(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103581108 B
(45)授权公告日 2017.05.03

(21)申请号 201210251542.7

(22)申请日 2012.07.19

(65)同一申请的已公布的文献号
申请公布号 CN 103581108 A

(43)申请公布日 2014.02.12

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼岛资本大厦一座四层847号邮箱

(72)发明人 黄冕

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王宝筠

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

(56)对比文件

WO 2012054779 A1,2012.04.26,说明书第[0023]-[0027]段、第[0029]段、第[0036]-[0039]段、第[0066]-[0076]段、第[0133]段、图1.

CN 102158465 A,2011.08.17,说明书第[0021]-[0022]段、第[0045]-[0051]段、第[0076]-[0077]段.

审查员 刘莉

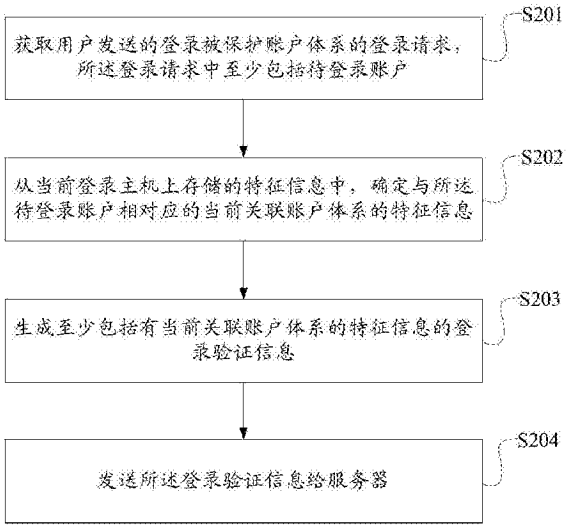
权利要求书2页 说明书10页 附图6页

(54)发明名称

一种登录验证方法、客户端、服务器及系统

(57)摘要

本申请提供了一种登录验证方法、客户端、服务器及系统，该方法中，在用户登录时，客户端获取用户发送的登录被保护账户体系的登录请求，并确定与待登录账户相对应的当前关联账户体系的特征信息；生成登录验证信息；发送所述登录验证信息给服务器，服务器通过与预先存储的、与所述待登录账户相对应的可信特征信息进行对比，当两者存在交集时，确定所述登录为可信登录。该方法中，服务器根据预先存储的，与待登录账户对应的可信特征信息对用户的登录行为进行验证，无需通过数字证书或U盾来进行额外的操作进行登录验证，简化了登录验证过程，提高了服务器进行登录验证的效率。



CN 103581108 B

1.一种登录验证方法,其特征在于,包括:

获取用户发送的登录被保护账户体系的登录请求,所述登录请求中至少包括待登录账户;

从当前登录主机上存储的特征信息中,确定与所述待登录账户相对应的当前关联账户体系的特征信息;

生成至少包括有所述当前关联账户体系的特征信息的登录验证信息;

发送所述登录验证信息给服务器,服务器通过与预先存储的、与所述待登录账户相对应的可信特征信息进行对比,当两者存在交集,且所述交集符合预设条件时,确定所述登录为可信登录的依据。

2.根据权利要求1所述的方法,其特征在于,所述可信特征信息按照以下步骤获得:

获取用户发送的,首次登录所述待登录账户的登录请求;

从首次登录的主机上存储的特征信息中,确定与所述待登录账户对应的首次关联账户体系的特征信息;

发送所述首次关联账户体系的特征信息给服务器,所述首次关联账户体系的特征信息为所述服务器确定与所述待登录账户对应的可信特征信息的依据。

3.根据权利要求1或2所述的方法,其特征在于,所述特征信息包括:账户体系所对应的网络流量中的预设报文或所述预设报文中的预设字段。

4.根据权利要求1或2所述的方法,其特征在于,还包括:

将所述当前关联账户体系的特征信息进行基于哈希值的不可逆处理。

5.一种登录验证方法,其特征在于,包括:

接收客户端发送的登录验证信息,所述登录验证信息至少包括有与待登录账户对应的当前关联账户体系的特征信息的登录验证信息,所述当前关联账户体系的特征信息为客户端获取用户发送的登录请求后,从当前登录主机存储的特征信息中确定的;

将所述当前关联账户体系的特征信息与预先存储的,与所述待登录账户相对应的可信特征信息进行对比;

当两者存在交集且所述交集符合预设条件时,确定所述登录为可信登录。

6.根据权利要求5所述的方法,其特征在于,当两者不存在交集或所述交集不符合预设条件时,还包括:

验证所述当前登录主机是否为可信主机,若是,则确定所述登录为可信登录,若否,则确定所述登录为不可信登录。

7.根据权利要求6所述的方法,其特征在于,当所述登录验证信息中还包括有所述当前登录主机的机器特征时,所述验证所述当前登录主机是否为可信主机的过程包括:

当所述当前登录主机的机器特征符合第一可信条件时,所述当前登录主机为可信主机。

8.根据权利要求6所述的方法,其特征在于,所述验证所述当前登录主机是否为可信主机的过程包括:

获取所述当前登录主机的历史登录记录;

当所述历史登录记录符合第二可信条件时,所述当前登录主机为可信主机。

9.根据权利要求6所述的方法,其特征在于,所述验证所述当前登录主机是否为可信主

机的过程包括：

对所述当前登录主机进行二次认证；

当所述当前登录主机二次认证通过时，所述当前登录主机为可信主机。

10.根据权利要求6-9中任意一项所述的方法，其特征在于，所述可信特征信息按照以下步骤获得；

接收客户端发送的，与所述待登录账户对应的首次关联账户体系的特征信息，所述首次关联账户体系的特征信息为，用户首次登录所述待登录账户时，从首次登录的主机上存储的特征信息中确定的；

依据所述首次关联账户体系的特征信息，确定与所述待登录账户对应的可信特征信息。

11.根据权利要求10所述的方法，其特征在于，当验证所述当前登录主机为可信主机，确定所述登录为可信登录后，还包括：

将所述当前关联账户体系的特征信息添加到所述预先存储的，与所述待登录账户相对应的可信特征信息中，以更新所述待登录账户对应的可信特征信息。

12.一种登录验证客户端，其特征在于，包括：

登录请求获取模块，用于获取用户发送的登录被保护账户体系的登录请求，所述登录请求中至少包括待登录账户；

当前关联账户体系的特征信息确定模块，用于从当前登录主机上存储的特征信息中，确定与所述待登录账户相对应的当前关联账户体系的特征信息；

登录验证信息生成模块，用于生成至少包括所述当前关联账户体系的特征信息的登录验证信息；

登录验证信息发送模块，用于发送所述登录验证信息给服务器，服务器通过与预先存储的、与所述待登录账户相对应的可信特征信息进行对比，当两者存在交集且所述交集符合预设条件时，确定所述登录为可信登录的依据。

13.一种登录验证服务器，其特征在于，包括：

登录验证信息接收模块，用于接收客户端发送的登录验证信息，所述登录验证信息至少包括与待登录账户对应的当前关联账户体系的特征信息的登录验证信息，所述当前关联账户体系的特征信息为客户端获取用户发送的登录请求后，从当前登录主机存储的特征信息中确定的；

