(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 107864112 B
(45)授权公告日 2021.01.26

(21)申请号 201610859658.7

(22)申请日 2016.09.28

(65)同一申请的已公布的文献号
申请公布号 CN 107864112 A

(43)申请公布日 2018.03.30

(73)专利权人 平安科技(深圳)有限公司
地址 518000 广东省深圳市福田区八卦岭工业区平安大厦六楼

(72)发明人 王胡园

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

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

(56)对比文件
CN 103581108 A,2014.02.12
CN 104580075 A,2015.04.29

审查员 李红玲

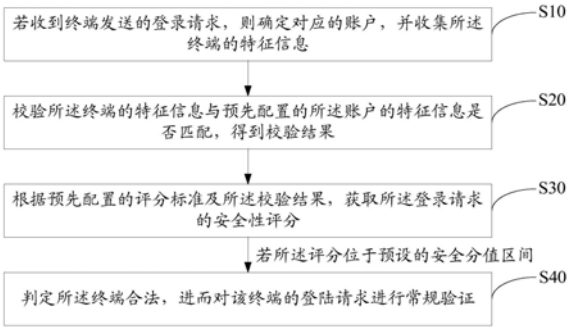
权利要求书2页 说明书11页 附图4页

(54)发明名称

登录安全验证方法和装置

(57)摘要

本发明公开了一种登录安全验证方法，该方法包括：若收到终端发送的登录请求，则确定对应的账户，并收集所述终端的特征信息；校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配，得到校验结果；根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分；若所述评分位于预设的安全分值区间，则判定所述终端合法，进而对该终端的登陆请求进行常规验证。本发明还公开了一种登录安全验证装置。本发明提高了登录验证的安全性。



CN 107864112 B

1.一种登录安全验证方法,其特征在于,所述登录安全验证方法包括以下步骤:

若收到终端发送的登录请求,则确定对应的账户,并收集所述终端的特征信息,收集的特征信息是当前终端所独有的、区别于其他终端的,收集的特征信息包括网络协议IP地址、浏览器或应用软件的类型、浏览器或应用软件的版本、浏览历史记录、历史行为特征以及所述终端的操作系统中的至少两项,所述历史行为特征包括收藏的页面、常用页面、操作习惯以及根据常用页面分析得到的常用购物网站和常用搜索网站;

逐项校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配,得到校验结果;

根据预先配置的评分标准及所述校验结果中各项特征信息的匹配结果,获取各项特征信息的评分,根据预先配置的各项特征信息的权重及各项特征信息的评分计算得到所述登录请求的安全性评分,在配置评分标准时根据所述特征信息的伪造难易程度为各项特征信息赋予不同的分值;

若所述安全性评分位于预设的安全分值区间,则判定所述终端合法,进而对该终端的登陆请求进行常规验证,并在登录请求通过验证后根据当前终端的特征信息更新当前登录的账户对应的特征信息;

若所述安全性评分位于预设的风险分值区间,则判定所述终端存在风险,进而对该终端的登陆请求进行常规验证,并在所述登录请求通过所述常规验证后提示用户该终端的登录操作存在风险;

若所述安全性评分位于预设的危险分值区间,则判定所述终端不合法,并锁定与所述登录请求对应的账户;

接收基于所述账户的解锁请求,并进行验证;

若所述解锁请求通过验证,则解锁所述账户,并收集成功登录所述账户的终端的特征信息,用以更新所述账户的特征信息。

2.一种登录安全验证装置,其特征在于,所述登录安全验证装置包括:

收集模块,用于若收到终端发送的登录请求,则确定对应的账户,并收集所述终端的特征信息,收集的特征信息是当前终端所独有的、区别于其他终端的,收集的特征信息包括网络协议IP地址、浏览器或应用软件的类型、浏览器或应用软件的版本、浏览历史记录、历史行为特征以及所述终端的操作系统中的至少两项,所述历史行为特征包括收藏的页面、常用页面、操作习惯以及根据常用页面分析得到的常用购物网站和常用搜索网站;

校验模块,用于逐项校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配,得到校验结果;

评分模块,用于根据预先配置的评分标准及所述校验结果中各项特征信息的匹配结果,获取各项特征信息的评分,根据预先配置的各项特征信息的权重及各项特征信息的评分计算得到所述登录请求的安全性评分,在配置评分标准时根据所述特征信息的伪造难易程度为各项特征信息赋予不同的分值;

验证模块,用于若所述安全性评分位于预设的安全分值区间,则判定所述终端合法,进而对该终端的登陆请求进行常规验证,并在登录请求通过验证后根据当前终端的特征信息更新当前登录的账户对应的特征信息;

验证模块,还用于若所述安全性评分位于预设的风险分值区间,则判定所述终端存在

风险，进而对该终端的登陆请求进行常规验证；

告警模块，用于若由所述验证模块判定存在风险的所述终端的所述登录请求通过所述常规验证，则在通过后提示用户该终端的登录操作存在风险；

锁定模块，用于若所述安全性评分位于预设的危险分值区间，则判定所述终端不合法，并锁定与所述登录请求对应的账户；

解锁模块，用于接收基于所述账户的解锁请求，并进行验证；若所述解锁请求通过验证，则解锁所述账户，并收集成功登录所述账户的终端的特征信息，用以更新所述账户的特征信息。

登录安全验证方法和装置

技术领域

[0001] 本发明涉及互联网技术领域，尤其涉及一种登录安全验证方法和装置。

背景技术

[0002] 用户登录WEB(网页)网站、APP(Application，应用软件)等所使用的账户中通常保存有用户的私人信息，甚至可能涉及用户的财产信息。而钓鱼攻击可以通过各种手段获取用户的登录凭据，例如登录密码，从而冒充用户登录。

[0003] 若用户的登录账户受到钓鱼攻击，被窃取登录凭据，则会造成用户隐私数据的泄露或财产损失。因此，目前仅验证登录请求，依靠登录密码等传统的登录凭据进行登录账户的验证，难以保障登录账户的安全性。

