可以通知终端分析系统，将该登录终端在数据库中记录为该用户的可信终端，同时将该终端在数据库中归类为手持可信终端或者办公可信终端，不再赘述。

通过以上实施例可知，服务器通过在对登录终端进行认证的过程中，引入对登录账号与登录终端的常用登录账号之间的关联性的判断，当判断出用户的登录账号与登录终端的常用登录账号相关联时，则判定该登录终端为该用户的可信终端。

通过该方案，实现了在用户之间交叉使用登录终端的应用场景中，可以通过用户的登录账号与登录终端的常用登录账号之间的关联性来判断该登录终端是否为该用户的可信终端，从而避免了对该登录终端进行复杂的重复认证。

在另一个可选的实施例中，在以上实施例的基础上，服务器在进行上述登录账号之间的关联性判断之前，服务端还可以对用户进行进一步的筛选以确定出所述登录终端的常用用户，只针对常用用户进行上述登录账号之间的关联性判断。

例如，用户认证系统还可以判断所述用户的登录账号在所述登录终端上的登入次数是否达到阈值；如果是，表明该用户为常用用户，可以继续判断所述用户的登录账号是否与所述登录终端的常用登录账号相关联；如果否，表明该用户为非常用用户，用户认证系统可以直接判定所述登录终端为该用户的非可信终端。

例如，以所述同一可信终端为同一家用可信终端为例，如果某一用户使用所述家用可信登录终端的登录次数小于阈值时，比如只有一次，那么该用

户很可能仅仅是造访的访客，对于这类用户，用户认证系统执行上述登录账号之间的关联性判断没有意义，因此用户认证系统可以直接判定该登录终端为该用户的非可信终端。

5       与上述方法实施例相对应，本申请还提供了一种可信终端验证装置的实施例。以软件实现为例，所述装置可以运行在服务器上，作为本申请装置的运行载体，所述服务器通常至少包括有 CPU、内存以及非易失性存储器，还可能包括 I/O 接口等硬件。请参考图 6，图 6 为本申请一种示例性实施例中提供的可信终端验证装置的逻辑结构示意图，所述装置 60 包括：

10       第一判断模块 601，用于判断用户的登录终端是否匹配本地记录的可信终端；

第二判断模块 602，用于在判断出所述登录终端不匹配本地记录的可信终端时，判断用户的登录账号与所述登录终端的常用登录账号是否相关联；如果是，判定所述登录终端为该用户的可信终端。

15       在本实施例中，所述装置 60 还包括：

归类模块 603，用于在第一判断模块判断用户的登录终端是否匹配本地记录的该用户的可信终端之前，根据所述可信终端的硬件信息识别所述可信终端的终端类型；

20       当识别出所述可信终端为手持终端时，将所述可信终端在本地归类为手持可信终端；

当识别出所述可信终端为 PC 终端时，判断所述可信终端的常用时间段是否为办公时间段或家用时间段；

当所述可信终端的常用时间段为办公时间段时，将所述可信终端在本地归类为办公可信终端；

25       当所述可信终端的常用时间段为家用时间段时，将所述可信终端在本地归类为家用可信终端。

在本实施例中，所述第二判断模块 602 具体用于：

在判断用户的登录账号与所述登录终端的常用登录账号是否相关联之前，判断所述用户的登录账号在所述登录终端上的登入次数是否达到阈值；

如果是，继续判断所述用户的登录账号是否与所述登录终端的常用登录账号相关联；

5 如果否，判定所述登录终端为该用户的非可信终端。

在本实施例中，所述第二判断模块 602 具体用于：

查询所述登录终端的常用登录账号；其中所述常用登录账号为所述登录终端的历史登录账号中登入次数达到阈值的登录账号；

10 判断所述用户的登录账号与所述常用登录账号是否曾在同一可信终端上登录，并且登录次数均达到阈值；

如果是，确定所述用户的登录账号与所述常用登录账号相关联，并在本地保存所述用户的登录账号与所述历史登录账号之间的关联关系。

在本实施例中，所述同一可信终端可以为同一家用可信终端。

对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际需要选择其中的部分或者全部模块来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

15 20

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

25 本申请还提供了一种服务器的实施例。

该服务器包括：处理器，以及用于存储所述处理器可执行指令的存储器；进一步，该服务器还可以包括输入/输出接口，网络接口，各种硬件等。

所述服务器可以被配置为：

判断用户的登录终端是否匹配本地记录的该用户的可信终端；

当判断出所述登录终端不匹配本地记录的该用户的可信终端时，判断所述用户的登录账号与所述登录终端的常用登录账号是否相关联；

5 如果是，判定所述登录终端为该用户的可信终端。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被  
10 视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