对比模块，用于将所述当前关联账户体系的特征信息与预先存储的，与所述待登录账户相对应的可信特征信息进行对比；

可信登录确定模块，用于当两者存在交集且所述交集符合预设条件时，确定所述登录为可信登录。

14.一种登录验证系统，其特征在于，包括：如权利要求12所述的客户端和如权利要求13所述的服务器。

一种登录验证方法、客户端、服务器及系统

技术领域

[0001] 本申请涉及互联网技术领域，特别涉及一种登录验证方法、客户端、服务器及系统。

背景技术

[0002] 随着互联网技术的发展，网络已经与人们的生活密不可分，越来越多的人选择网络作为通信、娱乐和购物的工具。通过申请QQ、MSN账号等与他人进行联系，或者通过注册淘宝等网上购物网站账号进行购物。但是，目前账号被盗现象非常明显，很多用户的QQ、MSN账号被他人利用盗号软件等非法手段盗取，非法登录，影响了用户的正常使用，更有甚者，造成了用户的经济损失，由于网络服务器无法识别用户的账号是正常登录还是非法登录，从而使得网络的安全性大大降低。

[0003] 目前，各个服务器为了能够准确识别用户登录是否可信，解决账号被非法登录的问题，很多服务提供者选择了数字证书或账号与硬件绑定等方式。数字证书就是互联网通讯中标志通讯各方身份信息的一系列数据，提供了一种通过网络在服务器端验证用户身份的方式，根据用户身份给予相应的网络资源访问权限，用户申请使用数字证书后，如果在其他电脑登录，在没有导入数字证书备份的情况下，用户只能查询账户，不能进行任何操作，从而增强该用户的账户的使用安全性。但是用户更换平常使用的电脑后，就需要重新申请数字证书才能使服务器对其准确识别。

[0004] 而账号与硬件绑定的方式还有U盾或移动数字证书，首先用户需要购买U盾，然后建立账号与U盾的联系。当进行网上交易时，银行会向用户发送由时间字串、地址字串、交易信息字串和防重放攻击字串组合在一起进行加密后得到的字串A，用户的U盾将根据用户的个人证书对字串A进行不可逆运算得到字串B，并将字串B发送给银行，银行端也同时进行该不可逆运算，如果银行运算结果和用户的运算结果一致便认为用户登录合法，交易便可以完成，如果不一致便认为用户不合法，交易便会失败，从而保证了网络的安全性。

[0005] 但是，综上所述可以看出，在对用户登录进行验证的过程中，无论是申请数字证书的过程还是建立U盾与用户账户间联系的过程都较为繁琐，无法在服务器端实现高效且准确的对用户登录是否可信识别。

发明内容

[0006] 本申请的目的在于，提供一种登录验证方法，以解决现有技术中无法在服务器端实现高效且准确的对用户登录是否可信识别的问题，具体方案如下：

[0007] 一种登录验证方法，包括：

[0008] 获取用户发送的登录被保护账户体系的登录请求，所述登录请求中至少包括待登录账户；

[0009] 从当前登录主机上存储的特征信息中，确定与所述待登录账户相对应的当前关联账户体系的特征信息；

[0010] 生成至少包括有所述当前关联账户体系的特征信息的登录验证信息；

[0011] 发送所述登录验证信息给服务器，所述登录验证信息中的当前关联账户体系的特征信息为，服务器通过与预先存储的、与所述待登录账户相对应的可信特征信息进行对比，当两者存在交集，且所述交集符合预设条件时，确定所述登录为可信登录的依据。

[0012] 优选的，所述可信特征信息按照以下步骤获得：

[0013] 获取用户发送的，首次登录所述待登录账户的登录请求；

[0014] 从首次登录的主机上存储的特征信息中，确定与所述待登录账户对应的首次关联账户体系的特征信息；

[0015] 发送所述首次关联账户体系的特征信息给服务器，所述首次关联账户体系的特征信息为所述服务器确定与所述待登录账户对应的可信特征信息的依据。

[0016] 优选的，所述特征信息包括：账户体系所对应的网络流量中的预设报文或所述预设报文中的预设字段。

[0017] 优选的，还包括：

[0018] 将所述当前关联账户体系的特征信息进行不可逆处理。

[0019] 一种登录验证方法，包括：

[0020] 接收客户端发送的登录验证信息，所述登录验证信息至少包括有与待登录账户对应的当前关联账户体系的特征信息的登录验证信息，所述当前关联账户体系的特征信息为客户端获取用户发送的登录请求后，从当前登录主机存储的特征信息中确定的；

[0021] 将所述当前关联账户体系的特征信息与预先存储的，与所述待登录账户相对应的可信特征信息进行对比；

[0022] 当两者存在交集且所述交集符合预设条件时，确定所述登录为可信登录。

[0023] 优选的，当两者不存在交集或所述交集不符合预设条件时，还包括：

[0024] 验证所述当前登录主机是否为可信主机，若是，则确定所述登录为可信登录，若否，则确定所述登录为不可信登录。

[0025] 优选的，当所述登录验证信息中还包括有所述当前登录主机的机器特征时，所述验证所述当前登录主机是否为可信主机的过程包括：

[0026] 当所述当前登录主机的机器特征符合第一可信条件时，所述当前登录主机为可信主机。

[0027] 优选的，所述验证所述当前登录主机是否为可信主机的过程包括：

[0028] 获取所述当前登录主机的历史登录记录；

[0029] 当所述历史登录记录符合第二可信条件时，所述当前登录主机为可信主机。

[0030] 优选的，所述验证所述当前登录主机是否为可信主机的过程包括：

[0031] 对所述当前登录主机进行二次认证；

[0032] 当所述当前登录主机二次认证通过时，所述当前登录主机为可信主机。

[0033] 优选的，所述可信特征信息按照以下步骤获得；

[0034] 接收客户端发送的，与所述待登录账户对应的首次关联账户体系的特征信息，所述首次关联账户体系的特征信息为，用户首次登录所述待登录账户时，从首次登录的主机上存储的特征信息中确定的；

[0035] 依据所述首次关联账户体系的特征信息，确定与所述待登录账户对应的可信特征

信息。

[0036] 优选的，当验证所述当前登录主机为可信主机，确定所述登录为可信登录后，还包括：

[0037] 将所述当前关联账户体系的特征信息添加到所述预先存储的，与所述待登录账户相对应的可信特征信息中，以更新所述待登录账户对应的可信特征信息。

[0038] 本申请还提供了一种登录验证客户端、服务器和系统，用以保证上述方法在实际中的实现及应用

[0039] 一种登录验证客户端，包括：

[0040] 登录请求获取模块，用于获取用户发送的登录被保护账户体系的登录请求，所述登录请求中至少包括待登录账户；

[0041] 当前关联账户体系的特征信息确定模块，用于从当前登录主机上存储的特征信息中，确定与所述待登录账户相对应的当前关联账户体系的特征信息；

[0042] 登录验证信息生成模块，用于生成至少包括所述当前关联账户体系的特征信息的登录验证信息；

[0043] 登录验证信息发送模块，用于发送所述登录验证信息给服务器，所述登录验证信息中的当前关联账户体系的特征信息为，服务器通过与预先存储的、与所述待登录账户相对应的可信特征信息进行对比，当两者存在交集且所述交集符合预设条件时，确定所述登录为可信登录的依据。

[0044] 一种登录验证服务器，包括：

[0045] 登录验证信息接收模块，用于接收客户端发送的登录验证信息，所述登录验证信息至少包括与待登录账户对应的当前关联账户体系的特征信息的登录验证信息，所述当前关联账户体系的特征信息为客户端获取用户发送的登录请求后，从当前登录主机存储的特征信息中确定的；