发明内容

[0004] 本发明的主要目的在于提供一种登录安全验证方法和装置，旨在解决账户登录安全性不高的技术问题。

[0005] 为实现上述目的，本发明提供一种登录安全验证方法，所述登录安全验证方法包括以下步骤：

[0006] 若收到终端发送的登录请求，则确定对应的账户，并收集所述终端的特征信息；

[0007] 校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配，得到校验结果；

[0008] 根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分；

[0009] 若所述评分位于预设的安全分值区间，则判定所述终端合法，进而对该终端的登陆请求进行常规验证。

[0010] 优选地，所述根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分的步骤之后，还包括：

[0011] 若所述评分位于预设的风险分值区间，则判定所述终端存在风险，进而对该终端的登陆请求进行常规验证；

[0012] 若所述登录请求通过所述常规验证，则在通过后提示用户该终端的登录操作存在风险。

[0013] 优选地，所述根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分的步骤之后，还包括，

[0014] 若所述评分位于预设的危险分值区间，则判定所述终端不合法，并锁定与所述登录请求对应的账户。

[0015] 优选地，所述锁定与所述登录请求对应的账户的步骤之后，还包括，

[0016] 接收基于所述账户的解锁请求，并进行验证；

[0017] 若所述解锁请求通过验证，则解锁所述账户，并收集成功登录所述账户的终端的特征信息，用以更新所述账户的特征信息。

[0018] 优选地，所述收集的特征信息包括网络协议IP地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征，所述终端的操作系统中的至少两项。

[0019] 此外，为实现上述目的，本发明还提供一种登录安全验证装置，所述登录安全验证装置包括：

[0020] 收集模块，用于若收到终端发送的登录请求，则确定对应的账户，并收集所述终端的特征信息；

[0021] 校验模块，用于校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配，得到校验结果；

[0022] 评分模块，用于根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分；

[0023] 验证模块，用于若所述评分位于预设的安全分值区间，则判定所述终端合法，进而对该终端的登陆请求进行常规验证。

[0024] 优选地，所述验证模块还用于，

[0025] 若所述评分位于预设的风险分值区间，则判定所述终端存在风险，进而对该终端的登陆请求进行常规验证；

[0026] 所述登录安全验证装置还包括：

[0027] 告警模块，用于若所述登录请求通过所述常规验证，则在通过后提示用户该终端的登录操作存在风险。

[0028] 优选地，所述登录安全验证装置还包括，

[0029] 锁定模块，用于若所述评分位于预设的危险分值区间，则判定所述终端不合法，并锁定与所述登录请求对应的账户。

[0030] 优选地，所述登录安全验证装置还包括，

[0031] 解锁模块，用于接收基于所述账户的解锁请求，并进行验证；若所述解锁请求通过验证，则解锁所述账户，并收集成功登录所述账户的终端的特征信息，用以更新所述账户的特征信息。

[0032] 优选地，所述收集的特征信息包括网络协议IP地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征，所述终端的操作系统中的至少两项。

[0033] 本发明提出的一种登录安全验证方法和装置，若收到终端发送的登录请求，则确定对应的当前请求登录的账户，并收集终端的特征信息，收集得到的特征信息可以将此终端与网络空间中的其他终端区别开来，反映了用户的个人特征；然后，校验终端的特征信息与预先配置的当前请求登录的账户的特征信息是否匹配，得到校验结果，从而可以判断当前终端是否登录当前账户的常用或是合法终端；然后，根据预先配置的评分标准及校验结果，为当前登录请求的安全性打分，获取登录请求的安全性评分；若评分位于预设的安全分值区间，则判定当前的终端合法，进而对登录请求进行常规验证，例如验证登录密码等登录凭据，完成对登录请求的验证。本发明中通过收集终端的特征信息，得到登录用户的个体特征，由于个体特征的差异化和个性化，不可能存在完全相同的两个个体，在登录时进行个体特征的匹配以保障登录安全，再结合登录请求的验证，有效提高了登录验证的安全性。本发明能够有效识别出钓鱼攻击者，保障用户账户的安全。

附图说明

[0034] 图1为本发明登录安全验证方法第一实施例的流程示意图；

[0035] 图2为本发明登录安全验证方法第二实施例的流程示意图；

[0036] 图3为本发明登录安全验证方法第三实施例的流程示意图；

[0037] 图4为本发明登录安全验证方法第四实施例的流程示意图；

[0038] 图5为本发明登录安全验证装置第一实施例的功能模块示意图；

[0039] 图6为本发明登录安全验证装置第二实施例的功能模块示意图；

[0040] 图7为本发明登录安全验证装置第三实施例的功能模块示意图；

[0041] 图8为本发明登录安全验证装置第四实施例的功能模块示意图。

[0042] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0043] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0044] 参照图1，本发明登录安全验证方法第一实施例提供一种登录安全验证方法，所述登录安全验证方法包括：

[0045] 步骤S10、若收到终端发送的登录请求，则确定对应的账户，并收集所述终端的特征信息。

[0046] 本发明在收到登录请求时，通过验证发送登录请求的终端的特征信息，判断当前登录的用户是否正常用户，从而实现对登录请求安全性的验证。

[0047] 具体的，作为一种实施方式，服务器端在收到手机、电脑等终端发送的登录请求时，根据登录请求携带的账户信息确定当前登录的账户。

[0048] 同时，服务器端收集当前终端的特征信息，收集的特征信息是当前终端所独有的、区别于其他终端的。

[0049] 进一步的，收集的特征信息包括IP(Internet Protocol，网络协议)地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征，当前终端的操作系统中的至少两项。

[0050] 其中，IP地址为当前终端的IP地址；若当前登录的是WEB应用，则收集发送登录请求的浏览器的类型、版本，若当前登录的是终端上安装的应用软件，则收集此应用软件的类型、版本；浏览历史记录包括浏览器或应用软件的浏览页面的历史记录，可仅获取预设的时间段内的历史记录。

[0051] 历史行为特征则是根据浏览历史记录分析得到的用户行为特征，包括收藏的页面、常用页面、操作习惯，以及根据常用页面分析得到的常用购物网站、常用搜索网站等个体特征信息。

[0052] 当前终端的操作系统包括了当前终端使用的操作系统类型及版本信息，例如Windows XP、Windows 7、安卓、IOS等。

[0053] 服务器端收集的终端特征信息可以根据实际需要，灵活选取需要收集的特征信息；或是根据预先配置的收集项，对应收集IP地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征以及终端的操作系统中的至少两项。

[0054] 虽然网络空间中存在大量的终端个体，但是网络空间中不会存在上述各项信息都

完全一致的两个终端，因此通过收集、整理得到的上述各项信息，可以作为一个终端的特征信息。当然，还可以进一步的收集终端其他的个性化信息，作为终端的特征信息。

[0055] 收集得到的终端的特征信息，在一定程度上反映了使用此终端的用户的个体特征。

[0056] 步骤S20、校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配，得到校验结果。

[0057] 在得到当前终端的特征信息后，服务器端将当前终端的特征信息与预先配置的当前账户的特征信息进行匹配校验，得到校验结果。

[0058] 作为一种实施方式，服务器端预先收集、配置有当前登录账户对应的终端特征信息，具体的，可以在账户正常登录的状态下进行登录终端特征信息的收集与分析整理，包括IP地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征，终端的操作系统中的至少两项，作为账户对应的特征信息保存。