## 权 利 要 求 书

1. 一种可信终端验证方法, 应用在服务端, 其特征在于, 所述方法包括:  
判断用户的登录终端是否匹配本地记录的该用户的可信终端;

当判断出所述登录终端不匹配本地记录的该用户的可信终端时, 判断所  
5 述用户的登录账号与所述登录终端的常用登录账号是否相关联;  
如果是, 判定所述登录终端为该用户的可信终端。

2. 根据权利要求 1 所述的方法, 其特征在于, 所述判断用户的登录终  
端是否匹配本地记录的该用户的可信终端之前, 所述方法还包括:

根据所述可信终端的硬件信息识别所述可信终端的终端类型;

10 当识别出所述可信终端为手持终端时, 将所述可信终端在本地归类为手  
持可信终端;

当识别出所述可信终端为 PC 终端时, 判断所述可信终端的常用时间段  
是否为办公时间段或家用时间段;

当所述可信终端的常用时间段为办公时间段时, 将所述可信终端在本地  
15 归类为办公可信终端;

当所述可信终端的常用时间段为家用时间段时, 将所述可信终端在本地  
归类为家用可信终端。

3. 根据权利要求 1 所述的方法, 其特征在于, 所述判断用户的登录账  
号是否与所述登录终端的常用登录账号相关联之前, 所述方法还包括:

20 判断所述用户的登录账号在所述登录终端上的登入次数是否达到阈值;  
如果是, 继续判断所述用户的登录账号是否与所述登录终端的常用登录  
账号相关联;

如果否, 判定所述登录终端为该用户的非可信终端。

4. 根据权利要求 1 所述的方法, 其特征在于, 所述判断用户的登录账  
25 号与所述登录终端的常用登录账号是否相关联包括:

查询所述登录终端的常用登录账号; 其中所述常用登录账号为所述登录

终端的历史登录账号中登入次数达到阈值的登录账号；

判断所述用户的登录账号与所述常用登录账号是否曾在同一可信终端上登录，并且登录次数均达到阈值；

如果是，确定所述用户的登录账号与所述常用登录账号相关联，并在本地保存所述用户的登录账号与所述历史登录账号之间的关联关系。

5 5. 根据权利要求 4 所述的方法，其特征在于，所述同一可信终端为同一家用可信终端。

6、一种终端验证装置，应用在服务端，其特征在于，所述装置包括：

第一判断模块，用于判断用户的登录终端是否匹配本地记录的可信终端；

10 第二判断模块，用于在判断出所述登录终端不匹配本地记录的可信终端时，判断用户的登录账号与所述登录终端的常用登录账号是否相关联；如果是，判定所述登录终端为该用户的可信终端。

7. 根据权利要求 6 所述的装置，其特征在于，所述装置还包括：

15 归类模块，用于在第一判断模块判断用户的登录终端是否匹配本地记录的该用户的可信终端之前，根据所述可信终端的硬件信息识别所述可信终端的终端类型；

当识别出所述可信终端为手持终端时，将所述可信终端在本地归类为手持可信终端；

20 当识别出所述可信终端为 PC 终端时，判断所述可信终端的常用时间段是否为办公时间段或家用时间段；

当所述可信终端的常用时间段为办公时间段时，将所述可信终端在本地归类为办公可信终端；

当所述可信终端的常用时间段为家用时间段时，将所述可信终端在本地归类为家用可信终端。

25 8. 根据权利要求 6 所述的装置，其特征在于，所述第二判断模块具体用于：

在判断用户的登录账号与所述登录终端的常用登录账号是否相关联之

前，判断所述用户的登录账号在所述登录终端上的登入次数是否达到阈值；

如果是，继续判断所述用户的登录账号是否与所述登录终端的常用登录账号相关联；

如果否，判定所述登录终端为该用户的非可信终端。

- 5        9. 根据权利要求 6 所述的装置，其特征在于，所述第二判断模块具体用于：

查询所述登录终端的常用登录账号；其中所述常用登录账号为所述登录终端的历史登录账号中登入次数达到阈值的登录账号；

- 10       判断所述用户的登录账号与所述常用登录账号是否曾在同一可信终端上登录，并且登录次数均达到阈值；

如果是，确定所述用户的登录账号与所述常用登录账号相关联，并在本地保存所述用户的登录账号与所述历史登录账号之间的关联关系。

10. 根据权利要求 9 所述的装置，其特征在于，所述同一可信终端为同一家用可信终端。

- 15       11、一种可信终端验证装置，其特征在于，包括：

处理器；用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为：

判断用户的登录终端是否匹配本地记录的该用户的可信终端；

- 20       当判断出所述登录终端不匹配本地记录的该用户的可信终端时，判断用户的登录账号与所述登录终端的常用登录账号是否相关联；

如果是，判定所述登录终端为该用户的可信终端。