[0046] 对比模块，用于将所述当前关联账户体系的特征信息与预先存储的，与所述待登录账户相对应的可信特征信息进行对比；

[0047] 可信登录确定模块，用于当两者存在交集且所述交集符合预设条件时，确定所述登录为可信登录。

[0048] 一种登录验证系统，包括：如上所述的客户端和如上所述的服务器。

[0049] 与现有技术相比，本申请包括以下优点：本申请实施例公开的一种登录验证方法，在用户登录时，客户端获取用户发送的登录被保护账户体系的登录请求，并从当前登录主机上存储的特征信息中，确定与待登录账户相对应的当前关联账户体系的特征信息；生成至少包括有所述登录请求和所述不可逆处理后的当前关联账户体系的特征信息的登录验证信息；发送所述登录验证信息给服务器，服务器通过与预先存储的、与所述待登录账户相对应的可信特征信息进行对比，当两者存在交集时，确定所述登录为可信登录。该方法中，服务器根据预先存储的，与待登录账户对应的可信特征信息对用户的登录行为进行验证，无需通过数字证书或U盾来进行额外的操作进行登录验证，简化了登录验证过程，提高了服务器进行登录验证的效率。

[0050] 进一步的，由于无需购买U盾或数字证书，降低了用户的使用成本。

[0051] 当然，实施本申请的任一产品并不一定需要同时达到以上所述的所有优点。

附图说明

[0052] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0053] 图1为本申请实施例公开的QQ账户体系与服务器进行数据交互时发送的报文示意图；

[0054] 图2为本申请实施例公开的一种登录验证方法的流程图；

[0055] 图3为本申请实施例公开可信特征信息建立过程流程图；

[0056] 图4为本申请实施例公开的又一登录验证方法的流程图；

[0057] 图5为本申请实施例公开的判断当前登录主机的机器特征是否符合第一可信条件的流程图；

[0058] 图6为本申请实施例公开的又一判断当前登录主机的机器特征是否符合第一可信条件的流程图；

[0059] 图7为本申请实施例公开的判断历史登录记录是否符合第二可信条件的流程图；

[0060] 图8为本申请实施例公开的又一判断历史登录记录是否符合第二可信条件的流程图；

[0061] 图9为本申请实施例公开的又一验证主机是否为可信主机的流程图；

[0062] 图10为本申请实施例公开的又一获得可信特征信息的流程图；

[0063] 图11为本申请实施例公开的登录验证客户端的结构示意图；

[0064] 图12为本申请实施例公开的登录验证服务器的结构示意图；

[0065] 图13为本申请实施例公开的登录验证系统的结构示意图。

具体实施方式

[0066] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅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。

[0067] 本申请可用于众多通用或专用的计算系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、包括以上任何系统或设备的分布式计算环境等等。

[0068] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0069] 本申请的主要思想之一可以包括，客户端获取用户发送的登录被保护账户体系的登录请求，所述登录请求中至少包括待登录账户；从当前登录主机上存储的特征信息中，确

定与所述待登录账户相对应的当前关联账户体系的特征信息;生成至少包括有所述登录请求和所述不可逆处理后的当前关联账户体系的特征信息的登录验证信息;发送所述登录验证信息给服务器,所述登录验证信息中的不可逆处理后的当前关联账户体系的特征信息为,服务器通过与预先存储的、与所述待登录账户相对应的可信特征信息进行对比,当两者存在交集时,确定所述登录为可信登录的依据。

[0070] 在用户进行登录的主机上,通常装很多基于账户体系的软件,如QQ,MSN,OutLook,迅雷、支付宝等,这些软件都会与服务器交互,同时发出含有一定特征流量信息的数据报文。本申请将用户通过这些账户体系与服务器进行信息交互时发送的网络流量中,某些包含有一定流量特征信息的数据报文,或者是,该数据报文中特定字段作为这些账户体系对应的特征信息,本实施例中,数据报文的类型以及特定的字段可以根据情况进行预先设定。以QQ账户体系为例,图1中所示为通过QQ账户体系与服务器进行数据交互时发送的报文,其包含有多个字节。可以将整个报文所包含的内容作为QQ账户体系对应的特征信息,也可以从其包含的多个字节中,选择特定位置处的字节所包含的信息,作为特征信息,例如,选择第7-10个字节所包含的信息,也就是QQ号码,作为QQ账户体系对应的特征信息。本申请也并不限定将账户体系与服务器进行信息交互时发送的数据报文或者数据报文中的字段作为特征信息,同样也可以将账户体系在登录主机上运行时所生成的本地数据作为特征信息,例如,运行QQ时,QQ软件获取的本地系统时间。本申请实施例公开的登录验证方法的基础在于,选择一个账户体系作为被保护账户体系,并确定某一个或某几个其他的账户体系作为被保护账户体系的关联账户体系。例如,确定支付宝为被保护账户体系,确定QQ为关联账户体系。通过关联账户体系的特征信息,来验证用户登录被保护账户体系时是否为可信。其具体的过程如下述实施例所示。

[0071] 如图2所示为本申请实施例公开的一种登录验证方法的流程,该流程应用于登录验证客户端,包括:

[0072] 步骤S201、获取用户发送的登录被保护账户体系的登录请求,所述登录请求中至少包括待登录账户;

[0073] 假设当前被保护账户体系为支付宝,当用户在主机上登录支付宝账户时,运行在主机上的登录验证客户端获取用户的登录请求。

[0074] 步骤S202、从当前登录主机上存储的特征信息中,确定与所述待登录账户相对应的当前关联账户体系的特征信息;

[0075] 假设与当前登录账户对应的关联账户体系为QQ。从当前登陆主机上存储的特征信息中,获取与登录的支付宝账户对应的当前的QQ特征信息。与支付宝账户对应的当前QQ特征信息可以为存储在当前主机上的,所有QQ账号对应的特征信息,也可以为,在预设时间段内在当前主机上进行登录过的QQ账号对应的特征信息。

[0076] 步骤S203、生成至少包括有所述当前关联账户体系的特征信息的登录验证信息;

[0077] 步骤S204、发送所述登录验证信息给服务器。

[0078] 所述登录验证信息中的当前关联账户体系的特征信息为,服务器通过与预先存储的、与所述待登录账户相对应的可信特征信息进行对比,当两者存在交集且所述交集符合预设条件时,确定所述登录为可信登录的依据。

[0079] 两者存在交集即表示,可信特征信息中包含有当前关联账户体系的特征信息中的

信息，或者，当前关联账户体系的特征信息中包含有可信特征信息中的信息。

[0080] 举例说明，假设服务器中预先存储的与待登录账户对应的可信特征信息中包含有QQ号码：A、B和C。本次登录时发送的当前关联账户体系的特征信息中包含有QQ号码A，则证明两者间存在交集。

[0081] 交集符合预设条件可以为：该交集中所包含的关联账户的个数不小于预设值，例如三个。该预设值可以根据实际情况任意设定，若当前应用的场景需要高度可靠时，该预设值可以为较大值，也就是说，当两者中的交集越多，越可靠。而若当前的应用场景无需高度可靠时，该预设值可以为一个较小值。若交集中所包含的关联账户的个数小于预设值，则虽然两者间存在交集，但是该交集不符合条件。

[0082] 进一步的，该交集符合预设条件还可为：交集中是否包含某一个或某几个特定的关联账户特征信息。例如，假设QQ号码A是特定的关联账户特征信息，若可信特征信息中包含有A、B和C，而当前关联账户特征信息中包含有B和C，若以此时的条件进行判断，由于其并不包含有特定的关联账户A，则表明两者间虽然存在交集，但是该交集并不符合预设条件。