[0059] 则，服务器端在获取当前收集的终端的特征信息后，可以逐项根据终端的特征信息进行核验匹配，也即，分别核验当前收集的终端的IP地址与当前账户特征信息中的IP地址是否一致；核验当前收集的终端的浏览器或应用软件的类型、版本，与当前账户特征信息中的浏览器或应用软件的类型、版本是否一致；核验当前收集的终端的浏览历史记录与当前账户特征信息中的同一时间段的浏览历史记录是否一致；核验当前收集的终端的历史行为特征与当前账户特征信息中的历史行为特征是否一致；核验当前收集的终端的操作系统与当前账户特征信息中的操作系统是否一致。

[0060] 在分别校验各项特征信息后，得到各项特征信息是否匹配的校验结果。

[0061] 步骤S30、根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分。

[0062] 在得到校验结果后，服务器端根据预先配置的评分标准，为当前登录请求的安全性打分。

[0063] 具体的，预先配置的评分标准中记录了各项特征信息对应的评分标准，同一项特征信息还可以根据匹配程度配置有不同的评分标准，例如，若当前收集的终端的IP地址与当前账户特征信息中的IP地址完全相同、完全匹配，则可以配置IP地址项获取此项特征信息的全部分值；若当前收集的终端的IP地址与当前账户特征信息中的IP地址不相同，但属于同一地区，匹配程度低，则可以配置IP地址项获取此项特征信息的部分分值；若当前收集的终端的IP地址与当前账户特征信息中的IP地址不相同，且不属于同一地区，完全不匹配，则可以配置IP地址项不获取此项特征信息的分值。

[0064] 进一步的，在配置评分标准时，可以根据特征信息的伪造难以程度，赋予不同的分值，例如IP地址容易伪造，可对应配置此项信息的分值较低；历史行为特征较难伪造，则可以配置此项信息的分值较高。

[0065] 服务器端根据预先配置的评分标准及校验结果中各项特征信息的匹配结果，依次为各项特征信息打分，获取各项特征信息的评分。

[0066] 然后，服务器端将各项特征信息的评分加和，作为当前登录请求的安全性评分；或服务器端根据预先配置的各项特征信息的权重及各项特征信息的评分，计算得到的总分值作为当前登录请求的安全性评分。

[0067] 由此，得到当前登录请求的安全性评分。

[0068] 步骤S40、若所述评分位于预设的安全分值区间，则判定所述终端合法，进而对该终端的登陆请求进行常规验证。

[0069] 在得到当前登录请求的安全性评分后，服务器端判断评分是否位于预设的安全分值区间。预设的安全分值区间内的分值较高，位于此分值区间内的评分可以认为是安全性高的评分。

[0070] 安全分值区间的最高分可以是预设的评分标准中，各项特征信息完全匹配时的评分之和；最低分可以是根据实际需要配置的安全阈值。则小于或等于最高分，且大于或等于安全阈值的评分，是位于安全分值区间的。

[0071] 若评分位于预设的安全分值区间，可以认为当前终端是登录当前账户常用的或合法的终端，进一步的，可以判定当前的登录请求是安全的。

[0072] 需要说明的是，在本实施例中，在所述终端被判断为合法终端后，服务器端会转入对该终端的登录请求进行常规验证的流程。所述常规验证流程包括，但不仅限于对登录请求中所携带的用户输入的用户账户信息，例如账户名、账户密码、用户指纹、验证码等信息的验证工作。该常规验证为现有技术，类似于常见的用户登陆验证操作，故此处不再赘述。其中，若所述常规验证通过，则所述终端登陆成功；若所述常规验证未通过，则所述终端登陆失败。

[0073] 进一步的，考虑到用户个体特征可能随着时间或其他因素发生变化，则在登录请求通过验证后，还可以根据当前终端的特征信息，更新当前登录的账户对应的特征信息，以保障后续登录安全性验证的准确性。

[0074] 在本实施例中，若收到终端发送的登录请求，则确定对应的当前请求登录的账户，并收集终端的特征信息，收集得到的特征信息可以将此终端与网络空间中的其他终端区别开来，反映了用户的个人特征；然后，校验终端的特征信息与预先配置的当前请求登录的账户的特征信息是否匹配，得到校验结果，从而可以判断当前终端是否登录当前账户的常用或是合法终端；然后，根据预先配置的评分标准及校验结果，为当前登录请求的安全性打分，获取登录请求的安全性评分；若评分位于预设的安全分值区间，则判定当前的终端合法，进而对登录请求进行常规验证，例如验证登录密码等登录凭据，完成对登录请求的验证。本实施例中通过收集终端的特征信息，得到登录用户的个体特征，由于个体特征的差异化和个性化，不可能存在完全相同的两个个体，在登录时进行个体特征的匹配以保障登录安全，再结合登录请求的验证，有效提高了登录验证的安全性。本实施例能够有效识别出钓鱼攻击者，保障用户账户的安全。

[0075] 进一步的，参照图2，本发明登录安全验证方法第二实施例提供一种登录安全验证方法，基于上述图1所示的实施例，所述S30的步骤之后，还包括，

[0076] 步骤S50、若所述评分位于预设的风险分值区间，则判定所述终端存在风险，进而对该终端的登陆请求进行常规验证；

[0077] 步骤S60、若所述登录请求通过所述常规验证，则在通过后提示用户该终端的登录操作存在风险。

[0078] 在获取当前登录请求的安全性评分后，若评分位于预设的风险分值区间此时，服务器端认为当前终端存在风险，发送的登录请求也存在风险。

[0079] 风险分值区间的最高分可以是安全阈值;最低分可以是根据实际需要配置的风险阈值,安全阈值大于风险阈值。则小于安全阈值,且大于或等于风险阈值的评分,是位于风险分值区间的。

[0080] 则服务器端进一步对登录请求进行常规验证,验证登录请求中的登录凭据,例如密码、验证码等。

[0081] 若登录请求通过常规验证,则可通过弹窗等形式,发布登录操作存在风险的告警提示。或是向当前账户绑定的邮箱、手机等发送登录操作存在风险的告警提示,以供用户及时处理非法登录。

[0082] 进一步的,考虑到用户个体特征可能随着时间或其他因素发生变化,则在登录请求通过验证后,还可以根据当前终端的特征信息,更新当前登录的账户对应的特征信息,以保障后续登录安全性验证的准确性。