[0083] 本实施例公开的登录验证方法中，客户端将当前登录主机上存储的，与被保护账户体系中的待登录账户对应的当前关联账户特征信息发送给服务器，从而使得服务器能够根据预先存储的与所述待登录账户对应的可信特征信息进行对比，当两者存在交集时，确定此次登录为可信登录。从而无需通过数字证书或U盾来进行额外的操作进行登录验证，简化了登录验证过程，提高了服务器进行登录验证的效率。

[0084] 进一步的，由于无需购买U盾或数字证书，降低了用户的使用成本。

[0085] 进一步的，还可以包括：

[0086] 将所述当前关联账户体系的特征信息进行不可逆处理；

[0087] 具体的操作可以为，将QQ特征信息进行取哈希值处理，得到与其对应的哈希值。

[0088] 上述将当前关联账户体系的特征信息进行不可逆处理的过程可以添加在发送所述登录验证信息给服务器之前，从而保证该特征信息传输过程中不被恶意更改，从而保证特征信息的准确性，进一步提高验证过程的准确性。

[0089] 进一步的，上述实施例中，服务器中预先存储有与待登录账户对应的可信特征信息，该可信特征信息通过以下步骤建立，具体流程如图3所示，包括：

[0090] 步骤S301、获取用户发送的，首次登录所述待登录账户的登录请求；

[0091] 用户首次注册所述待登录账户时，客户端获取器登录请求。

[0092] 步骤S302、从首次登录的主机上存储的特征信息中，确定与所述待登录账户对应的首次关联账户体系的特征信息；

[0093] 假设用户首次注册时所使用的主机上存储有三个QQ号码的特征信息，则这三个QQ号码的特征信息都将作为首次关联账户体系的特征信息。

[0094] 步骤S303、发送所述首次关联账户体系的特征信息给服务器，所述首次关联账户体系的特征信息为所述服务器确定与所述待登录账户对应的可信特征信息的依据。

[0095] 服务器接收到首次关联账户体系的特征信息后，将其进行存储，可以直接将其作为待登录账户的可信特征信息，也可以对其进行其他处理后，例如将其进行不断的更新，将更新后的内容作为与所述待处理账户对应的可信特征信息。

[0096] 本实施例中可以将客户端作为一个后台长期运行的进程，作为关联账户特征信息

学习器，该进程提取存储在主机上的关联账户特征信息等，不可逆处理后上传到服务器中。由服务器来进行存储维护，并根据客户端上传的特征信息对可信特征信息进行更新。

[0097] 由于用户在首次登录账户时很难出现不可信登录的情况，因此，将用户在首次登录时所利用的主机上存储的关联账户特征信息作为得到可信特征信息的依据是十分可靠的，能够在很大程度上保证验证过程的准确性。

[0098] 进一步的，本实施例中还可以包括：将所述首次关联账户体系的特征信息进行不可逆处理的过程。

[0099] 该过程可以添加在将所述首次关联账户体系的特征信息发送给服务器的步骤之前，从而保证该特征信息传输过程中不被恶意更改，从而保证特征信息的准确性，进一步提高后续依据该特征信息进行登录验证过程的准确性。

[0100] 图4为本申请同时公开的又一登录验证方法的流程，其应用在登录验证服务器端，具体包括：

[0101] 步骤S401、接收客户端发送的登录验证信息；

[0102] 所述登录验证信息至少包括有与待登录账户对应的当前关联账户体系的特征信息的登录验证信息，该当前关联账户体系的特征信息为客户端获取用户发送的登录请求后，从当前登录主机存储的特征信息中确定的；

[0103] 所述特征信息为账户体系所对应的网络流量中的预设报文或所述预设报文中的预设字段；

[0104] 步骤S402、将所述当前关联账户体系的特征信息与预先存储的，与所述待登录账户相对应的可信特征信息进行对比；

[0105] 假设当前关联账户体系的特征信息为QQ号码：A、B、C和D，而可信特征信息为QQ号码：C和D。

[0106] 步骤S403、当两者存在交集且所述交集符合预设条件时，确定所述登录为可信登录。

[0107] 对比上述两个特征，发现存在公共的交集C和D，若此时的预设条件为该交集中所包含的关联账户的个数不小于两个，则证明两者之间存在交集，并且，该交集符合预设条件，此次登录为可信登录。

[0108] 进一步的，当两者不存在交集，或，所述交集不符合预设条件时，还包括：验证所述当前登录主机是否为可信主机，若是，则确定所述登录为可信登录，若否，则确定所述登录为不可信登录。

[0109] 具体的，当客户端向服务器发送的登录验证信息中还包括当前登录主机的机器特征时，验证所述当前登录主机是否为可信主机的过程包括：

[0110] 判断当前登录主机的及其特征是否符合第一可信条件，如果符合，则当前登录主机为可信，若不符合，则为不可信。本申请实施例中所述的机器特征为主机的ID、主机的MAC地址、主机的硬盘序列号、主机的CPU ID等。

[0111] 上述判断当前登录主机的机器特征是否符合第一可信条件过程的一种具体实现方式如图5所示，包括：

[0112] 步骤S501、获取预先存储的，与所述待登录账户对应的首次登录机器特征；

[0113] 步骤S502、当所述首次机器登录特征与所述当前登录主机的机器特征相同时，确

定所述当前登录主机为可信主机。

[0114] 也就是说，该当前登录主机为用户第一次登录该待登录账户时的主机，因此，其为可信主机，此次登录也可认定为可信登录。

[0115] 上述判断当前登录主机的及其特征是否符合第一可信条件过程的又一实现过程如图6所示，包括：

[0116] 步骤S601、获取所述机器特征中的当前登录主机ID；

[0117] 步骤S602、当预先存储的公共主机ID集合中包含有所述当前登录主机的ID时，确定所述当前登录主机为公共主机，所述当前登录主机为不可信主机。

[0118] 上述过程中，通过判断当前登录主机是否为公共主机，例如，网吧内的主机或者公共机房内的主机，如果该当前登录主机不是公共主机，则可认定其为可信主机，若其为公共主机，则其为不可信主机。

[0119] 验证所述当前登录主机是否为可信主机的过程还可以包括：获取所述当前登录主机的历史登录记录；

[0120] 当所述历史登录记录符合第二可信条件时，所述当前登录主机为可信主机。

[0121] 上述判断历史登录记录符合第二可信条件的过程的一种实现方式如图7所示，包括：

[0122] 步骤S701、获取历史登录记录中，属于被保护账户体系下的历史登录账户个数；

[0123] 步骤S702、当所述个数不大于预设登录个数时，所述当前登录主机为可信。

[0124] 该过程中，通过当前登录主机的历史登录记录中，历史登录账户个数判断该主机是否为公共主机，若为公共主机，则不可信。

[0125] 上述判断历史登录记录符合第二可信条件的过程的又一种实现方式如图8所示，包括：

[0126] 步骤S801、获取历史登录记录中，与所述待登录账户对应的登录记录；

[0127] 步骤S802、当其登录次数超过预设次数，或者，持续登录时间超过预设时间时，所述当前登录主机为可信。

[0128] 本实施例中，通过历史登录记录，判断用户是否多次在该主机上登录，或者用户是否持续在该主机上登录了一段时间来判断该主机是否可信。其预设次数可以为五次或十次等任意设定的值。该预设时间可以为一周或一个月等任意设定的时间值。

[0129] 进一步的，验证所述当前登录主机是否为可信主机的过程还可以如图9所述，包括：

[0130] 步骤S901、对所述当前登录主机进行二次认证；

[0131] 具体的二次认证方式可以有多种，例如发送手机验证码等，在此不再赘述。

[0132] 步骤S902、当所述当前登录主机二次认证通过时，所述当前登录主机为可信主机。

[0133] 本实施例并不限定只能采用如图5-9中所示的流程来判断当前登录主机是否可信，其他能够验证主机是否可信的方法都是本申请实施例保护的范围。

[0134] 并且，本实施例也并不限定只能单独按照图5-9中任意一个流程来验证主机是否可信。本领域技术人员可以根据实际的场景，任意的将其中的判别条件进行组合，利用组合后的条件对主机进行验证，从而进一步的提高验证结果的可靠性。

[0135] 本申请实施例同时公开了服务器端获得可信特征信息的过程，如图10所示，包括：

[0136] 步骤S1001、接收客户端发送的，与所述待登录账户对应的首次关联账户体系的特征信息；

[0137] 所述首次关联账户体系的特征信息为，用户首次登录所述待登录账户时，从首次登录的主机上存储的特征信息中确定的；

[0138] 步骤S1002、依据所述首次关联账户体系的特征信息，确定与所述待登录账户对应的可信特征信息。

[0139] 本实施例中，确定与所述待登录账户对应的可信特征信息可以为，将所述首次关联账户体系的特征信息进行存储，并将其作为与待登录账户对应的可信特征信息。或者，不断对首次关联账户体系的特征信息进行更新，将更新后的内容作为可信特征信息。

[0140] 其具体的更新过程可以为：

[0141] 当验证所述当前登录主机为可信主机，确定所述登录为可信登录后，将所述不可逆处理后的当前关联账户体系的特征信息添加到所述预先存储的，与所述待登录账户相对应的可信特征信息中，以更新所述待登录账户对应的可信特征信息。

[0142] 假设用户首次关联账户体系的特征信息为QQ号码A、B和C。当前登录主机中的当前关联账户体系的特征信息为QQ号码D、E和F，当该登录主机为可信主机时，将QQ号码D、E和F添加到可信特征信息中，作为更新后可信特征信息。

[0143] 本申请实施例同时公开了一种登录验证客户端，该客户端运行在主机上，其结构如图11所示，包括：

[0144] 登录请求获取模块111，用于获取用户发送的登录被保护账户体系的登录请求，所述登录请求中至少包括待登录账户；

[0145] 当前关联账户体系的特征信息确定模块112，用于从当前登录主机上存储的特征信息中，确定与所述待登录账户相对应的当前关联账户体系的特征信息；

[0146] 登录验证信息生成模块113，用于生成至少包括所述不可逆处理后的当前关联账户体系的特征信息的登录验证信息；

[0147] 登录验证信息发送模块114，用于发送所述登录验证信息给服务器，所述登录验证信息中的当前关联账户体系的特征信息为，服务器通过与预先存储的、与所述待登录账户相对应的可信特征信息进行对比，当两者存在交集且所述交集符合预设条件时，确定所述登录为可信登录的依据。

[0148] 进一步的，还可以将当前关联账户体系的特征信息进行不可逆处理。

[0149] 进一步的，本实施例并不限定其工作过程如上所述，其具体的工作过程还可参考图2或图3所示流程。

[0150] 本实施例公开的登录验证客户端，当获取到用户登录被保护体系的登录请求时，主动获取当前登录主机上的关联账户的特征信息，并发送至服务器，作为验证登录是否可信的依据。从而实现了简化登录验证过程，提高服务器进行登录验证效率的目的。

[0151] 本申请同时公开了一种登录验证服务器，其结构如图12所示，包括：

[0152] 登录验证信息接收模块121，用于接收客户端发送的登录验证信息，所述登录验证信息至少包括与待登录账户对应的当前关联账户体系的特征信息的登录验证信息，所述当前关联账户体系的特征信息为客户端获取用户发送的登录请求后，从当前登录主机存储的特征信息中确定的；

[0153] 对比模块122，用于将所述当前关联账户体系的特征信息与预先存储的，与所述待登录账户相对应的可信特征信息进行对比；

[0154] 可信登录确定模块123，用于当两者存在交集且所述交集符合预设条件时，确定所述登录为可信登录。

[0155] 进一步的，还包括：主机验证模块124，用于当两者不存在交集或所述交集不符合预设条件时，验证所述当前登录主机是否为可信主机，若主机为可信，则登录为可信登录，若主机为不可信，则登录为不可信登录。

[0156] 进一步的，本实施例并不限定其工作过程如上所述，其具体的工作过程还可参考图4-10中所示流程。

[0157] 本实施例公开的登录验证服务器，通过将客户端发送的当前关联账户体系特征信息与可信特征信息进行对比，通过是否包含交集判断其是否为可信登录，简化了验证步骤，提高了验证的效率，并且，进一步提高了验证的可靠性。

[0158] 本申请同时公开了一种登录验证系统，其结构如图13所示，包括：如图11所示的登录验证客户端和如图12所示的登录验证服务器。两者的工作过程在此不再赘述。

[0159] 本实施例中的登录验证系统，通过登录验证客户端和登录验证服务器的协同配合，实现用户登录行为的验证，简化了现有验证过程的步骤，提高了验证效率。

[0160] 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于系统类实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0161] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0162] 以上对本申请所提供的用户身份识别方法及服务器进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

字节	描述
0	0x02 开始报文
1-2	版本号，如2007B3为0x1051
3-4	命令
5-6	序列号
7-10	QQ号
11-N	数据段
N+1	0x03 结束标志