[0083] 在本实施例中,若登录请求安全性的评分位于预设的风险分值区间,则判定当前终端存在风险,进而对该终端的登陆请求进行常规验证;若当前登录请求通过常规验证,则在通过后提示用户该终端的登录操作存在风险,提醒用户及时处理风险登录。本实施例在登录请求存在风险的情况下,能够及时提醒用户存在的风险,实现了多种信任机制配合进行登录请求安全性的验证,提高了登录请求安全性验证的灵活性,更加贴近实际应用。

[0084] 进一步的,参照图3,本发明登录安全验证方法第三实施例提供一种登录安全验证方法,基于上述图1或图2所示的实施例(本实施例以图1为例),所述步骤S30之后,还包括,

[0085] 步骤S70、若所述评分位于预设的危险分值区间,则判定所述终端不合法,锁定与所述登录请求对应的账户。

[0086] 在获取当前登录请求的安全性评分后,若评分位于预设的危险分值区间此时,服务器端认为当前的终端异常,终端发送的登录请求也存在异常。

[0087] 风险分值区间的最高分可以是风险阈值;最低分可以是根据实际需要配置的危险阈值或不配置。则小于风险阈值的评分,都是位于危险分值区间的。

[0088] 则服务器端直接锁定与当前的登录请求对应的账户,使当前账户无法登陆。锁定当前账户的时间可以是预设的时间段,例如一天、两个小时等,在预设的时间段内均拒绝此账户的登录请求,在超过预设的时间段后在重新验证。

[0089] 当然,为了保障账户的安全性,还可以一直锁定此账户,直至用户使用信任机制更高的方式进行解锁。

[0090] 在本实施例中,在评分较低、位于预设的危险分值区间的情况下,自动锁定与当前登录请求对应的账户,以保障账户的安全性,实现了多种信任机制配合进行登录请求安全性的验证,提高了登录请求安全性验证的灵活性,更加贴近实际应用。

[0091] 进一步的,本发明登录安全验证方法第四实施例提供一种登录安全验证方法,基于上述图3所示的实施例,所述步骤S70之后,还包括:

[0092] 步骤S80、接收基于所述账户的解锁请求,并进行验证;

[0093] 步骤S90、若所述解锁请求通过验证,则解锁所述账户,并收集登录成功所述账户的终端的特征信息,用以更新所述账户的特征信息。

[0094] 在当前登录的账户被锁定后,若服务器端收到基于此账户发送的解锁请求,则进行解锁请求的验证。

[0095] 用户可以通过多种形式进行账户解锁，例如拨打服务电话，根据自助语音提示输入身份证号等信任机制更高的信息进行解锁，或是通过短信、邮箱等多种方式申请解锁。当然，还可以通过人工服务进行账户的解锁。

[0096] 服务器端在收到解锁请求后，根据账户预先配置的安全验证信息验证解锁请求，若解锁请求通过验证，则服务器端解锁账户。

[0097] 然后，服务器端重新收集登录此账户的终端特征信息，更新此账户的特征信息。收集的特征信息包括IP地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征，终端的操作系统中的至少两项。

[0098] 在本实施例中，账户被锁定后，接收基于此账户的解锁请求，并进行验证；若解锁请求通过验证，则解锁此账户，收集成功登录此账户的终端的特征信息，用以更新账户的特征信息，从而在用户更换常用终端或离开常用场景时，能够重新配置或更新账户对应的特征信息，保障后续验证登录请求安全性的准确率。

[0099] 参照图5，本发明登录安全验证装置第一实施例提供一种登录安全验证装置，所述登录安全验证装置包括：

[0100] 收集模块10，用于若收到终端发送的登录请求，则确定对应的账户，并收集所述终端的特征信息。

[0101] 本发明在收到登录请求时，通过验证发送登录请求的终端的特征信息，判断当前登录的用户是否正常用户，从而实现对登录请求安全性的验证。登录安全验证装置可部署在服务器端。

[0102] 具体的，作为一种实施方式，收集模块10在收到手机、电脑等终端发送的登录请求时，根据登录请求携带的账户信息确定当前登录的账户。

[0103] 同时，收集模块10收集当前终端的特征信息，收集的特征信息是当前终端所独有的、区别于其他终端的。

[0104] 进一步的，收集的特征信息包括IP(Internet Protocol，网络协议)地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征，当前终端的操作系统中的至少两项。

[0105] 其中，IP地址为当前终端的IP地址；若当前登录的是WEB应用，则收集发送登录请求的浏览器的类型、版本，若当前登录的是终端上安装的应用软件，则收集此应用软件的类型、版本；浏览历史记录包括浏览器或应用软件的浏览页面的历史记录，可仅获取预设的时间段内的历史记录。

[0106] 历史行为特征则是根据浏览历史记录分析得到的用户行为特征，包括收藏的页面、常用页面、操作习惯，以及根据常用页面分析得到的常用购物网站、常用搜索网站等个体特征信息。

[0107] 当前终端的操作系统包括了当前终端使用的操作系统类型及版本信息，例如Windows XP、Windows 7、安卓、IOS等。

[0108] 收集模块10收集的终端特征信息可以根据实际需要，灵活选取需要收集的特征信息；或是根据预先配置的收集项，对应收集IP地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征以及终端的操作系统中的至少两项。

[0109] 虽然网络空间中存在大量的终端个体，但是网络空间中不会存在上述各项信息都

完全一致的两个终端，因此通过收集、整理得到的上述各项信息，可以作为一个终端的特征信息。当然，还可以进一步的收集终端其他的个性化信息，作为终端的特征信息。

[0110] 收集模块10收集得到的终端的特征信息，在一定程度上反映了使用此终端的用户的个体特征。

[0111] 校验模块20，用于校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配，得到校验结果。

[0112] 在得到当前终端的特征信息后，校验模块20将当前终端的特征信息与预先配置的当前账户的特征信息进行匹配校验，得到校验结果。

[0113] 作为一种实施方式，登录安全验证装置预先收集、配置有当前登录账户对应的终端特征信息，具体的，可以在账户正常登录的状态下进行登录终端特征信息的收集与分析整理，包括IP地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征，终端的操作系统中的至少两项，作为账户对应的特征信息保存。