图1

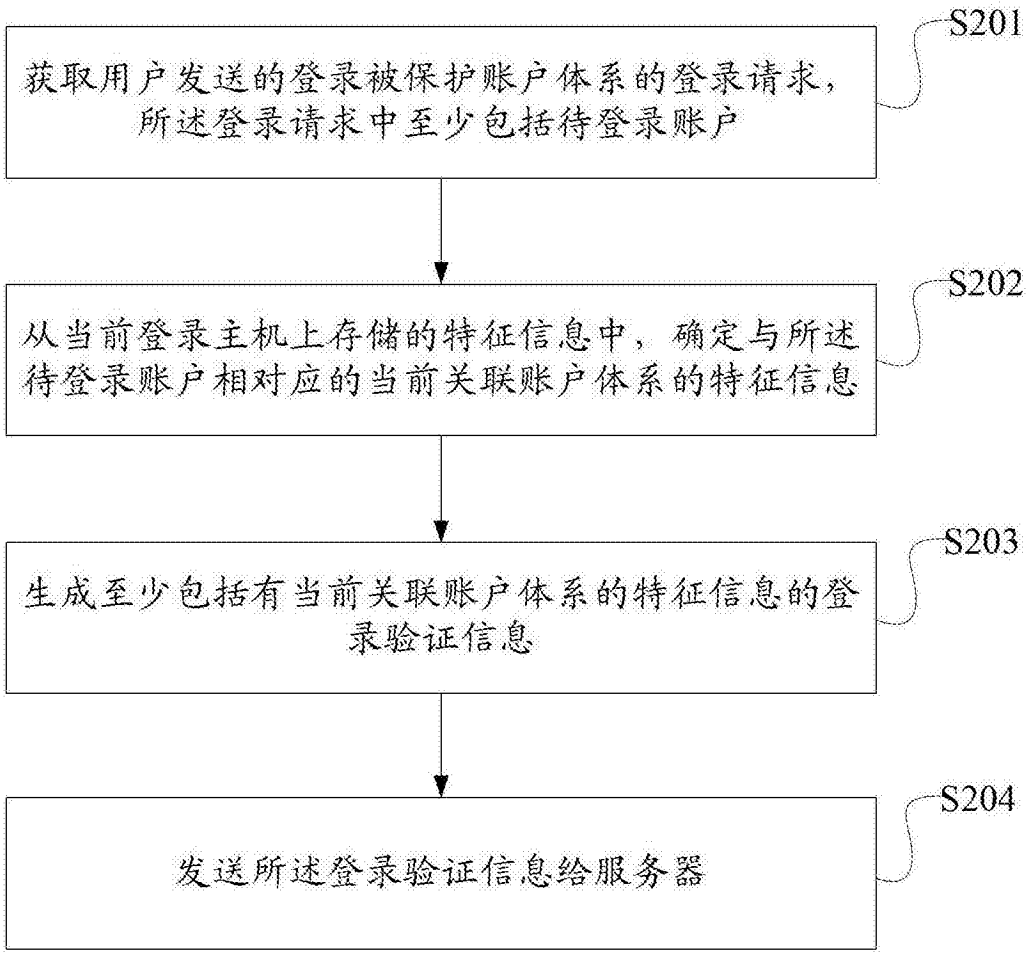


图2

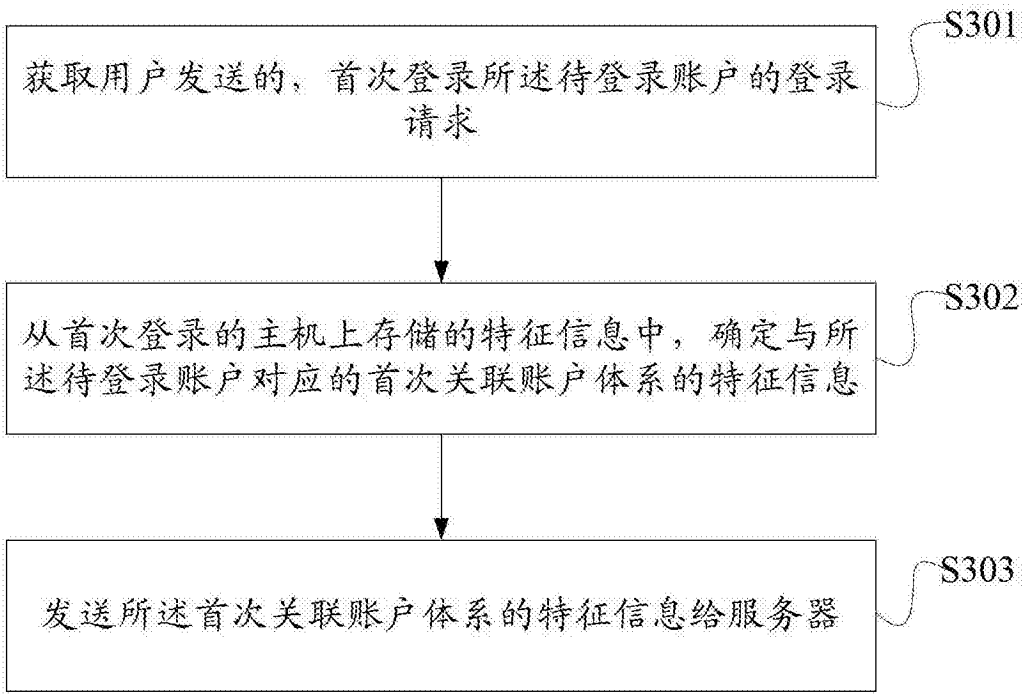

S301
获取用户发送的，首次登录所述待登录账户的登录请求
S302
从首次登录的主机上存储的特征信息中，确定与所述待登录账户对应的首次关联账户体系的特征信息
S303
发送所述首次关联账户体系的特征信息给服务器

图3

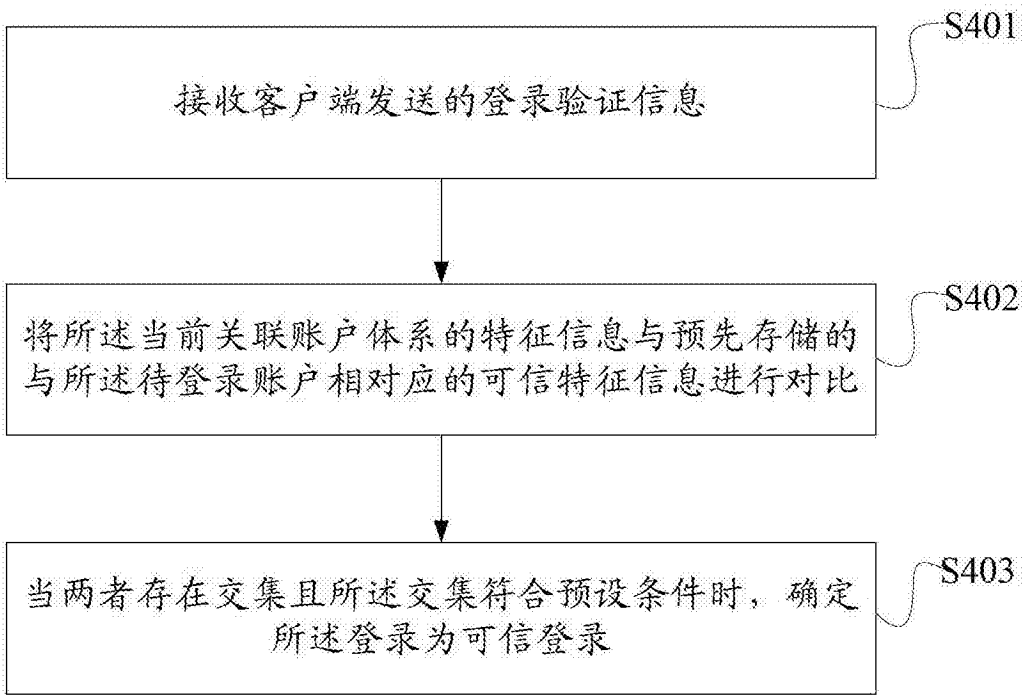

S401
接收客户端发送的登录验证信息
S402
将所述当前关联账户体系的特征信息与预先存储的与所述待登录账户相对应的可信特征信息进行对比
S403
当两者存在交集且所述交集符合预设条件时，确定所述登录为可信登录