[0114] 则，在获取当前收集的终端的特征信息后，校验模块20可以逐项根据终端的特征信息进行核验匹配，也即，分别核验当前收集的终端的IP地址与当前账户特征信息中的IP地址是否一致；核验当前收集的终端的浏览器或应用软件的类型、版本，与当前账户特征信息中的浏览器或应用软件的类型、版本是否一致；核验当前收集的终端的浏览历史记录与当前账户特征信息中的同一时间段的浏览历史记录是否一致；核验当前收集的终端的历史行为特征与当前账户特征信息中的历史行为特征是否一致；核验当前收集的终端的操作系统与当前账户特征信息中的操作系统是否一致。

[0115] 在分别校验各项特征信息后，校验模块20得到各项特征信息是否匹配的校验结果。

[0116] 评分模块30，用于根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分。

[0117] 在得到校验结果后，评分模块30根据预先配置的评分标准，为当前登录请求的安全性打分。

[0118] 具体的，预先配置的评分标准中记录了各项特征信息对应的评分标准，同一项特征信息还可以根据匹配程度配置有不同的评分标准，例如，若当前收集的终端的IP地址与当前账户特征信息中的IP地址完全相同、完全匹配，则可以配置IP地址项获取此项特征信息的全部分值；若当前收集的终端的IP地址与当前账户特征信息中的IP地址不相同，但属于同一地区，匹配程度低，则可以配置IP地址项获取此项特征信息的部分分值；若当前收集的终端的IP地址与当前账户特征信息中的IP地址不相同，且不属于同一地区，完全不匹配，则可以配置IP地址项不获取此项特征信息的分值。

[0119] 进一步的，在配置评分标准时，可以根据特征信息的伪造难以程度，赋予不同的分值，例如IP地址容易伪造，可对应配置此项信息的分值较低；历史行为特征较难伪造，则可以配置此项信息的分值较高。

[0120] 评分模块30根据预先配置的评分标准及校验结果中各项特征信息的匹配结果，依次为各项特征信息打分，获取各项特征信息的评分。

[0121] 然后，评分模块30将各项特征信息的评分加和，作为当前登录请求的安全性评分；或服务器端根据预先配置的各项特征信息的权重及各项特征信息的评分，计算得到的总分

值作为当前登录请求的安全性评分。

[0122] 由此，评分模块30得到当前登录请求的安全性评分。

[0123] 验证模块40，用于若所述评分位于预设的安全分值区间，则判定所述终端合法，进而对该终端的登陆请求进行常规验证。

[0124] 在得到当前登录请求的安全性评分后，验证模块40判断评分是否位于预设的安全分值区间。预设的安全分值区间内的分值较高，位于此分值区间内的评分可以认为的安全性高的评分。

[0125] 安全分值区间的最高分可以是预设的评分标准中，各项特征信息完全匹配时的评分之和；最低分可以是根据实际需要配置的安全阈值。则小于或等于最高分，且大于或等于安全阈值的评分，是位于安全分值区间的。

[0126] 若评分位于预设的安全分值区间，可以认为当前终端是登录当前账户常用的或合法的终端，进一步的，验证模块40可以判定当前的登录请求是安全的。

[0127] 需要说明的是，在本实施例中，在所述终端被判断为合法终端后，验证模块40会转入对该终端的登录请求进行常规验证的流程。所述常规验证流程包括，但不仅限于对登录请求中所携带的用户输入的用户账户信息，例如账户名、账户密码、用户指纹、验证码等信息的验证工作。该常规验证为现有技术，类似于常见的用户登陆验证操作，故此处不再赘述。其中，若所述常规验证通过，则所述终端登陆成功；若所述常规验证未通过，则所述终端登陆失败。

[0128] 进一步的，考虑到用户个体特征可能随着时间或其他因素发生变化，则在登录请求通过验证后，登录安全验证装置还可以根据当前终端的特征信息，更新当前登录的账户对应的特征信息，以保障后续登录安全性验证的准确性。

[0129] 在本实施例中，若收到终端发送的登录请求，则收集模块10确定对应的当前请求登录的账户，并收集终端的特征信息，收集得到的特征信息可以将此终端与网络空间中的其他终端区别开来，反映了用户的个人特征；然后，校验模块20校验终端的特征信息与预先配置的当前请求登录的账户的特征信息是否匹配，得到校验结果，从而可以判断当前终端是否登录当前账户的常用或是合法终端；然后，评分模块30根据预先配置的评分标准及校验结果，为当前登录请求的安全性打分，获取登录请求的安全性评分；若评分位于预设的安全分值区间，则验证模块40判定当前的终端合法，进而对登录请求进行常规验证，例如验证登录密码等登录凭据，完成对登录请求的验证。本实施例中通过收集终端的特征信息，得到登录用户的个体特征，由于个体特征的差异化和个性化，不可能存在完全相同的两个个体，在登录时进行个体特征的匹配以保障登录安全，再结合登录请求的验证，有效提高了登录验证的安全性。本实施例能够有效识别出钓鱼攻击者，保障用户账户的安全。

[0130] 进一步的，参照图6，本发明登录安全验证装置第二实施例提供一种登录安全验证装置，基于上述图6所示的实施例，所述验证模块40还用于，

[0131] 若所述评分位于预设的风险分值区间，则判定所述终端存在风险，进而对该终端的登陆请求进行常规验证；

[0132] 所述登录安全验证装置还包括：

[0133] 告警模块50，用于若所述登录请求通过所述常规验证，则在通过后提示用户该终端的登录操作存在风险。

[0134] 在获取当前登录请求的安全性评分后，若评分位于预设的风险分值区间此时，验证模块40认为当前终端存在风险，发送的登录请求也存在风险。

[0135] 风险分值区间的最高分可以是安全阈值；最低分可以是根据实际需要配置的风险阈值，安全阈值大于风险阈值。则小于安全阈值，且大于或等于风险阈值的评分，是位于风险分值区间的。

[0136] 则验证模块40进一步对登录请求进行常规验证，验证登录请求中的登录凭据，例如密码、验证码等。

[0137] 若登录请求通过常规验证，则告警模块50可通过弹窗等形式，发布登录操作存在风险的告警提示。或是向当前账户绑定的邮箱、手机等发送登录操作存在风险的告警提示，以供用户及时处理非法登录。

[0138] 进一步的，考虑到用户个体特征可能随着时间或其他因素发生变化，则在登录请求通过验证后，登录安全验证装置还可以根据当前终端的特征信息，更新当前登录的账户对应的特征信息，以保障后续登录安全性验证的准确性。