图4

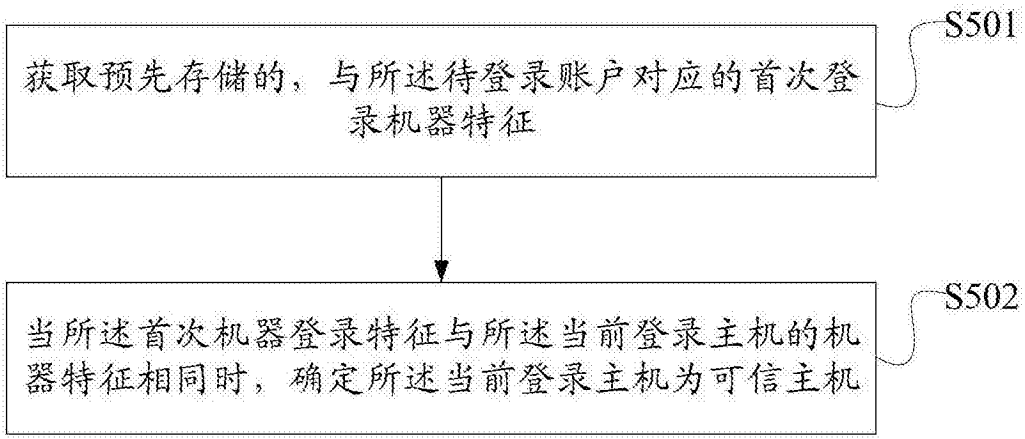

S501
获取预先存储的，与所述待登录账户对应的首次登录机器特征
S502
当所述首次机器登录特征与所述当前登录主机的机器特征相同时，确定所述当前登录主机为可信主机

图5

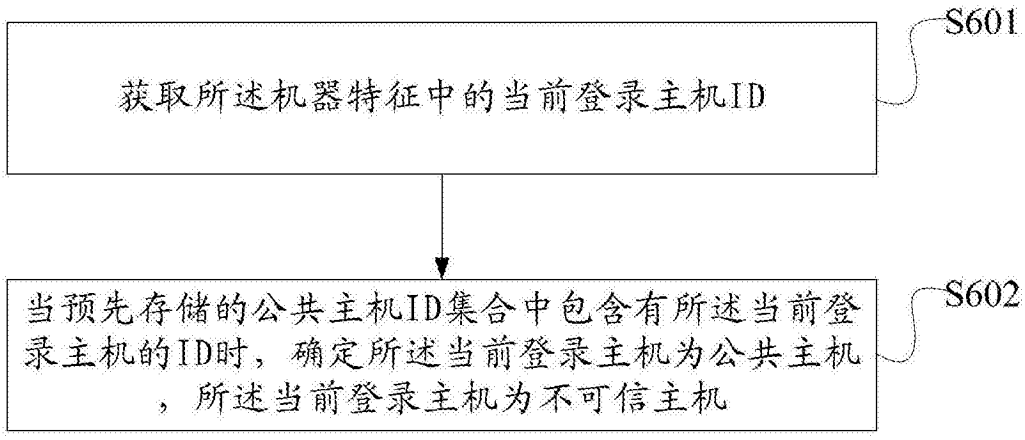

S601
获取所述机器特征中的当前登录主机ID
S602
当预先存储的公共主机ID集合中包含有所述当前登录主机的ID时，确定所述当前登录主机为公共主机，所述当前登录主机为不可信主机