[0139] 在本实施例中，若登录请求安全性的评分位于预设的风险分值区间，则判定当前终端存在风险，验证模块40进而对该终端的登陆请求进行常规验证；若当前登录请求通过常规验证，则告警模块50在通过后提示用户该终端的登录操作存在风险，提醒用户及时处理风险登录。本实施例在登录请求存在风险的情况下，能够及时提醒用户存在的风险，实现了多种信任机制配合进行登录请求安全性的验证，提高了登录请求安全性验证的灵活性，更加贴近实际应用。

[0140] 进一步的，参照图7，本发明登录安全验证装置提供一种登录安全验证装置，基于上述图5或6所示的实施例(本实施例以图5为例)，所述登录安全验证装置还包括，

[0141] 锁定模块60，用于若所述评分位于预设的危险分值区间，则判定终端不合法，锁定与所述登录请求对应的账户。

[0142] 在获取当前登录请求的安全性评分后，若评分位于预设的危险分值区间此时，锁定模块60认为当前的终端异常，终端发送的登录请求也存在异常。

[0143] 风险分值区间的最高分可以是风险阈值；最低分可以是根据实际需要配置的危险阈值或不配置。则小于风险阈值的评分，都是位于危险分值区间的。

[0144] 则锁定模块60直接锁定与当前的登录请求对应的账户，使当前账户无法登陆。锁定当前账户的时间可以是预设的时间段，例如一天、两个小时等，在预设的时间段内均拒绝此账户的登录请求，在超过预设的时间段后在重新验证。

[0145] 当然，为了保障账户的安全性，还可以一直锁定此账户，直至用户使用信任机制更高的方式进行解锁。

[0146] 在本实施例中，在评分较低、位于预设的危险分值区间的情况下，锁定模块60自动锁定与当前登录请求对应的账户，以保障账户的安全性，实现了多种信任机制配合进行登录请求安全性的验证，提高了登录请求安全性验证的灵活性，更加贴近实际应用。

[0147] 进一步的，参照图8，本发明登录安全验证装置第四实施例提供一种安全验证装置，基于上述图7所示的实施例，所述登录安全验证装置还包括，

[0148] 解锁模块70，用于接收基于所述账户的解锁请求，并进行验证；若所述解锁请求通过验证，则解锁所述账户，并收集成功登录所述账户的终端的特征信息，用以更新所述账户

的特征信息。

[0149] 在当前登录的账户被锁定后，若解锁模块70收到基于此账户发送的解锁请求，则进行解锁请求的验证。

[0150] 用户可以通过多种形式进行账户解锁，例如拨打服务电话，根据自助语音提示输入身份证号等信任机制更高的信息进行解锁，或是通过短信、邮箱等多种方式申请解锁。当然，还可以通过人工服务进行账户的解锁。

[0151] 解锁模块70在收到解锁请求后，根据账户预先配置的安全验证信息验证解锁请求，若解锁请求通过验证，则解锁模块70解锁账户。

[0152] 然后，解锁模块70重新收集登录此账户的终端特征信息，更新此账户的特征信息。解锁模块70收集的特征信息包括IP地址，浏览器或应用软件的类型、版本，浏览历史记录，历史行为特征，终端的操作系统中的至少两项。

[0153] 在本实施例中，账户被锁定后，解锁模块70接收基于此账户的解锁请求，并进行验证；若解锁请求通过验证，则解锁模块70解锁此账户，收集成功登录此账户的终端的特征信息，用以更新账户的特征信息，从而在用户更换常用终端或离开常用场景时，能够重新配置或更新账户对应的特征信息，保障后续验证登录请求安全性的准确率。

[0154] 以上仅为本发明的可选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

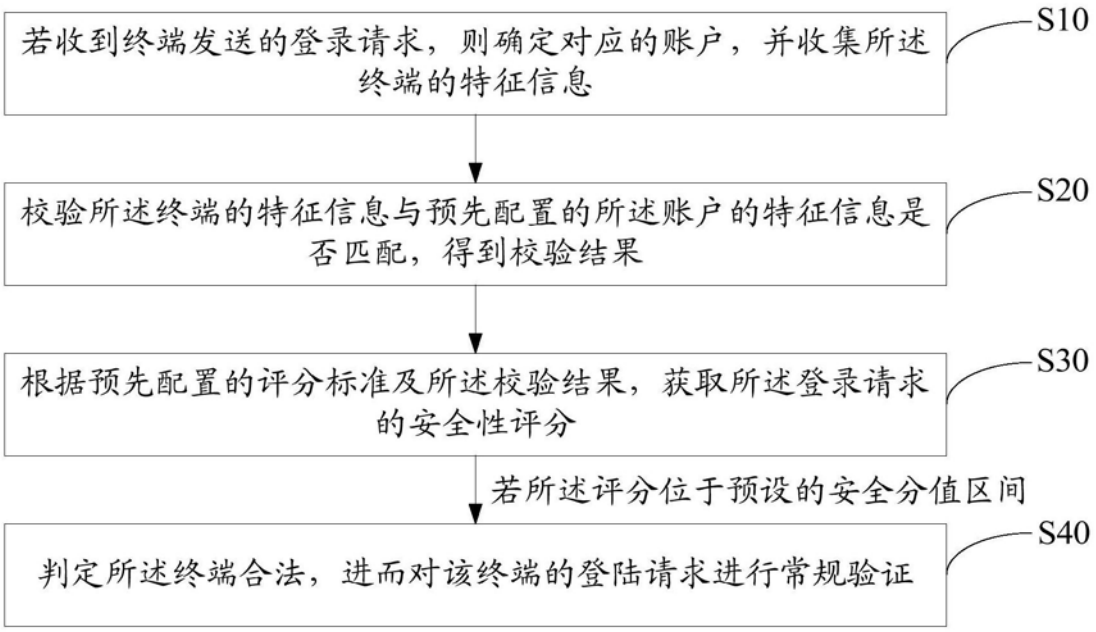

若收到终端发送的登录请求，则确定对应的账户，并收集所述终端的特征信息
S10
校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配，得到校验结果
S20
根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分
S30
若所述评分位于预设的安全分值区间
判定所述终端合法，进而对该终端的登陆请求进行常规验证
S40

图1

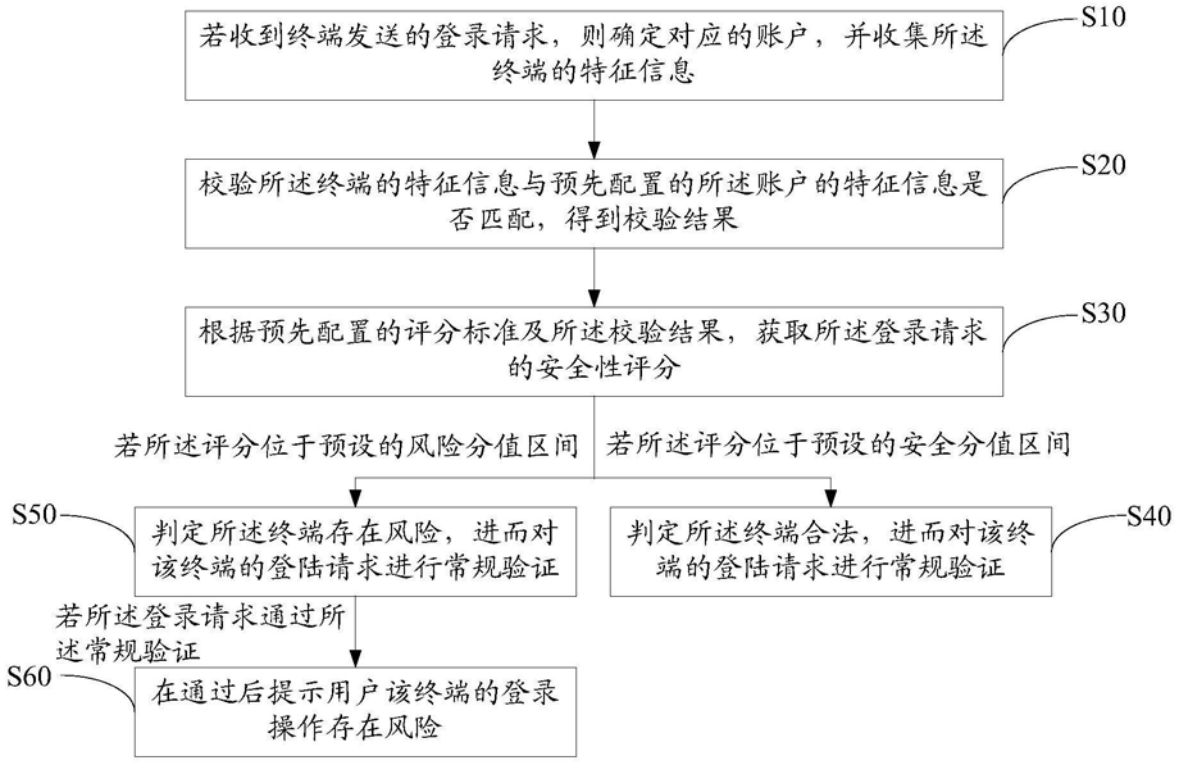

若收到终端发送的登录请求，则确定对应的账户，并收集所述终端的特征信息
S10
校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配，得到校验结果
S20
根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分
S30
若所述评分位于预设的风险分值区间
若所述评分位于预设的安全分值区间
S50
判定所述终端存在风险，进而对该终端的登陆请求进行常规验证
判定所述终端合法，进而对该终端的登陆请求进行常规验证
S40
若所述登录请求通过所述常规验证
S60
在通过后提示用户该终端的登录操作存在风险

图2

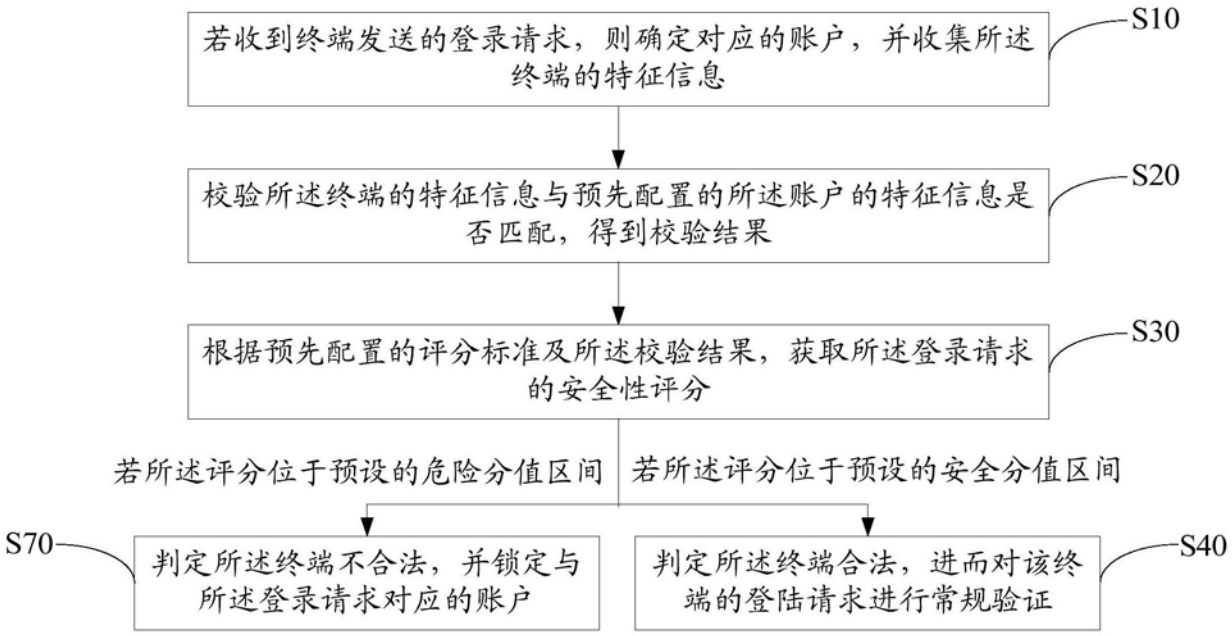

若收到终端发送的登录请求，则确定对应的账户，并收集所述终端的特征信息
S10
校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配，得到校验结果
S20
根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分
S30
若所述评分位于预设的危险分值区间
若所述评分位于预设的安全分值区间
S70
判定所述终端不合法，并锁定与所述登录请求对应的账户
判定所述终端合法，进而对该终端的登陆请求进行常规验证
S40