图6

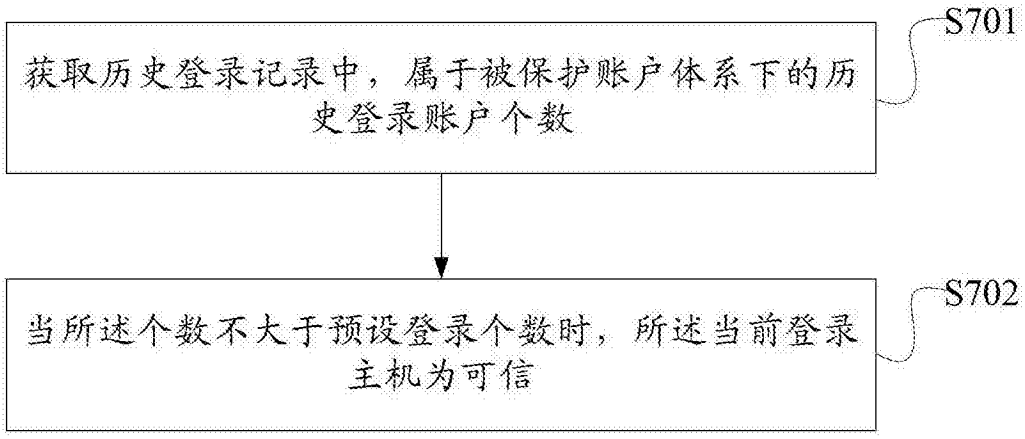

S701
获取历史登录记录中，属于被保护账户体系下的历史登录账户个数
S702
当所述个数不大于预设登录个数时，所述当前登录主机为可信

图7

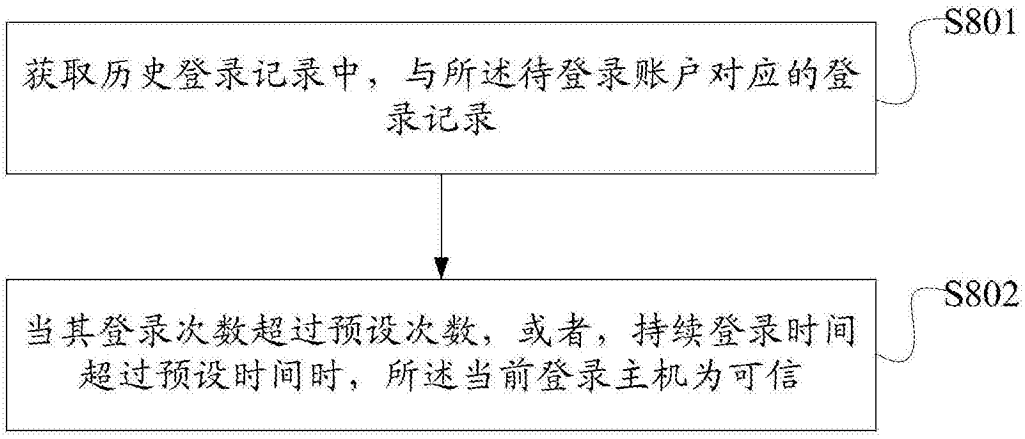

S801
获取历史登录记录中，与所述待登录账户对应的登录记录
S802
当其登录次数超过预设次数，或者，持续登录时间超过预设时间时，所述当前登录主机为可信

图8

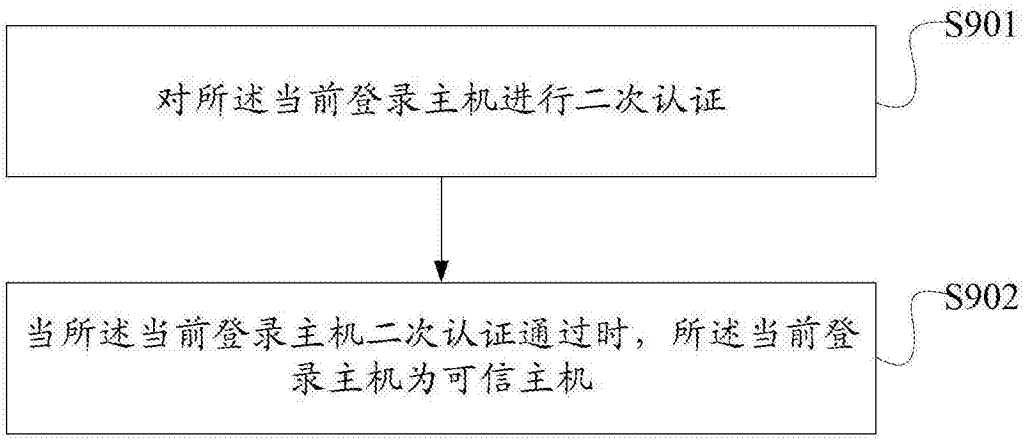

S901
对所述当前登录主机进行二次认证
S902
当所述当前登录主机二次认证通过时，所述当前登录主机为可信主机

图9

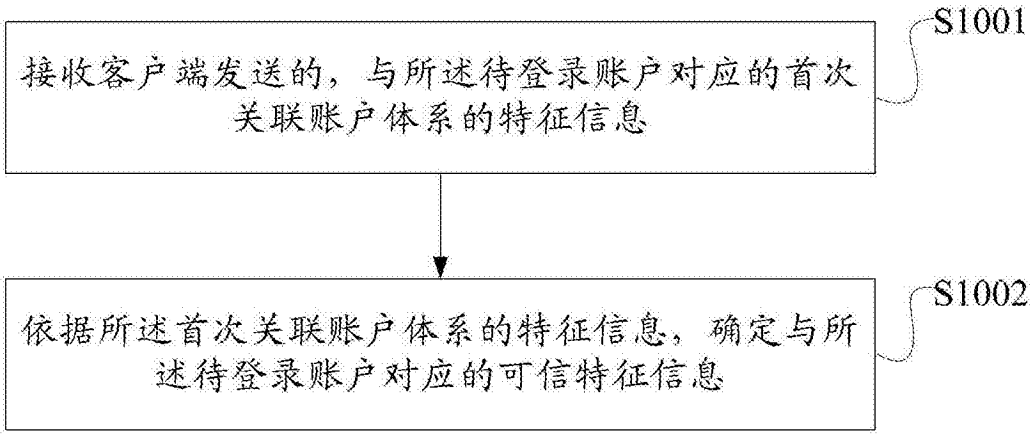

S1001
接收客户端发送的，与所述待登录账户对应的首次关联账户体系的特征信息
S1002
依据所述首次关联账户体系的特征信息，确定与所述待登录账户对应的可信特征信息

图10

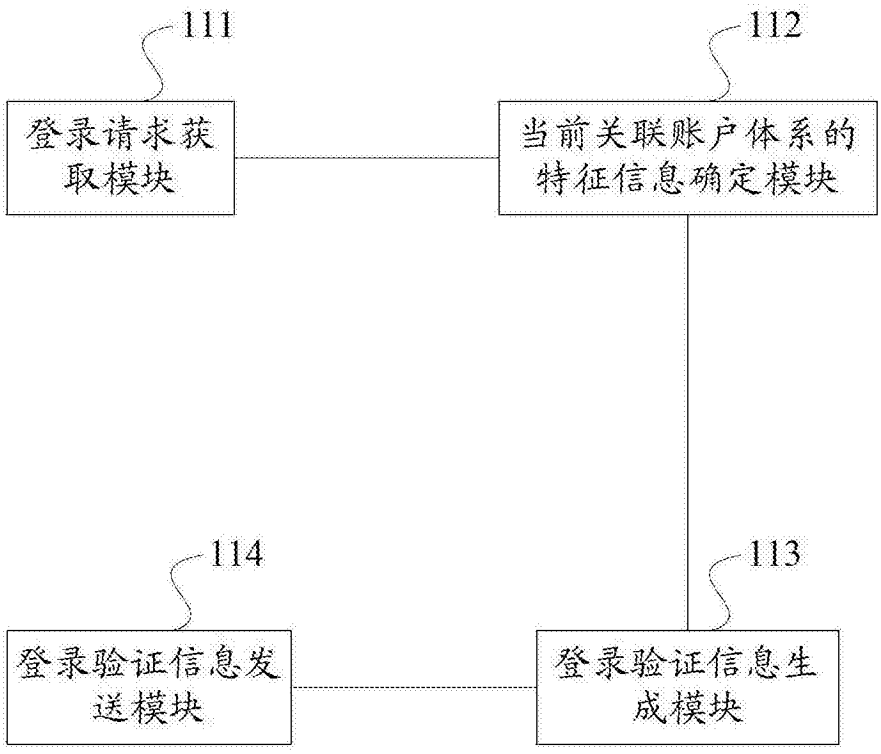

111
登录请求获取模块
112
当前关联账户体系的特征信息确定模块
114
登录验证信息发送模块
113
登录验证信息生成模块

图11

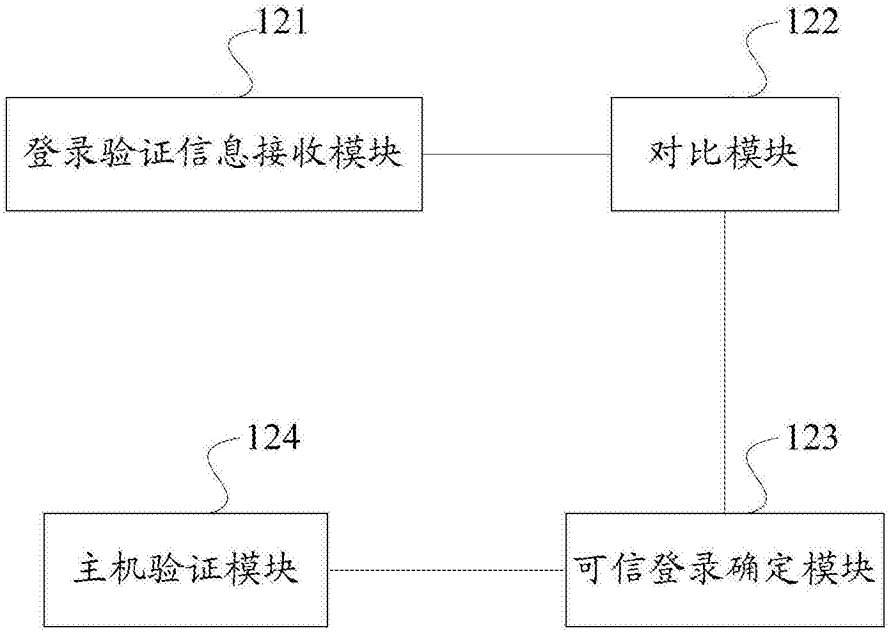

121
登录验证信息接收模块
122
对比模块
124
主机验证模块
123
可信登录确定模块

图12

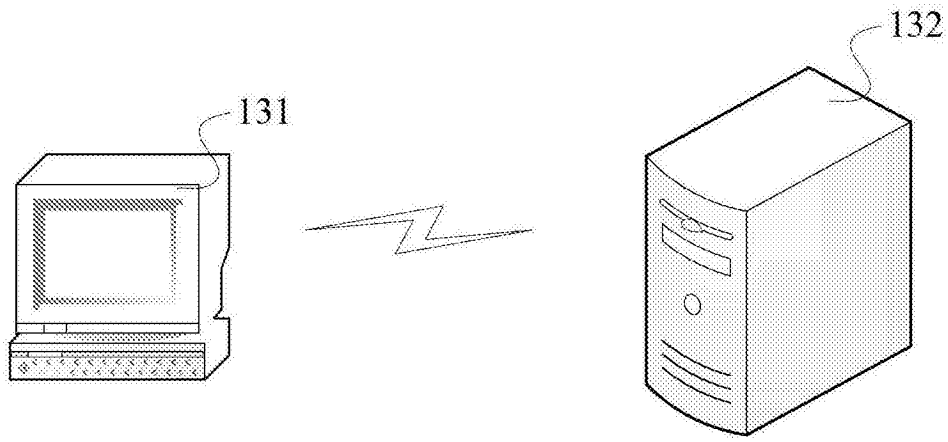


图13