图3

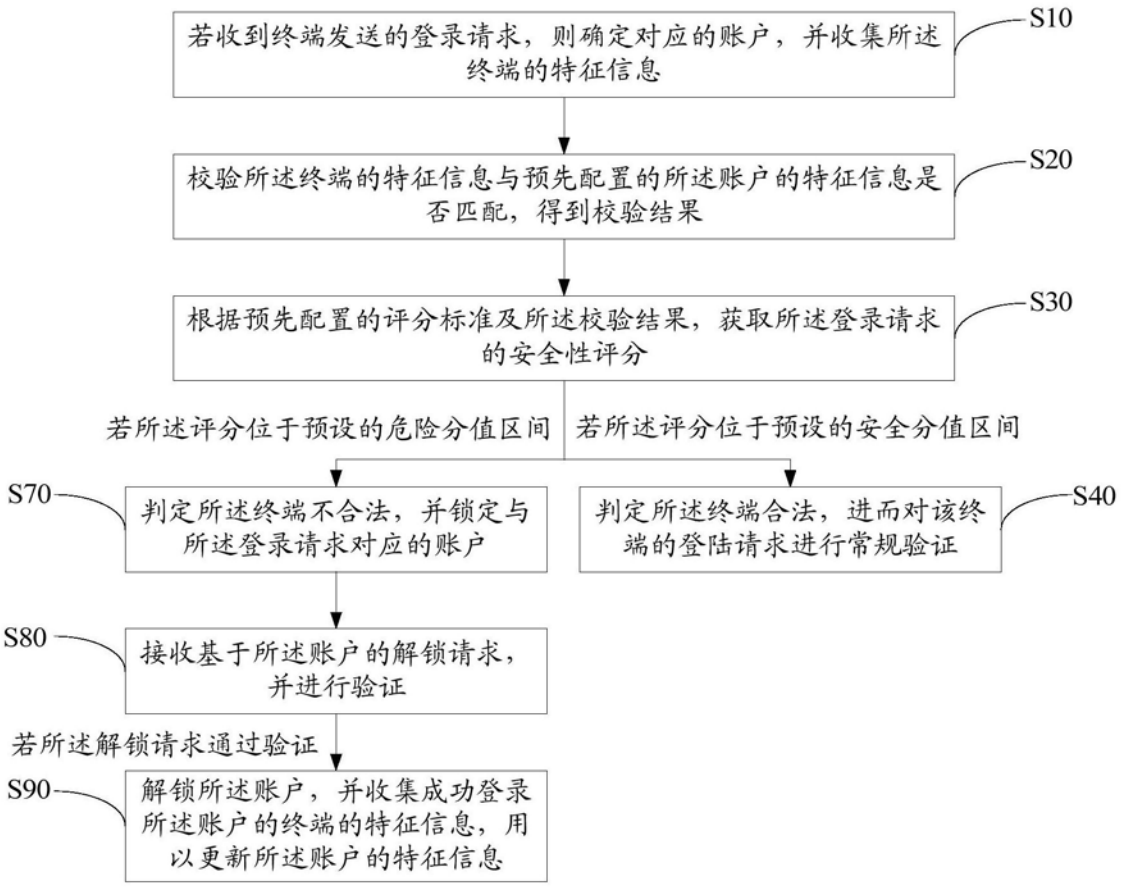

若收到终端发送的登录请求，则确定对应的账户，并收集所述终端的特征信息
S10
校验所述终端的特征信息与预先配置的所述账户的特征信息是否匹配，得到校验结果
S20
根据预先配置的评分标准及所述校验结果，获取所述登录请求的安全性评分
S30
若所述评分位于预设的危险分值区间
若所述评分位于预设的安全分值区间
S70
判定所述终端不合法，并锁定与所述登录请求对应的账户
判定所述终端合法，进而对该终端的登陆请求进行常规验证
S40
S80
接收基于所述账户的解锁请求，并进行验证
若所述解锁请求通过验证
S90
解锁所述账户，并收集成功登录所述账户的终端的特征信息，用以更新所述账户的特征信息

图4

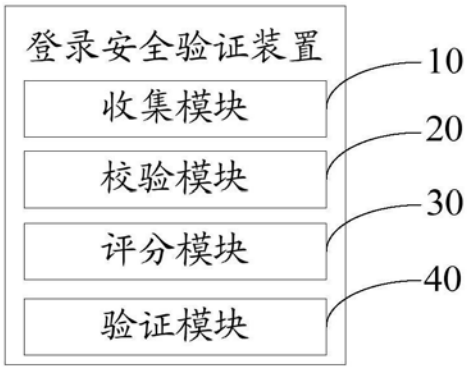

登录安全验证装置
收集模块
校验模块
评分模块
验证模块
10
20
30
40

图5

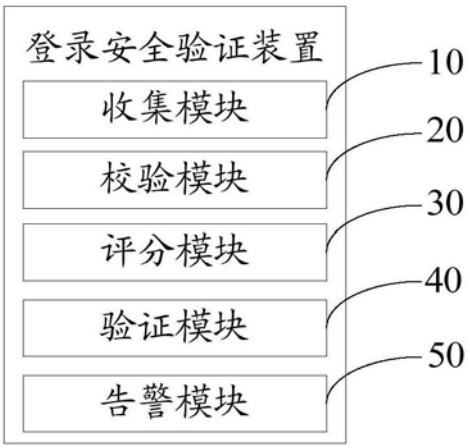

登录安全验证装置
收集模块
校验模块
评分模块
验证模块
告警模块
10
20
30
40
50

图6

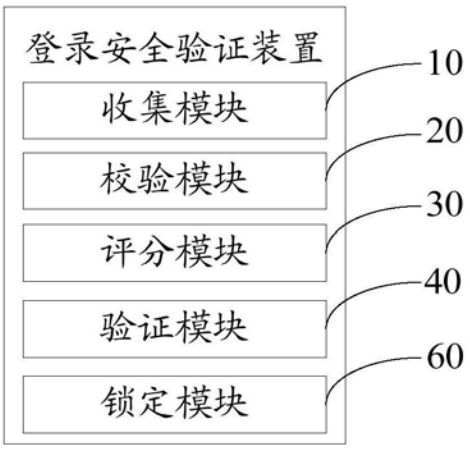

登录安全验证装置
收集模块
校验模块
评分模块
验证模块
锁定模块
10
20
30
40
60

图7

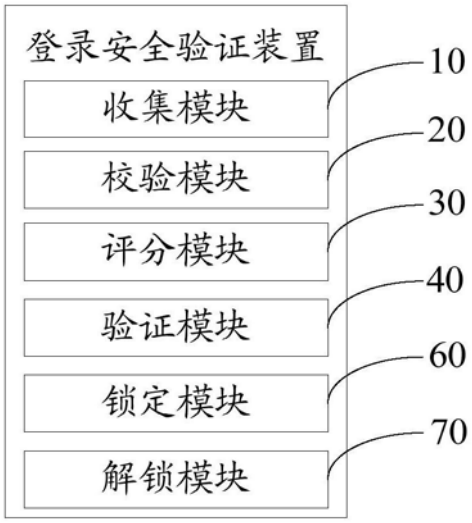


图8